Introduction

There is no single, conclusive definition of the term "cybercrime"; however, it has become an umbrella term that refers to a wide range of offenses and behaviors. Other terms that are also used are computer crime, computer-related crime, virtual crime, digital crime, e-crime, high-tech crime, electronic crime, cyber-enabled crime, or even online offending. In general, it refers to any criminal offenses that are committed or aided by use of the internet. It is difficult to provide an exact definition of cybercrime because it is always changing and evolving as technology advances and becomes more sophisticated.

Some define cybercrime as any crime that involves a computer or a network. Sometimes the computers are used to commit the crime, but other times they are the target of the crime. According to the U.S. Department of Justice, the term "cybercrime" refers to any illegal activity for which a computer is used as its primary means of commission, transmission, or storage.

Some definitions of the term make a distinction between cybercrime and computer crimes. Those who make this difference describe cybercrime as those offenses in which the offender obtains special of cyberspace and relies on that knowledge to carry out a criminal offense. This would happen, for example, if a person hacked into another person's account and accessed private photos of them and then uploaded the photos to social media. On the other hand, computer crimes can be thought of as those times when an offender uses special knowledge about computer technology to commit a crime. An example is when a person uses a computer to download confidential information onto a zip drive and removes it from that source. They are using a computer to commit a crime—but not the internet. In short, one offender relies on the larger concept of cyberspace whereas the other relies on the more hands-on offenses committed by the use of tangible items (software or computer equipment) (Holt, Burruss, and Bossler, 2015, p. 7).

There are other distinctive definitions of specific cybercrimes. One of those is a computer-assisted crime, such as child pornography. Here, the offender uses the computer to commit the crime. They will use the computer to create the illegal material (virtual pornography) and then to distribute it. A computer-focused offense is one in which the computer is an essential part of the offense, such as hacking into an account. This offense could not be carried out without the computer.

Wall (2001) recognizes four categories of cybercrime. The first is cybertrespass, which he defines as those times when an offender crosses the undefined or invisible but often recognized lines of ownership in an online environment. This occurs when hackers steal passwords and obtain access to resources for their own

benefit. They have used the online environment (the internet) to steal something that belongs to another person. The second category includes cyberdeception and cybertheft. This involves the use of computers to steal money from bank accounts or to illegally access intellectual property or copyrighted material (music, movies, books, software) from another person. This is also referred to as piracy. Cyberdeception occurs through phishing, when a cybercriminal sends a sham e-mail to a victim asking for bank account information. Because the e-mail appears to be real, the victim provides the information. The stolen information can be used by the offender to steal money, or it can be sold to other offenders.

The third category of cybercrime, according to Wall, is cyberpornography and obscenity. Internet and computer technology allow pedophiles to create and trade graphic pictures or meet victims. The final category of cybercrime is cyberviolence, which is hurtful or dangerous behavior committed online. Computers give offenders the ability to create and distribute threatening and hurtful information about others. Examples of these offenses include cyberharassment, cyberstalking, and cyberbullying.

It is difficult to list all of the cybercrimes that exist, as there are many different kinds of cybercrimes. Many cybercrimes were considered to be criminal offenses prior to the evolution of the internet (e.g., bullying, child pornography, or theft) but have evolved into a cybercrime; others are new offenses that did not exist before (e.g., hacking or sexting). Below is a partial list of offenses that are often committed in cyberspace or by use of a computer.

(a) Ransomware: Malware used by offenders to lock digital files of another person or company until money or other form of ransom is paid to the offender.
(b) Phishing: A way for criminals to obtain private information from a victim by sending an e-mail that appears to be from a legitimate organization. The e-mail often uses letterhead from the agency or a logo from the company to make it look real. The message indicates that an account or password needs to be updated. The victim is tricked into providing that information to the offender, who then uses it to steal the victim's money or sells the information to another offender.
(c) Identity theft: A criminal obtains a victim's personal information (possibly through phishing) and uses that to commit theft or fraud offenses, open fake credit card accounts, or get bank loans. They use a victim's name, birthday, social security number, driver's license number, or passport information. A victim of identity theft can suffer extreme and long-lasting financial harm. This offense is not punishable under the federal Identity Theft and Assumption Deterrence Act of 1998, which "makes it a federal offense to possess, transfer or use a means of identification of another person without authorization with the intent to commit or aid in the commission of illegal activity at the local, state or federal level."
(d) Online child predators (child pornography): This offense has been defined as "the sexual or sexualized physical abuse of children under 16 years of age or who appear to be less than 16 that would offend a reasonable

