Encyclopedia of Law & Society: American and Global Perspectives

Cybercrime

Contributors: Yvonne Jewkes
Editors: David S. Clark
Book Title: Encyclopedia of Law & Society: American and Global Perspectives
Chapter Title: "Cybercrime"
Pub. Date: 2007
Access Date: December 08, 2014
Publishing Company: Sage Publications, Inc.
City: Thousand Oaks
Print ISBN: 9780761923879
Online ISBN: 9781412952637
DOI: http://dx.doi.org/10.4135/9781412952637.n165
Print pages: 386-388

http://dx.doi.org/10.4135/9781412952637.n165

Broadly speaking, one can classify cybercrimes in two categories. First, there are crimes that require a computer and cannot be committed in any other way or against any other type of victim. These also include crimes where the computer is the target of the offense, for example, unauthorized access to systems, tampering with programs and data, and planting viruses. Second, there are familiar or conventional crimes that are facilitated by computers and information and communication technologies (ICTs), such as "cyber" versions of identity theft, stalking, pedophile activities, or trading counterfeit goods. In some cases, criminal activities may encompass both categories. For example, acts of terrorism can involve qualitatively new offenses enabled by computer technologies or, alternatively, may integrate cyberspace into more traditional activities, such as planning, intelligence, logistics, and finance. Finally, there are several activities that are not strictly cybercrimes, insofar as they are not illegal, but they may cause what most people would consider harm to some users (such as certain forms of pornography, gambling, unsolicited e-mail, or unregulated sales of medicines and prescription drugs).

Newman and Clarke identified 26 crimes made possible by ICTs. They summarize the criminogenic attributes of cybercrimes in the acronym SCAREM: Stealth (cyberspace makes carrying out furtive crimes much easier), Challenge (an intellectual climate among hackers usually summed up as a desire to "beat" the system), Anonymity (an aspect of cyberspace that is obviously conducive to committing crime and not getting caught), Reconnaissance (the Internet provides a context in which informed criminals can plan their operations, survey all possible targets, and then act accordingly), Escape (in an environment where the identity and location of the offender are unknown and frequently unknowable, the opportunities for escape without leaving a trail of evidence are extremely high), and Multiplicity (hacking into valuable databases offers the opportunity to commit multiple crimes and create millions of victims simultaneously).

When it comes to the assessment of crime and crime control in cyberspace, there are essentially two diametrically opposed views. One is an upbeat—some would say, idealistic—view that the Internet is democratizing and the fact that control over content rests not with one, powerful interest group but potentially with each and every user makes the cyberenvironment a great social leveler, whereby we can all "police" each other. The other assessment of cybercrime is a negative response that ranges from doomand-gloom resignation to shrill warnings about apocalyptic meltdown. Inevitably, our reliance on ICTs in nearly every aspect of our public and private lives raises important concerns about security, trust, and control. In part, feelings of vulnerability may arise from the speed with which the personal computer (PC) became ubiquitous in everyday life in the 1980s and 1990s and the rate at which "new generation" technologies continue to be developed. Furthermore, the fear that hackers and virus writers are becoming less concerned with technical mastery for its own sake and are becoming explicitly criminal in intent may be a consequence of the more general anxiety concerning terrorist threats after the attacks on America on September 11, 2001.

Meanwhile, the average childhood experience has undergone major reorganization in advanced societies over the last half century, with children subjected to a greater degree of protective control and regulation **[p. 386 ↓]** than ever before. As young people's horizons of play become increasingly restricted to the immediate environs of the home and home computer, fears have multiplied about their potential exposure to pornographic material and to pedophiles posing as fellow children in order to "groom" their victims. The combination of these factors has resulted in high levels of global anxiety and numerous media-fueled scares concerning the problem of cybercrime, combining technological determinism with more generalized fears about the nature and prevalence of risk in the late-modern world.

The widespread notion that cyberspace is a playground for criminals is reinforced by pessimistic assessments of the effectiveness of law-and-order agents to control and combat it. The sheer size and scope of the Internet, the volume of electronic traffic it facilitates, the varying moral and legal responses to cybercrime in different countries, and other interjurisdictional difficulties, such as lack of cooperation or compatibility between police forces, combine to ensure that the police feel they remain in a perpetual game of "catch-up" with the criminally minded individuals who lurk in the shadowy corners of cyberspace. For example, organized criminals have been quick to exploit legal loopholes exposed within countries that have relatively relaxed attitudes to cybercrime. At the turn of the new millennium, Russia became a major source of child pornography because it had no specific laws governing the production or circulation of such material. Thus, while numerous criminal groups from other countries used Russian Internet sites to broadcast child pornography around the world, officials estimated that less than 1 percent of the content was actually produced in Russia. Online casinos have also proliferated on the Internet—unsurprisingly, since gambling is illegal in many jurisdictions.

Other factors result in a widening gap between the activities of online offenders and those who monitor and police them. These include underreporting of cybercrimes by victims (who, in many cases, may not be aware that they have been victimized); police culture, which tends to be conservative and technologyaverse; and limited resources—given that cybercrime is potentially as limitless as cyberspace itself, any funding strategy quickly starts to resemble a bottomless money pit. Nevertheless, a sense of perspective is required. Some discussion of cybercrime dwells on the possibilities of deliberate acts of sabotage that will disrupt a nation's water and electricity supplies, close all international communications, manipulate air traffic control or military systems, paralyze financial systems, and even result in cyberhomicide. However, most commentators believe that the likelihood of such calamitous events occurring through human or software error is far greater than the chance of malicious hackers or terrorists bringing down a country's infrastructure. For the time being, then, such grim forecasts remain the stuff of Hollywood writers' imaginations.

YvonneJewkes

http://dx.doi.org/10.4135/9781412952637.n165

See also

- Gambling
- Internet Law
- Mafia and Organized Crime
- Pornography
- Risk
- Sex Offenders
- Terrorism

Further Readings

Goodman, Marc D., and Susan W.Brenner. “The Emerging Consensus on Criminal Conduct in Cyberspace.” International Journal of Law & Information Technology 10 (2002). 139–223. http://dx.doi.org/10.1093/ijlit/10.2.139

Hamelink, Cees J. (2000). The Ethics of Cyberspace . London: Sage. http://dx.doi.org/10.4135/9781446219911

Jewkess, Yvonne, Ed. (2003). Dot.coms: Crime, Deviance, and Identity on the Internet . Cullompton, UK: Willan.

Jewkess, Yvonne, Ed. (2003). “Policing Cybercrime.” In Handbook of Policing , edited by Tim Newburn, ed. . Cullompton, UK: Willan, 501–24.

Jewkess, Yvonne, Ed. (2007). Crime Online . Cullompton, UK: Willan.

Newman, Graeme R., and Ronald V.Clarke. (2003). Superhighway Robbery: Preventing E-Commerce Crime . Cullompton, UK: Willan.