DEFINING "CYBER-CRIME": ISSUES IN DETERMINING THE NATURE AND SCOPE OF COMPUTER-RELATED OFFENSES

Thomas A. Petee, Auburn University
Jay Corzine, University of Central Florida
Lin Huff-Corzine, University of Central Florida
Janice Clifford, Auburn University
Greg Weaver, Auburn University

In recent years, there has been considerable focus within the criminal justice system on computer-related crime. This so-called "cyber-crime" has garnered increased attention because computers have become so central to several areas of social activity connected to everyday life, including, but not limited to, personal and institutional finances, various record-keeping functions, interpersonal communications, and so on. Because of its widespread accessibility, the advent of the Internet has further served to facilitate predatory personal crimes and property offenses committed with a computer. The U.S. Bureau of Census reports that in 2000, there were 94 million people in the United States who made use of the Internet (Newburger, 2001). This greatly expands both the potential victim and offender pools for both personal and property crimes. Moreover, the nature of this forum has allowed some potential offenders to move more easily toward actual criminal behavior, because the victim(s) can be depersonalized in the initial stages of an offense. With the Internet, an offender does not have to come face-to-face with a potential target, which may make it easier for the offender to complete the victimization of the target.

But what exactly is "cyber-crime", and is it distinct from other, more traditional forms of crime? To begin answering these questions, it would be helpful to briefly look at the components of crime in general. Traditionally, crime has been defined as an intentional violation of the legal code that is punishable by the state. Central to this definition is the premise that crime occurs within the boundaries of some physical reference point, that is, a location that constitutes a specific jurisdiction. For example, when a conventional case of fraud occurs, one of the important considerations is where the actual offense took place so that questions of the appropriate jurisdiction for prosecution can be addressed. Officials need to know where the victim and offender came into contact with one another in the perpetration of the offense so that investigative and prosecutorial authority can be determined. However, this component is confounded when cyber-crime is committed because the location is no longer a static concept. With the advent of cyberspace, jurisdiction has become much more problematic, transcending local, state, and even national boundaries. One need only look at the various e-mail scams that emanate from such locales as Nigeria (i.e., the "419" scams), the United Kingdom, or China to begin to

understand how crime is being redefined in the cyber-age.[1]

An equally confounding issue has to do with the scope of cyber-crime. There is a vast range of illegal behavior that could be identified as cyber-crime. Consequently, there seems to be a degree of ambiguity about what is being discussed when the subject of cyber-crime is broached. Fraud, technology theft, security breaches, identity theft, child pornography, and even stalking all potentially fall within the realm of cyber-criminality. Even within the computer community, there seems to be some disagreement about which kinds of behavior should be classified as criminal. There are some who would argue that certain forms of hacking, where a secure computer system is breached and perhaps altered, should never be thought of as a criminal act. Advocates for this position would maintain that the motivation for these actions is often not malicious and may even prove to be beneficial in terms of identifying security shortcomings. Instead, this group would rather see a focus on only those cases where sabotage or financial gain is involved (Schell, Dodge and Moutsatos, 2002). Others, including those in law enforcement communities, would strongly disagree with this position, pointing out that the so-called harmless events of hacking collectively cost billions of dollars of damage.

Some definitions of cyber-crime are relatively narrow in focus. In some cases, only hacking behavior would fall under the definition of what constituted cyber-criminality. For example, the Council of Europe's Cybercrime Treaty makes reference to only those offenses that involve damage to data or to copyright and content infringements (see Sussman, 1999). However, most experts would agree that this definition is much too narrow and needs to take into account more traditional crimes, such as fraud and stalking, that make use of computers (Gordon and Ford, 2006; Zeviar-Geese, 1997-1998).