adult" (Krone, 2004, p. 1). Images of child pornography show children participating in sexual acts. Children who are forced into participating in the acts suffer trauma and are often permanently injured, both physically and emotionally. The production and consumption of child pornography are both illegal acts, regardless of whether the computer is involved. The internet allows people to access child pornography for free, but there are multiple sites on the dark web that make these images readily available. It is estimated that there are 20,000 images of child pornography added to the internet each week (Pittaro, 2008). Because of the sheer amount of child pornography available on the internet, law enforcement has a difficult time tracking users. It is easy for offenders to skirt the law and get away with this offense.

(e) Viruses: A form of malware, viruses are computer programs that a user unknowingly uploads onto their computer when they open an infected e-mail or attachment, or when they visit a particular website. The virus is uploaded onto the computer, giving the offender access to the files on that machine. The virus allows the offender to steal data, destroy data, or access personal information. It will then replicate itself onto other computers through e-mails.

(f) Denial-of-service attacks (DoS attacks): These attacks are carried out by cybercriminals who block or prevent a legitimate user from using a website. Offenders are able to flood a computer network with enough traffic that the site crashes, shutting it down to other users. This type of attack can result in significant losses to the company as they must spend time and resources to get their site working once again. A similar attack is a distributed denial-of-service attack (DDoS) that occurs when a site is overwhelmed by botnets (a group of infected computers and networks) that overwhelm a targeted website with requests and render the site or servers unavailable to users.

(g) Malware: This term is a combination of the words "malicious" and "software." It refers to any software that has the intent of harming networks or devices or giving an offender unauthorized access to computers or networks belonging to another person or organization. It is usually uploaded onto a victim's computer or network without their knowledge and may remain there for an extended time. Types of malware include viruses, spyware, worms, ransomware, adware, and Trojan horses.

(h) Cyberbullying: This occurs when a person harasses or teases another person, usually a teenager, through social media. It can be relentless and extremely harmful, and it has led some victims to commit suicide. When this behavior is directed toward an adult, it is called cyberharassment.

(i) Cyberterrorism: According to the FBI, cyberterrorism involves crimes of terrorism that occur electronically or through the use of the internet. They can be directed against individuals, businesses, agencies, and the government. It can be acts on the internet that are meant to threaten or extort others, often politically motivated. If an attack is carried out, it can cause disruption of services that may be harmful or even cause death.

(j) Hacking: Illegally breaching security or gaining access to a computer system by an offender who is called a hacker. Some hackers intend to do harm, either by stealing money or information, whereas others hack into a system as a way to uncover unknown weaknesses or vulnerabilities in software.
(k) Piracy: The unauthorized copy and distribution of movies, music, or other copyrighted property without permission of the owner or creator. This can happen when a person downloads a program, video game, or a song without paying for it.
(l) Spyware: A type of malware that can be secretly installed in a victim's computer to allow an offender to steal a victim's information. An offender is able to steal passwords, e-mails, and credit card information without the victim knowing.
(m) Nigerian e-mail schemes: These are also known as advance fee e-mail schemes. Here, the victim receives an e-mail pleading for money to be sent somewhere, with promises that more money will be provided in the future. They often appear to be from an official or member of royalty who needs help to leave their country. The offender will request the bank account number where the promised money can be sent. The scams often originate in Nigeria but are also called 419 scams after the Nigerian statute that bans this kind of communication.
(n) Work-at-home schemes: These often involve job solicitations where the victim is given the chance to work at home completing menial tasks (stuffing envelopes) and earn a significant income for only a few hours of work each day. The victim is required to pay up-front for training materials or supplies, but materials are never sent.
(o) Romance schemes: A victim meets their perfect romantic partner through an online dating site. The offender will ask for money to travel and meet their new soul mate, to pay get out of legal trouble, or to pay off debts. They may initially ask for a small amount, but then it increases over time. Victims have paid tens of thousands of dollars before realizing their new mate doesn't exist.

However you define it, cybercrime costs billions of dollars to companies, governments, and individuals in financial losses of information and trade secrets. Losses are also due to repairs to systems that are damaged or harmed as the result of a cyberattack. Individuals, governments, and agencies must also spend billions in prevention of a possible attack.

