Thomas J. Holt and Karen M. Holt

17 Cybercrime

Abstract: This chapter provides an overview of the issue of cybercrime, or the use of the Internet and computer technology in order to offend. The definitional challenges associated with cybercrime are discussed, along with the various behaviors that have come to be defined as cybercrimes by criminologists.

Keywords: cybercrime, technology, online, Internet

Computers, mobile phones and the internet have revolutionized modern life. More than half of the world's population use the internet (Internet World Stats, 2020), and a majority of the populations of Western nations are accessing and utilizing this technology. This has transformed communication and relationships. Many now prefer to communicate via text message rather than voice phone calls (Zickuhr, 2011). Social media applications are now a critical resource for both personal communications and commerce (Perrin and Anderson, 2019). In addition, virtually all aspects of personal and business transactions are supported by the internet.

The benefits of technology are offset by the overwhelming opportunities they present for criminals who seek access to people, money, and digital information stored online (Holt and Bossler, 2015; Maimon and Louderbach, 2019). Computers and the internet have enabled and simplified traditional forms of crime, like acts of fraud (Button and Cross, 2017), stalking, and sexual offenses (Holt and Bossler, 2015). Technology has also created new forms of offending that are dependent on computers, such as hacking where individuals attempt to access computer networks without permission (see Hacking by Wall) (Steinmetz, 2016).

While much of the extant criminological literature has focused on the nature and qualities of online offenses, there is also an argument to be made that there has been an increase in the ability of the state and commercial institutions to centralize power and surveillance, which can cause more harm than online crimes themselves (Steinmetz, 2023; 4). The surveillance capabilities of the state have far-reaching implications, notably related to invasions of privacy, censorship, restriction of the internet, and the classification of citizens based on tracking their online movements. Thus, a critical approach to understanding cybercrime must examine not only the ways in which individuals can use technology for harm, but also how regimes can employ surveillance and use this technology under the guise of crime control (see Surveillance by Lyon).

Over the last two decades, criminologists have increasingly focused attention on the range of behaviors enabled by technology, which are commonly referred to as cybercrime (Leukfeldt and Holt, 2019; Payne and Hadzhidimova, 2020). Cybercrime is treated as an umbrella term which includes all offenses either occurring in or being wholly facilitated by an online environment. Thus, offenses occurring in physical spaces and involving minimal technological assistance would fall outside of the

 https://doi.org/10.1515/9783111062037-018

scope of cybercrime. Here we will explore the meaning of this term, and the ways in which it has been operationalized by scholars over time. The range of behaviors that constitute cybercrimes will also be reviewed to provide a better appreciation for the scope of crimes occurring online.

Defining cybercrime

The current popularity and consistency in the use of the term cybercrime belies decades of debate among criminologists. In fact, some of the first pieces examining the misuse of technology in criminology can be found in the late 1980s, and used the term computer crime to reference the fact that a computer was involved to facilitate fraud at a Florida dog racing track (Hollinger and Lanza-Kaduce, 1988). At the time, the notion of the internet and cyberspace as we currently understand it was in its infancy.

As the World Wide Web became dominant in the 1990s and technology access flattened, criminologists began to consider the ways that the online environment may enable individuals to share information on offending that could be used on and offline (Mann and Sutton, 1998). David Wall (1998) argued that the growth of technology and online spaces created a phenomenon whereby not only were new offenses possible, but the environment in which they could occur did also not exist otherwise. For instance, the global access afforded by the internet makes it possible for offenders to identify victims in other countries with ease (Holt and Bossler 2015). Furthermore, computers act as a force multiplier for offenders, allowing them to affect hundreds of victims at the same time in ways that are not possible in physical space (Wall, 1998).

By contrast, Peter Grabosky (2001) argued that technology-enabled offenses were simply "old wine in new bottles," meaning they were traditional forms of crime occurring in a novel space using new tools. For instance, acts of fraud and theft could be performed in off-line spaces, though technology made it easier to do so online (Grabosky, 2001). The internet did not eliminate traditional forms of offending, it simply created an alternative environment in which they could occur.