The legal definition of cyber-crime used in the United States takes a relatively broad view of the kinds of behavior constituting computer crime. The United States Code proscribes a range of conduct related to the use of computers in criminal behavior, including conduct relating to the obtaining and communicating of restricted information; the unauthorized accessing of information from financial institutions, the United States government, and "protected computers"; the unauthorized accessing of a government computer; fraud; the damaging of a protected computer resulting in certain types of specified harm; trafficking in passwords; and extortionate threats to cause damage to a "protected computer"

[1] "419" refers to Section 419 of the Nigerian Criminal Code. This is a variation on the classic "bait and hook" scheme, where the e-mail recipient is lured into providing personal information such as bank account numbers with the promise that they will be given a share of millions of dollars if they help the sender move funds out of the country.

(United States Code, Section 1030 of title 18). Taking into account the statutory provisions of the United States Code, the Federal Bureau of Investigation identifies a number of computer-related crimes that are part of their "cyber mission," including serious computer intrusions and the spread of malicious code, online sexual predation of minors and child pornography, the theft of U.S. intellectual property, breaches of national security, and organized criminal activity engaging in Internet fraud (Federal Bureau of Investigation, 2006).

Despite the specific identification of offenses, the legal definition of cyber crime tends to read like a grocery list and fails to anticipate future criminal variations in cyber offending.[2] In fact, another confounding issue in defining cyber-crime has to do with the constantly changing landscape for computer-related crime. As Gordon and Ford (2006) have noted, definitions of cyber crime have evolved experientially. As technology continues to expand and as offenders become more sophisticated in their criminality, new variations in computer crime are bound to emerge. Consequently, it may be better to try to define cyber-crime in categorical terms rather than with precision. For example, Broadhurst (2006, p. 413) constructed a typology of computer-related crime, which provides a more comprehensive framework for the scope of criminal activities involved in cyber- crime. He identifies six offense categories and the current kinds of cyber crime that tend to fall in these categories:

- *Interference with lawful use of a computer* – which includes such crimes as cyber-vandalism, cyber-terrorism, and the spread of viruses, worms and other forms of malicious code.
- *Dissemination of offensive materials* – which includes child pornography, other forms of pornographic material, racist/hate-group material, online gambling, and treasonous content.
- *Threatening communication* – which includes extortion and cyber-stalking.
- *Forgery and Counterfeiting* – which includes identity theft, phishing, IP offenses, various kinds of software and entertainment piracy, and copyright violations.[3]
- *Fraud* – which includes credit card fraud, e-funds transfer fraud, theft on internet or telephone services, online securities fraud, and other types of Internet fraud.
- *Other types of cyber-crime* – which includes interception of communications, commercial and corporate espionage, communications used in criminal

[2] This, in fact, should be expected, since the law is often reactive in nature – making provisions for new kinds of criminality only when criminal trends begin to occur.

[3] "Phishing" is generally defined as attempting to fraudulently acquire personal or other sensitive information, such as bank account numbers, passwords, or credit card information by masquerading as a trustworthy person or business in an electronic communication.

conspiracy, and electronic money laundering.

Gordon and Ford (2006) formulate an even more generic typology. Their typology includes any crime that is "facilitated or committed using a computer, network, or hardware device" (Gordon and Ford, 2006, p.14). They then categorize cyber-crime on a continuum. At one end of this continuum are offenses that tend to be discrete events, which are facilitated by crimeware programs (e.g., keystroke loggers, viruses, Trojan horses) and by the vulnerabilities of the system being exploited (identified as Type I offenses by Gordon and Ford). Examples of offenses at this end of the continuum would include hacking, phishing, and various forms of fraud. At the other end of the spectrum are offenses that involve repeated contact between the victim and offender, and which tend to use more common software (e.g., Instant Messaging, e-mail, FTP protocol) to facilitate the crime (Type II offenses). Offenses at this end of the spectrum would include cyberstalking, child predation, extortion, corporate espionage, and cyber-terrorism. The benefit of this particular typology is that it categorizes offenses according to their orientation toward either technology (the Type I offenses) or their orientation toward people (Type II offenses). Some offenses are going to be almost completely technological in nature, while others are going to be more traditional crimes that are facilitated by computers. This typology also allows for further expansion as new forms of computer-related crime emerge over time. For example, the linkage of more electronic devices through the Internet that will occur with the implementation of IP6 will increase the opportunities for the misappropriation of personal information. Similarly, the linkages of Onstar systems and cellular phones to the GPS make it possible to identify an individual's location for criminal, as well as legal, purposes.

