Cybercrime and Criminological Theory
Fundamental Readings on Hacking, Piracy, Theft and Harassment

First Edition

Edited by Thomas J. Holt

Included in this preview:
• Table of Contents
• Introduction

For additional information on adopting this book for your class, please contact us at 800.200.3908 x501 or via e-mail at info@cognella.com
Cybercrime and Criminological Theory

Fundamental Readings on Hacking, Piracy, Theft, and Harrassment

Edited by Thomas J. Holt
an introduction to cybercrime

Virtual Criminality: Old Wine in New Bottles? | Peter Grabosky 9

“At Light Speed”: Attribution and Response to Cybercrime/Terrorism/Warfare | Susan W. Brenner 13

routine activities theory

The Novelty of “Cybercrime”: An Assessment in Light of Routine Activity Theory | Majid Yar 65

Examining the Applicability of Lifestyle–Routine Activities Theory for Cybercrime Victimization | Thomas J. Holt and Adam M. Bossler 75

Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory | Travis C. Pratt, Kristy Holtfreter, and Michael D. Reisig 89

Being Pursued Online: Applying Cyberlifestyle–Routine Activities Theory to Cyberstalking Victimization | Bradford W. Reynolds, Billy Henson, and Bonnie Fisher 105

social learning and self-control

### Explaining Deviant Peer Associations: An Examination of Low Self-Control, Ethical Predispositions, Definitions, and Digital Piracy
Scott E. Wolfe and George E. Higgins

Page 137

### The Effect of Self-Control on Victimization in the Cyberworld
Adam M. Bossler and Thomas J. Holt

Page 147

### General Strain Theory

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traditional and Nontraditional Bullying Among Youth: A Test of General Strain Theory</td>
<td>171</td>
</tr>
<tr>
<td>Justin W. Patchin and Sameer Hinduja</td>
<td></td>
</tr>
<tr>
<td>Traditional Bullying, Cyber Bullying, and Deviance: A General Strain Theory Approach</td>
<td>185</td>
</tr>
<tr>
<td>Carter Hay, Ryan Meldrum, and Karen Mann</td>
<td></td>
</tr>
</tbody>
</table>

### Subcultural Theories

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Social Organization of Audio Piracy on the Internet</td>
<td>201</td>
</tr>
<tr>
<td>Jon Cooper and Daniel M. Harrison</td>
<td></td>
</tr>
<tr>
<td>Examining the Role of Technology in the Formation of Deviant Subcultures</td>
<td>213</td>
</tr>
<tr>
<td>Thomas J. Holt</td>
<td></td>
</tr>
</tbody>
</table>
an introduction to cyber crime
Over the last three decades, computer technology has become an entirely ubiquitous component of modern life. Individuals regularly utilize laptops, desktops, tablet computers, and smartphones to engage in all facets of life, from communications to finance (Moore, 2011; Smith, 2011). Social networking sites like Facebook allow us to stay in touch with friends and family around the world, while streaming media services keep individuals entertained 24 hours a day on demand. On-line retail generates billions of dollars in income every year, and most consumers now utilize electronic banking services to manage their accounts and pay bills (Anderson, 2010). In fact, government and industry now depend on the Internet and computers to maintain sensitive records and provide real-time information to consumers and citizens about any issue that may be of interest.

The increasing dependence on technology to support and manage our lives has created unparalleled opportunities for crime and misuse. In fact, most any form of crime now involves technology in some way, whether through the use of cell phones and text messages or more novel applications of
technology to commit crimes that are not otherwise possible outside of digital devices (Taylor, Fritsch, Liederbach, & Holt, 2010; Wall, 2007). The World Wide Web and the Internet also provide a venue for individuals who engage in crime and deviance to communicate and share information; this would not otherwise be possible in the real world (Quinn & Forsyth, 2005). As a result, it is vital that we begin to understand how these changes are occurring, and what this means for offending in the 21st century.

To that end, it is necessary to define and classify the crimes that involve computers in some fashion. The terms “cybercrime” and “computer crime” are most frequently used to identify these offenses and have become nearly synonymous, although they technically refer to different behaviors. Cybercrime refers to crimes “in which the perpetrator uses special knowledge of cyberspace,” whereas computer crimes are offenses where “the perpetrator uses special knowledge about computer technology” (Furnell, 2002: 21; Wall, 2001). Many in the popular media treat these terms interchangeably (Furnell, 2002). However, this text will use the term “cybercrime” because of the large number of offenses that can occur in on-line environments and the overwhelming number of computers that are connected to the Internet.

Understanding what acts constitute cybercrime has led to a great body of research on the various offenses that fall under this term. One of the most well-referenced and constructed frameworks to understand cybercrimes is Wall’s (2001) four-category typology to identify the wide range of behaviors involving technology and the Internet in some fashion. The first category is cyber-trespass, encompassing the crossing of invisible, yet salient, boundaries of ownership on-line (Wall, 2001). Computer hackers are most likely to engage in acts of cyber-trespass due to their desire to penetrate computer systems. Defined broadly, hackers are individuals with a profound interest in computers and technology who have used their knowledge to access computer systems for malicious or ethical purposes (Holt, 2007; Jordan & Taylor, 1998). Though hackers engage in and develop security tools, many in the general public only view hacking in its malicious context because of the economic and personal harm they may cause (Furnell, 2002). In fact, malicious hacking is often tied to the creation and distribution of malicious software, or malware, that can automate attacks against computer systems (Bossler & Holt, 2010; Chu, Holt, & Ahn, 2010). These programs can disrupt e-mail and network operations, access private files, delete or corrupt files, and generally damage computer software and hardware (Computer Security Institute, 2012). Thus, acts of cyber-trespass are a significant concern for home users, businesses, and governments alike.