These contrasting arguments also led to debate over the use of the terms cybercrime and computer crime. Though they were treated as synonymous during this period, they differed as to the function of technology in the course of the offense (Furnell, 2002; Wall, 2001). Computer crimes were thought to involve special use of computer technology in order to offend, while cybercrimes involved special knowledge of cyberspace (Furnell, 2002). This segmentation eventually disappeared in the mid-2010s, with the term cybercrime becoming dominant (Holt and Bossler, 2015). The use of cybercrime is particularly appropriate now, as virtually any and all devices are connected to the internet, including so-called Internet of Things devices like thermostats, home appliances, and even vehicles (Steinmetz and Yar, 2019).

Though cybercrime is now the dominant term, there are still some points of differentiation used by scholars, governments, and policy agencies. For example, academics

have critiqued the utility of the term cybercrime and presented alternatives to identify the unique nature of technological influences on behavior. McGuire (2007) argued for the use of the term hypercrime as a way to recognize that offenses occur as a result of the interconnected nature of virtual and real spaces which mirrors the World Wide Web itself. Others have argued in favor of terms like ecrime, technocrime, and informated crime as a means to avoid the unclear nature of what constitutes cyber in practice (see Steinmetz, 2023 for discussion). In fact, Cross (2019) argued we should abandon the term cyber when referring to all technology-facilitated fraud schemes, and simply note them as frauds as it otherwise limits the allocation of resources to properly combat these offenses.

The terms cyber-dependent and cyber-enabled crimes are used by some policymakers in the UK, Europe, and Australia as a means to identify how the offense occurs (Holt and Bossler, 2015; McGuire and Dowling, 2013). Cyber-dependent crimes are those that require a computer or technology in order to occur, such as the distribution of malicious software that affects the operations of computer hardware and software (McGuire and Dowling, 2013). Cyber-enabled crimes are those that are simplified by the use of computers and the internet, such as fraud and identity-based crimes (McGuire and Dowling, 2013). The use of cyber-dependent and cyber-enabled crimes have not been popularized or used consistently across place, making their overall utility limited.

Forms of cybercrime

While cybercrime in an incredibly important term in criminology, it should be noted that it is an umbrella term encompassing a wide range of offenses. There are various typologies of cybercrime proposed by researchers, though their acceptance is generally inconsistent (see Holt and Bossler, 2015 for review). One of the only typologies that gained acceptance in the field was created by David Wall (2001), which recognized four categories of offenses: 1) cyber-trespass; 2) cyber-deception and theft; 3) cyber-porn and obscenity; and 4) cyber-violence.

Acts of cyber-trespass are those that involve crossing boundaries of ownership in online spaces. For instance, a password-protected WiFi hotspot is effectively establishing a boundary of access, where only those with the password are allowed to use the connection (Holt and Bossler, 2015). Individuals who attempt to access these networks by guessing the password or using tools to break that password without authorization from the owner are effectively engaging in acts of trespass. Cyber-trespass activities are most often associated with computer hackers, as they often attempt to gain access to networks, email accounts, and other protected systems without permission (Jordan and Taylor, 1998; Steinmetz, 2016). Though not all hackers engage in such illegal activities, those who perform such acts cause significant financial harm to individuals, as well as public and private entities around the world (Holt and Bossler, 2015).

The second category involves acts of cyber-deception and theft which is complex and overlaps with acts of cyber-trespass (Wall, 2001). The term deception is used as criminals can readily misrepresent their identity while online through the use of fake names, email accounts, and stolen legitimate user credentials to access sensitive (Button and Cross, 2017; Leukfeldt et al., 2017). For example, hackers can utilize various methods to gain access to protected networks in order to obtain sensitive personally identifiable information and financial data (Hutchings and Holt, 2015; Leukfeldt et al., 2017; Roks et al., 2021). Actors then sell this information to others in online black markets in order to engage in fraudulent financial transactions, such as purchasing goods and services without the account holder's permission (Hutchings and Holt, 2015).

This category also includes independent acts of fraud that are enabled by email, social media, text messaging, and other forms of computer-mediated communication. For instance, there has been substantive criminological focus on the problem of romance scams, where offenders create false profiles on social media and dating applications and message potential targets in the hopes of generating a response (Button and Cross, 2017; Whitty, 2013). Once in contact, the offender then tries to develop an emotional and romantic rapport with the victim by asking personal questions and noting their love and attraction to them. As the relationship intensifies, the offender often asks the victim for financial support to travel to see them, or claim they have experienced a financial hardship that they cannot work through (Button and Cross, 2017). Such financial requests continue until such time as the victim ceases to support their requests. Victims of romance frauds frequently report intense emotional and psychological consequences as a result of their experiences with fraudsters (Button and Cross, 2017).

