Book Review of Cyber Criminology: Exploring Internet Crimes and Criminal Behavior

Jose R. Agustina[1]
Universitat Internacional de Catalunya, Barcelona, Spain

Cyber Criminology: Exploring Internet Crimes and Criminal Behavior, K. Jaishankar, 2011, CRC Press, Taylor and Francis Group. Pages 461. ISBN 978-1-43982-949-3

As cyber crime has proliferated exponentially across the globe, those in the criminal justice field have lacked suitable and updated knowledge concerning the pedestrian reality of modern cyber crime. Popular media has created an image of cyber crime that suggests a lone hacker breaking through seemingly impossible security measures to access lucrative secret data. Crimes like these are very rare, but cyber crime is all too common. Criminals use the Internet to commit fraud, harass or bully people, download illegal pornography, or download stolen music far more than they use the Internet to violate national security. Edited by K. Jaishankar, *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* is a collection of chapters on cyber crime which focuses on common instances of internet crime that law enforcement officials are likely to deal with on a daily basis. The chapters within this edited collection are written by international scholars and provide the reader with provocative and thoughtful viewpoints upon which to develop one's own thoughts. Moreover, the book strengthens a timely and necessary debate among academics and practitioners, and beyond.

While ordinary everyday crimes may seem minor, they cause the most victimization. With more people around the world spending more time on the Internet for work and entertainment, criminals are able to find and exploit suitable targets far more often than in the past, which is emphasized by Professor David Wall in his Foreword, "Even if we do not use the Internet, much of our personal information will be stored somewhere on a networked computer, so in one way or another it affects all of us" (p. xi). The individual crimes are often small, but they have a huge effect in aggregate financial losses and are difficult to pursue legally because of the international nature of much of the crime.

The chapters are organized into topical sections, somehow loosely related because of the variety of crimes and perspectives of analysis. Preceding the five sections, Jaishankar's Introduction sets the stage for all of them. He also summarizes his "Space Transition Theory of Cyber Crimes" (STT) (2008), which tries to show why people behave differently when they move from one space to another. Jaishankar's theory is closely related to opportunity theories, anonymity as a crime predictor and Marcus Felson's (2003) convergence settings approach. Thus, STT relies on opportunity, space and

[1]Professor, Department of Criminal Law and Criminology, Universitat Internacional de Catalunya, Barcelona, Spain. Email: jragustina@uic.es

displacement. In this way, Jaishankar argues that persons with repressed criminal behavior in physical space have a propensity to commit crimes in cyberspace that they, otherwise, would not commit due to their status and position. It is also built up upon the lack of deterrence associated to anonymity. Although anonymity already was a traditional predictor of crime in real space, it becomes more criminogenic in virtual space. Thus, while online, some people self-disclose or act out more frequently or intensely than they would in person, the "online disinhibition effect" (Suler, 2004). In a sense, STT could be seen as a step forward in the context of Routine Activity Theory approach, applying some of its main tenets to virtual space.

The first section, "Deviance and Criminal Subculture in Cyberspace," contains a pair of chapters about specific criminal subcultures in different parts of the world. It includes both the "Yahooboys" of Nigeria and the Internet gambling companies headquartered mostly in the Caribbean. The former deals with the growing menace of cyber crime in Nigeria. Through survey research and participant observation, the findings confirmed the author's main hypothesis, that inactivity on the part of the political leadership, poverty, unemployment, and social standards of life deterioration, has been the main factors facilitating the poisonous and detrimental utilization of the Internet platform in defrauding naïve individuals across the globe. On the other hand, regarding the Internet gambling account, the chapter focuses on a real problem affecting 5% of the US population, as individual's resources and interests become focused on the next chance to gamble. Thus, gambling at home on the computer "avoids feelings of discomfort about the wagering procedures at places such as blackjack tables, where many eyes—most especially, those of the dealer–are focused on gambler's movements." (p. 13). The authors relate the David and Goliath dispute between the US and the small Caribbean islands of Antigua and Barbuda, which was the first attempt by the World Trade Organization to examine cross-border electronic services, and upon it they offer a view of what they regard as the inevitable path that the trajectory of Internet gambling will take.

The second section, "Perpetrators' perspectives and offender use of the Internet," concerns the offenders' view of themselves and how they justify their behavior. Most of the chapters discuss about pedophiles and Internet child pornographers, but the first and the last ones covered other offenders, such as computer hackers and terrorists. Qualitative methods are prevalent throughout the whole section. As an example, the description of hackers' subculture in chapter 3, how they interpret their lives, behavior, and beliefs (as well as their perceptions of how society treats them) provides a deeper, sharper picture on the complexity of such phenomenon than a survey could. Through a narrative interview technique, the author interviewed 54 hackers and, among other interesting, complex issues he stresses how hacking has been difficult to interpret due to the lack of a solid definition and vague boundaries between computer experts and hackers (as well as those characteristics that differentiate various types of hackers).