The second and related category is cyber-deception and -theft. This form of computer crime includes all the various criminal acquisitions that may occur on-line, particularly for thefts due to trespass. For example, businesses lost over $5 million to theft of proprietary or confidential information in 2007 (Computer Security Institute, 2008). Similarly, there are several different types of fraud that are perpetrated on-line, including electronic auction or retail-based fraud schemes, stock scams, and the sale of counterfeit goods (Newman & Clarke, 2003; Wall, 2004). Another high-profile form of cyber-theft is digital piracy, or the illegal copying of digital media such as computer software, digital sound recordings, and digital video recordings without the explicit permission of the copyright holder (Higgins, 2005; Hinduja, 2003). Pirated materials can be downloaded easily in a variety of outlets via the Web, and are thought to cause billions of dollars in losses through lost revenue and jobs (Higgins, 2005).

The third category within Wall’s (2001) typology includes cyber-porn and obscenity. Sexually explicit images and video are immediately accessible on-line and constitute a multibillion dollar industry (Edelman, 2009; Lane, 2000). Though these materials may not be illegal, the Internet has also fostered the growth of a wide range of communities supportive of deviant sexual behaviors (DiMarco, 2003). On-line spaces enable individuals to find others who share their interests, creating supportive communities
where individuals can be part of a group that validates their practices (Rosenmann & Safir, 2006). For instance, the customers of prostitutes regularly use technology to communicate with others who share their interests and solicit illicit sexual services in the real world (Holt & Blevins, 2007). The Internet has also become a popular venue for pedophiles and sexual predators to gain access to potential child victims or child pornography (Durkin, 1997; Quayle & Taylor, 2002).

The final form of crime within Wall’s (2001) typology is cyber-violence, representing the distribution of a variety of injurious, hurtful, or dangerous materials on-line. For example, individuals can now use the Internet as a means to threaten, bully, or harass others (Bocij, 2004; Finn, 2004). Harassment can take a variety of forms, such as threatening or sexual messages delivered via e-mail, instant messaging services, or posts in chatrooms. In addition, social networking sites engage individuals to post hurtful or mean comments for everyone to see without any direct contact with the intended target (Hinduja & Patchin, 2009). Victims of stalking and harassment may feel physical or emotional stress as a consequence, while others may report being able to ignore such comments entirely (Finn, 2004; Hinduja & Patchin, 2009). Estimates of on-line harassment and stalking appear to be on the rise, particularly among young people and college students, due in part to frequent Internet use among this population (Bocij, 2004; Finn, 2004; Wolak, Mitchell, & Finkelhor, 2006).

This text provides an exploration of activities from each of these four forms, with particular emphasis on participation in and victimization by hacking, fraud, theft, piracy, bullying, and stalking. These works provide an overview of the correlates and predictors of cybercrime victimization and offending, as well as the utility of traditional theories of crime for these emerging activities. But first, it is necessary to give adequate context to the evolution of research perspectives on cybercrime. Thus, selections from two seminal works are provided to frame the challenges that cybercrime poses to our concepts of law, policing, and criminality as a whole. The first article, by Grabosky (2001), provides one of the first discussions of cybercrimes during the earliest periods of investigation in this field. In this work, he argues that crime in cyberspace is “old wine in new bottles,” in that traditional forms of offending are enabled through new tools. Computer technology simply provides another medium by which such information can be obtained from potential victims (Grabosky, 2001). In turn, this creates substantive challenges for police and private industry to investigate these offenses. In the second piece, Brenner (2007) provides a more recent discussion on the issue of cybercrime and its relationship to cyberterrorism, whereby extremist groups can engage in cyber-attacks to affect government and civilian targets. The inherent challenges these offenses pose to law enforcement require a reconceptualization of how cyberspace can be policed, and the role of civilians in order maintenance on-line. Thus, Brenner (2007) discusses these issues in detail and provides a model for the future of policing on- and off-line.

The fundamental insights provided by these pieces demonstrate the myriad threads in cyberspace and the difficulties that traditional criminal justice models face in combating cybercrimes. In order to improve the justice system’s response to the constant shifts in offender behavior on-line, it is critical that researchers identify the causes and nature of participation in cybercrimes generally. Insights into the root causes of offending can be used to develop targeted enforcement strategies that may more effectively detect active criminals and deter prospective offenders. As a result, criminologists have created a number of theories to account for a range of deviant and criminal behaviors in the real world. There is, however, a lack of clarity as to the value of this body of knowledge to account for offenses in virtual environments. Thus, the remainder of this text presents seminal and cutting edge tests of traditional theories of both crime victimization and offending to consider their applicability to cybercrimes. In turn, this should enlighten our knowledge of cybercrime and criminological theories and identify key questions within each theoretical perspective that can advance the field as a whole.
discussion questions

1. What are some of the factors that immediately differentiate cybercrimes from more traditional real-world offenses? For instance, does the anonymity afforded by the Internet make it more difficult to identify an individual responsible for an act of cybercrime?

2. What potential forms of cybercrime victimization do you think you may be exposed to on a daily basis? For instance, how frequently do you receive questionable e-mail messages with links to websites you have never seen before?

3. Why are cybercrimes such a challenge for traditional models of policing and criminal justice processing? Do you agree with Brenner’s (2007) argument that citizens be greater incorporated into the regulation of on-line spaces?

references