The act of illegally copying, sharing and/or obtaining digital media files, including computer software, audio, video, and e-books, without the permission of the copyright holder is also included in this category (Gopal et al., 2004). Digital piracy can be performed in a variety of ways, such as file sharing services, and is extremely common globally (Brown, 2016; Brown and Holt, 2018 for review). In fact, evidence suggests that most young people have engaged in piracy and easily justify their activities on the basis of the lack of harm caused to copyright holders and the costs associated with the legitimate purchase of media (Brown and Holt, 2018; Ingram and Hindjua, 2008).

The third category in Wall's (2001) typology of cybercrime involves cyber-porn and obscenity, reflecting a wide variety of sexual expression in online spaces. Sexually explicit content featuring adults, commonly defined as pornography, is readily available online and has become a major industry (Lane, 2000; Quinn and Forsyth, 2013). Such content can be produced with great ease due to the availability of high definition digital cameras, high-speed internet connectivity, and editing software. The consumption of adult sexual content is generally defined as legal in most nations, though it may be considered socially unacceptable depending on local mores (Quinn and Forsyth, 2013).

Technology has also transformed the nature of sex work in general (see Sex Work by Rand). The rise of social media and subscription-based media channels like Patreon

and OnlyFans has also allowed individuals to produce sexual content for a fee (Moloney, 2019; Rana, 2020). Similarly, sex workers utilize the internet to advertise sexual services that take place in offline settings, which may be illegal depending on the laws within a given country (Campbell et al., 2019). Their customers frequently use web forums and various online platforms as a tool to discuss their experiences, identify specific providers, and warn others about police and other efforts to curb sex work (Sanders et al., 2018).

The ease with which individuals can produce sexualized images and content has also led to individuals sending images of themselves to prospective or current romantic partners via direct text message or email. This practice has become colloquially known as sexting, and is popular as it is perceived as a somewhat secure method for sharing content to attract or stimulate a partner (Henry and Powell, 2018). Sexual content is not, however, secure, as the recipient can now readily share sexted images and video with others via text or social media, or on websites designed to embarrass or harass the sender (Henry and Powell, 2018). Such activities constitute revenge porn, and may be performed after a relationship ends, or by individuals who hack individual accounts to obtain access to their content (Henry and Powell, 2018).

This category also includes the sharing of child sexual abuse materials (CSAM), or images, video, and other media featuring images of people under the age of 18 engaging in sexualized acts (Eke and Seto, 2023). The distribution of CSAM is a global problem, and has been criminalized in virtually all nations. This content is shared on virtually all platforms online, which makes it exceedingly difficult for police to disrupt (Seto et al., 2018). In addition, some use the internet, particularly social media, as a means to connect with children in order to groom them into offline relationships, or to generate CSAM themselves (Eke and Seto, 2023).

The final category of Wall's (2001) typology of cybercrime encompasses acts of cyber-violence, recognizing the potential of the internet to allow individuals to engage in harmful behavior to others through online spaces. The most common behaviors included involve the use of social media, email, text, and other forms of online communication to bully, harass, threaten, or stalk others online (Vogels, 2021). The severity and frequency of messages an individual receives can lead victims to experience emotional harm, including embarrassment, shame, and may even lead some to physical harm through suicidal ideation (Wilson et al., 2022).

In addition, terrorists and extremist groups also use the internet as a means to recruit others into their movement, and promote their beliefs publicly and privately (Herath and Whittaker, 2021). The expression of hate speech and violence toward minoritized groups in society has become commonplace, particularly on social media (see Hate Crime and Networked Hate by Powell, Stratton, and Cameron). Actors also utilize various technologies as a means to coordinate and plan acts of offline violence (Hamm and Spaaij, 2017).

Furthermore, some extremist groups use the internet as a means to engage in cyberattacks against individuals, governments, and businesses. There is evidence that actors associated with animal and earth liberation groups have performed various cyber-

attacks over the last decade (Holt et al., 2021). Similarly, the hacker group Anonymous used DDoS attacks in order to stage protests against government, industry, and civilian targets (Olson, 2013). This has led some scholars to use the term hactivism to refer to cyberattack activities that may be deemed an act of protest or dissent by the actors (see Holt and Bossler, 2015) Thus, the use of technology has expanded the capability of extremist groups to affect populations and targets well beyond their overall capacity in offline environments.