Cybercrime poses a threat to our country's national security and infrastructure. Other governments and terrorist organizations have threatened to attack the infrastructure of the United States (power grids and financial institutions). The U.S. government spends billions of dollars each year to thwart possible attacks on its agencies, as well as to keep citizens safe. It is an ongoing process that must evolve as threats evolve.

Cybercrime is difficult to combat for many reasons. One is that cybercriminals do not respect physical boundaries. The internet is a global phenomenon that

crosses borders, and so is cybercrime. This makes it difficult for law enforcement to track. It is difficult to know who the offender is or where that person is physically located. Investigating cybercrime requires offices to have knowledge of technical forensic methods, which few do. To effectively battle cybercriminals, there must be cooperation on an international level. Interpol currently helps to fight cybercrime, but more needs to be done. Because it is so tough to track, there is a relatively low risk of detection and prosecution to offenders.

In the United States, the Federal Bureau of Investigation (FBI) is the primary federal agency that has the responsibility to investigate any threat of, or actual events of, cybercrime. They have a cyber division that coordinates the nation's attack on cybercrime. Each field office has a cyber squad comprising specially trained agents who work to protect against crimes and also to react to attacks. The FBI has formed cyber action teams that respond worldwide to an attack to gather intelligence and work to identify the crime and criminals. The FBI has created 93 computer crimes task forces that work with state and local experts in the fight against cybercrime. They also partner with other federal agencies, including the Department of Defense, Department of Homeland Security, and others. The FBI's Internet Crime Complaint Center gives the public a way to report acts of cybercrime.

Cybercrimes such as these are often committed by criminals who are seeking to profit from their crimes. They hack into an account to get money, or use ransomware for the same reason. Cybercrimes are committed by terrorists who are seeking to intimidate others, or even to profit from their crimes. Hackers sometimes commit cybercrimes just for the challenge, or to see if they can break into a system. The internet gives offenders the chance to harm many people at one time, something that might not be possible without using a computer. There is a large pool of victims available to the offender. It is also an inexpensive way to commit a crime. In some cases, all it takes to scam a victim is to send an e-mail. There is a large amount of malware that offenders can purchase that allows them to carry out an attack even though they have no expertise in writing software.

Cybercrimes are growing as more people have access to computers and rely on them for daily tasks such as shopping, banking, and communicating with each other. The true range of cybercrime is unknown, as many people do not report when they have been a victim, or they may not even know that they have been attacked. Businesses may not want to make it known to their customers that they have been the victim of a cybercrime and risk harming their reputation. Threats to mobile devices are also on the rise as people use them as computers, keeping personal information, contacts and calendars on them. Both individuals and companies need to become more aware of how to protect themselves from cybercrime. It can be as simple as purchasing programs that will protect against viruses and malware—or using passwords that are difficult to hack. Teaching employees and individuals to recognize fake e-mails is also critical, so they do not fall prey to cybercriminals who only want to have access to bank accounts.

Nancy E. Marion

Further Reading

Clough, Jonathan. 2015. *Principles of cybercrime*. Cambridge, UK: Cambridge University Press.

Federal Bureau of Investigation, Internet Crime Complaint Center (IC3). https://www.ic3.gov

Finch, Emily. 2007. "The problem of stolen identity and the internet." In *Crime online*, edited by Yvonne Jewkes. Devon, UK: Willan Publishing, pp. 29–43.

Gillespie, Alisdair A. 2016. *Cybercrime: Key issues and debates*. New York: Routledge.

Holt, Thomas J., George W. Burruss, and Adam M. Bossler. 2015. *Policing cybercrime and cyberterror*. Durham, NC: Carolina Academic Press.

Hutchings, Alice, and Yi Ting Chua. 2017. "Gendering cybercrime." In *Cybercrime through an interdisciplinary lens*, edited by Thomas J. Holt. New York: Routledge, pp. 167–188.

Krone, T. 2004. "A typology and online child pornography offending." *Trends and Issues in Crime and Criminal Justice* 279: 2–6.

Lininger, Rachael, and Russell Dean Vines. 2005. *Phishing*. Indianapolis, IN: Wiley Publishing.

Pittaro, M. 2008. "Sexual addiction to the internet: From curiosity to compulsive behavior." In *Crimes of the internet*, edited by F. Schmalleger and M. Pittaro. Upper Saddle River, NJ: Pearson Education, Inc., pp. 134–150.

Wall, D. S. 2001. "Cybercrimes and the internet." In *Crime and the internet*, edited by D. S. Wall. New York: Routledge, pp. 1–17.