The question remains, however, about whether cyber-crime is distinct from other forms of crime. On one hand, every current example of cyber-crime has an analogy in more traditional crime. Several examples illustrate this point. Hacking activities are, more or less, computer-aided versions of trespassing or vandalism. When a hacker enters a restricted computer system, he/she is entering another person's property without authorization—the definition of trespassing. Likewise, when a hacker purposely alters a website or destroys data, the action is analogous to vandalism. Various phishing schemes are essentially theft. Sexual predation, pornography, and credit card fraud are even more straight-forward, having obvious connections to their non-computer counterparts. To that end, an argument could be made that, at the present time, cyber-crime is essentially conventional criminal behavior that makes use of computers.[4] From this position, the

[4] In fact, Gordon and Ford (2006) argue that the term "cyber-crime" should be removed

impact of the computer on crime is not that it opened a Pandora's Box of criminal behaviors that previously had been impossible to perform.[5] The primary implication of computers, the Internet, and cyberspace for policing is how to adopt traditional and/or develop new enforcement strategies to existing criminal offenses that are completed or facilitated through a new channel or medium of communication. This line of argument is not intended to belittle the challenges of cyber-crime for the law enforcement community, however. The scope of changes in society that are occurring through the adoption of computers have not been seen since the invention of the automobile and airplane in the early-20th century revolutionized transportation. We believe that cyber-crime will be the primary challenge for policing in the 21st century.

On the other hand, any discussion of police futures pertaining to this topic has to consider what cyber-crime may look like in the coming years. While it is likely that the use of computers in the commission of crime will continue to expand in the near future, it is more difficult to envision a unique form of offending emerging that would fall into the categorization of cyber-crime. Nonetheless, the possibility of such an offense surfacing at some point in the future cannot be dismissed outright.

A final related issue that complicates the examination of cyber-crime has to do with the determination of its frequency of occurrence. To put it simply, it is extremely difficult to measure the extent of cyber-crime occurring in the United States. This is in large part due to the fact that when cyber-crime is recorded by authorities, it is not necessarily recorded as a computer-related offense. Rather, it is most often recorded as a case of fraud, pornography, or some other conventional crime. Consequently, the scope of cyber-crime, at least as far as official statistics are concerned, is masked by reporting and recording practices. Presently, the best data available on the question of the extent of cyber-crime are found in survey data, particularly the FBI's Cyber-Crime Survey. These data, however, can only give us an estimate of the scope of cyber-crime. The lack of substantial data on computer-related crime may be another argument against classifying cyber-crime as a unique form of criminality at the present time. Yet, it may also be a reason for more clearly defining, and thus being able

---

from our lexicon entirely, although they concede that it likely never will.

[5]The logical and obvious exception to this line of reasoning is the theft of computer hardware or software or of digital information, specific examples of theft that were impossible before the existence of the products.

to measure, cyber-crime. Therefore, it is important that we offer what will likely prove to be a temporally bounded definition of cyber-crime that can be useful for the present day. To this end, we define cyber-crime as "any criminal offense that is committed or facilitated through the use of the communication capabilities of computers and computer systems."

REFERENCES

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies and Management*, *29*, 408-433.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal of Computer Virology*, *2*, 13-20.

Newburger, E. C. (2001). *Home computers and internet use in the United States: August 2000* (Current Population Reports). Washington, DC: US Bureau of Census.

Sussman, M. A. (1999). The critical challenges from international high-tech and computer-related crime at the millennium. Duke Journal of Comparative and International Law, 9, 451-489.

Zeviar-Geese, G. (1998). The state of the law on cyberjurisdiction and cybercrime on the Internet. [Electronic version]. *Gonzaga Journal of International Law, 1.*