Conclusion

Taken as a whole, cybercrime as a term reflects a wide range of offenses which differ in the degree to which they are facilitated by technology and impact people or computers and data. These differences highlight the inherent weaknesses of the use of the phrase, as virtually any act of crime or delinquency with some connection to computers and the internet could be classified as cybercrime. Though other ways of defining such offenses have been proposed, few have been able to supplant the socially accepted nature of the phrase (Steinmetz, 2023). It is possible that the concept of 'cyber' will become outmoded with continued technological advancements, which may enable the abandonment of the term in favor of the more realist approach of treating these offenses simply as crimes (Cross, 2019).

Suggested reading

Holt, T. J., & Bossler, A. M. (2015). *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses.* London: Routledge.

Holt, T. J., & Lavorgna, A. (eds.) (2021). *Researching Cybercrimes: Methodologies, Ethics, and Critical Approaches.* Springer Nature.

Lusthaus, J. (2018). *Industry of Anonymity: Inside the Business of Cybercrime.* Cambridge, MA: Harvard University Press.

Steinmetz, K. F., & Yar, M. (2019). *Cybercrime and Society.* London: Sage.

Wall, D. (2007). *Cybercrime: The Transformation of Crime in the Information Age* (Vol. 4). Cambridge: Polity.

References

Brown, S. C. (2016). Where do beliefs about music piracy come from and how are they shared? An ethnographic study. *International Journal of Cyber Criminology*, 10(1), 21 – 39.

Brown, S. C., & Holt, T. J. (eds.) (2018). *Digital Piracy.* London: Routledge.

Button, M., & Cross, C. (2017). *Cyber Frauds, Scams and Their Victims.* London: Routledge.

Campbell, R., Sanders, T., Scoular, J., Pitcher, J., & Cunningham, S. (2019). Risking safety and rights: online sex work, crimes and 'blended safety repertoires'. *The British Journal of Sociology*, 70(4), 1539 – 1560.

Cross, C. (2019). Is online fraud just fraud? Examining the efficacy of the digital divide. *Journal of Criminological Research, Policy and Practice*, 5(2), 120 – 131.

Eke, A. W., & Seto, M. C. (2023). Correspondence of child age and gender distribution in child sexual exploitation material and other child content with age and gender of child sexual assault victims. *Sexual Abuse*, 35(3), 375 – 397.

Furnell, S. (2002). *Cybercrime: Vandalizing the Information Society.* London: Addison-Wesley.

Gopal, R. D., Sanders, G. L., Bhattacharjee, S., Agrawal, M., & Wagner, S. C. (2004). A behavioral model of digital music piracy. *Journal of Organizational Computing and Electronic Commerce*, 14(2), 89 – 105.

Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies*, 10(2), 243 – 249.

Hamm, M. S., & Spaaij, R. (2017). *The Age of Lone Wolf Terrorism.* New York: Columbia University Press.

Herath, C., & Whittaker, J. (2021). Online radicalisation: Moving beyond a simple dichotomy. *Terrorism and Political Violence*, 35(5), 1 – 22.

Henry, N., & Powell, A. (2018). Technology-facilitated sexual violence: A literature review of empirical research. *Trauma, Violence, & Abuse*, 19(2), 195 – 208.

Hollinger, R. C., & Lanza-Kaduce, L. (1988). The process of criminalization: The case of computer crime laws. *Criminology*, 26(1), 101 – 126.

Holt, T. J., & Bossler, A. M. (2015). *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses.* London: Routledge.

Holt, T. J., Stonhouse, M., Freilich, J., & Chermak, S. M. (2021). Examining ideologically motivated cyberattacks performed by far-left groups. *Terrorism and Political Violence*, 33(3), 527 – 548.

Hutchings, A., & Holt, T. J. (2015). A crime script analysis of the online stolen data market. *British Journal of Criminology*, 55(3), 596 – 614.

Ingram, J. R., & Hinduja, S. (2008). Neutralizing music piracy: An empirical examination. *Deviant Behavior*, 29(4), 334 – 366.

Internet World Stats. (2023). Internet usage statistics. https://www.internetworldstats.com/stats.htm

Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review*, 46(4), 757 – 780.

