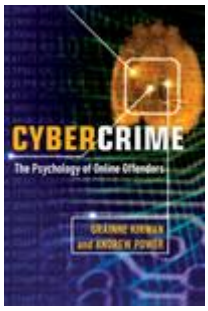
PsycCRITIQUES
June 2, 2014, Vol. 59, No. 22, Article 6



Theorizing the Motives of Cybercriminals

A Review of

Cybercrime: The Psychology of Online Offenders
by Gráinne Kirwan and Andrew Power
New York, NY: Cambridge University Press, 2013. 256 pp. ISBN 978-1-107-00444-3 (hardcover); ISBN 978-0-521-18021-4 (paperback). $95.00, hardcover; $38.99, paperback

http://dx.doi.org/10.1037/a0036522

Reviewed by

Thomas J. Holt

Much has been made in popular media about the threat posed by cybercrimes and the potential for cyberterrorism. There has been a substantial increase in the body of social science research pertaining to various forms of cybercrime over the last two decades, much of it focusing on digital piracy and harassment. Less research has considered the factors associated with computer hacking, malware creation, and identity crimes, although this is beginning to change. There has also been a substantive expansion in the number of universities offering courses or specializations in cybercrime within social science units. This has caused an increase in the number of cybercrime-related textbooks available on the market, ranging from technically oriented works on digital forensics to more descriptive textbooks on the range of offenses enabled by the Internet.

Cybercrime: The Psychology of Online Offenders by Gráinne Kirwan and Andrew Power falls squarely on the side of more general and introductory texts. In defining the scope of cybercrimes, the authors do not use existing or well-established definitions or typologies. Instead, they suggest that cybercrime is a form of crime that can be separated into property crimes, like identity theft, or crimes against persons, such as sexual abuse of children. They also use their own typology of Internet-specific and Internet-enabled crime and crime in virtual worlds to account for cybercrimes (Power & Kirwan, 2011) rather than more cited or recognized frames such as those proposed by Furnell (2002) or Wall's (2001) four-category framework. They identify Internet-enabled crimes as those that can also occur in the real world (e.g., piracy), whereas Internet-specific crimes (e.g., malicious software distribution) cannot exist off-line. Their contribution stands out through the introduction of crimes in virtual worlds, where nonhuman characters and representations of people engage in offenses that would otherwise be dictated as crimes in the real world. Although this perspective is useful, the lack of clear definitions for *traditional crime*, its relationship to *deviance*, and how cybercrimes fit into these definitions limit the utility of the book to those who are already familiar with these concepts.

Kirwan and Power next provide cursory introductions to the field of forensic psychology and criminological theories. This section would be appropriate for individuals who have some degree of knowledge of these fields, although a novice may benefit from more detail in order to understand the applicability of theories designed to account for real-world crime to virtual offenses.

The authors then provide a thematic chapter-by-chapter breakdown of cybercrimes in much the same vein as do other introductory textbooks in the field. The value of this work comes in its exposition of offender typologies and theoretical research oriented toward understanding the motives of various cybercriminals, including hackers, malware writers, digital pirates, and sexual offenders. Some discussion is also given to the prevention and sanctioning of each form of cybercrime, although the depth of these discussions is quite variable. These sections are all written in a very approachable fashion and give readers enough detail without overwhelming them with concepts.

Although this book is a unique contribution to the field, there are several limitations that must be considered. First, the absence of any substantive discussion of computer hardware and software is somewhat surprising, as most introductory works provide some context for the evolution of offender behavior in tandem with changes in both access to and ease of use of computers and the Internet. Such information is present in the authors' discussion of malicious software, but it would be helpful for readers to consider how digital evidence in browser histories, laptops, and mobile devices can be used to better profile the practices of all sorts of cybercriminals.

Second, the authors' selection and discussion of relevant works seem at times arbitrary and somewhat dated. For instance, there is substantive discussion of the Hacker Profiling Project research findings in the section on hacking but relatively little consideration of the larger body of research on the hacker subculture and its role in providing justifications for action and information to facilitate attacks (e.g., Holt, 2007; Jordan & Taylor, 1998; Schell & Dodge, 2002; Taylor, 1999). There is also a heavy emphasis on the use of techniques of neutralization research but little consideration of the role of peer offending in predicting individual action. The latter is one of the more substantial correlates identified in cybercrime offending research (see Holt & Bossler, 2014).

Finally, research and theoretical findings in each chapter are presented in chronological order, with generally little synthesis of concepts. This may be useful for introductory readers, although it does not give substantive exposition for the more serious scholar. Furthermore, this writing style may become somewhat repetitive for readers over time.

Overall, this work provides a relatively basic introduction to concepts of cybercrime and some exposition on theories relevant to both psychological and criminological research. The presentation is suitable for undergraduate students being introduced to the concept of cybercrime in the social sciences, although it would not satisfy the needs of the serious scholar or student. The lack of technical details regarding computer hardware, software, and digital forensics may make this work more attractive for computer scientists and readers who are already familiar with these issues. This may, however, be a limitation for social science students who want to understand the ways that technology provides evidence of offender activities and the evolving role of computers and cell phones in the facilitation of crime.

References

Furnell, S. (2002). *Cybercrime: Vandalizing the information society*. London, England: Addison- Wesley.

Holt, T. J. (2007). Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior*, *28*, 171–198. http://dx.doi.org/10.1080/01639620601131065 PsycINFO →

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, *35*, 20–40. http://dx.doi.org/10.1080/01639625.2013.822209 PsycINFO →

Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review*, *46*, 757–780. http://dx.doi.org/10.1111/1467-954X.00139

Power, A., & Kirwan, G. (2011). Ethics and legal aspects of virtual worlds. In A. Dudley, J. Braman, & G. Vincenti (Eds.), *Investigating cyber law and cyber ethics: Issues, impacts, and practices* (pp. 117–131). Hershey, PA: Information Science Reference. http://dx.doi.org/10.4018/978-1-61350-132-0.ch007

Schell, B. H., & Dodge, J. L. (2002). *The hacking of America: Who's doing it, why, and how*. Westport, CT: Quorum Books.

Taylor, P. (1999). *Hackers: Crime in the digital sublime*. London, England: Routledge. http://dx.doi.org/10.4324/9780203201503

Wall, D. S. (2001). Cybercrimes and the Internet. In D. S. Wall (Ed.), *Crime and the Internet* (pp. 1–17). New York, NY: Routledge.