Lane, F. S. (2001). *Obscene Profits: Entrepreneurs of Pornography in the Cyber Age.* London: Routledge.

Leukfeldt, R., & Holt, T. J. (eds.) (2019). *The Human Factor of Cybercrime.* London: Routledge.

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017). Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. *The British Journal of Criminology*, 57(3), 704 – 722.

McGuire, M. (2007). *Hypercrime: The New Geometry of Harm.* Abingdon and New York: Routledge-Cavendish.

McGuire, M., & Dowling, S. (2013). *Cyber Crime: A Review of the Evidence. Summary of Key Findings and Implications.* Home Office Research Report, 75, 1 – 35.

Maimon, D., & Louderback, E. R. (2019). Cyber-dependent crimes: An interdisciplinary review. *Annual Review of Criminology*, 2, 191 – 216.

Mann, D., & Sutton, M. (1998). NETCRIME: More change in the organization of thieving. *The British Journal of Criminology*, 38(2), 201 – 229.

Moloney, A. (2019). What are premium Snapchat accounts and are they just porn? *Metro*, February 21, 2019. https://metro.co.uk/2017/11/21/what-are-premium-snapchat-accounts-7088201/

Olson, P. (2013). *We Are Anonymous.* London: Random House.

Payne, B. K., and Hadzhidimova, L. (2020). Disciplinary and interdisciplinary trends in cybercrime research: An examination. *International Journal of Cyber Criminology*, 14(1), 81 – 105.

Perrin, A., & Anderson, M. (2019). *Share of U.S. adults using social media, including Facebook, is mostly unchanged since 2018.* Pew Charitable Trust. [Online] Available at https://www.pewresearch.org/fact-tank/2019/04/10/share-of-u-s-adults-using-social-media-including-facebook-is-mostly-unchanged-since-2018/

Quinn, J. F., & Forsyth, C. J. (2013). Red light districts on blue screens: A typology for understanding the evolution of deviant communities on the internet. *Deviant Behavior*, 34(7), 579 – 585.

Rana, P. (2020). Top 10 celebrity OnlyFans accounts: Cardi B and Bella Thorne to Tyga, here's all the steamy footage you need. *Meaww*, October 20, 2020. https://meaww.com/cardi-b-bella-thorne-tyga-shea-coulee-top-10-accounts-adult-site-only-fans-subscribe-what-they-post

Roks, R. A., Leukfeldt, E. R., & Densley, J. A. (2021). The hybridization of street offending in the Netherlands. *The British Journal of Criminology*, 61(4), 926 – 945.

Sanders, T., Scoular, J., Campbell, R., Pitcher, J., & Cunningham, S. (2018). *Internet Sex Work: Beyond the Gaze.* Cham: Springer International Publishing.

Seto, M. C., Buckman, C., Dwyer, R. G., & Quayle, E. (2018). *Production and Active Trading of Child Sexual Exploitation Images Depicting Identified Victims.* National Center for Missing and Exploited Children. https://calio.dspacedirect.org/handle/11212/4669

Steinmetz, K. F. (2016). *Hacked: A Radical Approach to Hacker Culture and Crime* (Vol. 2). New York: NYU Press.

Steinmetz, K. F., (2023). *Against Cybercrime: Toward a Realist Criminology of Computer Crime.* London: Routledge.

Steinmetz, K. F., & Yar, M. (2019). *Cybercrime and Society.* London: Sage.

Vogels, E. A. (2021). *The State of Online Harassment.* Pew Research Center. https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2021/01/PI_2021.01.13_Online-Harassment_FINAL-1.pdf

Wall, D. S. (1998). Catching cybercriminals: Policing the internet. *International Review of Law, Computers & Technology*, 12(2), 201 – 218.

Wall, D. S. (2001). Cybercrimes and the internet. In D. S. Wall (ed.), *Crime and the Internet* (pp. 1 – 17). London: Routledge.

Whitty, M. T. (2013). The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam. *British Journal of Criminology*, 53(4), 665 – 684.

Wilson, C., Sheridan, L., & Garratt-Reed, D. (2022). Examining cyberstalking perpetration and victimization: A scoping review. *Trauma, Violence, & Abuse*, 24(3), 2019 – 2033.

Zickuhr, K. (2011). *Generations Online in 2010.* Pew Internet and American Life Project. Available at: www.pewinternet.org/Reports/2010/Generations-2010/Overview.aspx