Interestingly, the author of Chapter 4 argues, addressing sexual addiction on the Internet, that Internet anonymity promotes pedophilia within the otherwise normal populace. Her study aims to correlate the association of sexually compulsive or addictive behavior with social isolation. Based upon a study of 22 forensic interviews, the chapter outlines a framework for understanding the psychology of the sex offender from a clinical perspective and describes five stages from inception to incarceration that the virtual sex offender follows. In chapter 5, the authors try to understand the psychology of the child pornography consumer and the differences between an Internet and a non-Internet

consumer using Bandura's theory of reciprocal determinism. Through an examination of the results of survey addressed to demographic, personality, and behavioral characteristics, statistical analyses revealed a relationship between higher scores on exploitive-manipulative amoral dishonesty traits, lower scores on internal moral choice, and the viewing of child pornography. The authors conclude that the consumption of child pornography over the Internet is likely to increase unless researchers decide to make this area of study a priority. Authors of chapters 6 and 7 discuss, respectively, the online exploitation of children by using a novel methodology—a sting operation, and how far the sites that encourage sexual relationships between adults and children are criminogenic in nature.

The third section, "Digital Piracy," covers such a field of deviation with an almost exclusive focus on music piracy. While the chapters are primarily focused on those who are downloading the music, the book also contains an article discussing the failure of those who hold the rights to downloaded content to effectively utilize the legal system to prevent infringement. Chapter 9 reasons how the rational choice theory establishes the link between low self-control and digital piracy, being a significant contribution to cyber criminology literature. Chapter 10 discusses the Recording Industry Association of America, which filed a lawsuit to prevent the illegal sharing of music files, and chapter 11 addresses the issue of Internet piracy among college students. The authors of Chapters 12 provide evidence that the level of neutralization used by a potential music pirate affects the piracy that actually occurs. Participants in music piracy are often misguided about their perceptions of the harm that is caused through participation in this behavior—as well as the responsibility that resides with them. This perception, and a lack of education in this subject area, increases the likelihood of participation in this "victimless" crime. The authors also discuss digital piracy as an issue and the differences among nations. The authors argue that the main reason why less developed nations do not see it as a big issue is that such nations cannot afford to buy software or music that are expensive, and they feel that capitalistic nations alone should not own this software. However, their study was conducted in the US, thereby being necessary to analyze the issue in less developed nations. Finally, Chapter 13 tries to analyze digital piracy with neutralization theory and shows, as other chapters do. However, digital piracy is still an issue of debate and not many may accept it as a crime.

Victims and potential victims are covered in the fourth section with a discussion about why some people become cyber crime victims while others don't. There are chapters about cyber stalking, malware, and online social networking victimization, and there is a concentration on Felson's Routine Activity Theory and how such a theory affects victimization. Chapter 14 aims at examining the factors responsible for computer-crime victimization based on Routine Activity Theory and Lifestyle Theory main tenets (i.e. lifestyle variables along with daily routine activities in cyberspace and the presence of digital guardians). Similarly, chapter 15 focuses on adolescent online victimization in relation with constructs of Routine Activity Theory. Teenagers, by nature, are in fact always at the forefront of new technologies, pushing their boundaries, and exploring themselves and the freedom that these technologies bring. Given the teen's developing brain function, susceptibility to peer pressure, attraction to risky behaviors and lack of self-regulating skills, they are particularly vulnerable to the harms associated with the Internet. One risky behavior that has not been addressed but it is particularly important as a threshold for online victimization is sexting. Thus, the distribution of nude or semi-nude pictures taken and exchanged among friends or lovers sets the stage for being victimized.

In this context, minors' precociousness and promiscuity along with technology accessibility have led to some problematic phenomena when viewed from legal and criminological perspectives.

Chapter 16 discusses online harassment and intimidation, which has been termed cyber stalking. In this chapter, the author discusses how cyber stalking, despite the fact that is an extension of traditional stalking, it is not as predictable as traditional stalking. And, respectively, chapters 17 and 18 discuss online social networking in relation with women victimization and malware victimization. The final section focuses on legal issues and policy implications, with articles on cyber vandalism in Islamic laws and the human rights concerns in the Digital Age. Additionally, chapter 20 discusses cyber bullying as a psychologically devastating form of social cruelty among adolescents. It reviews the current policy vacuum of the legal obligations and expectations of schools to monitor and supervise online discourse, while balancing student safety, education, and interaction in virtual space, which also encompasses a discussion of the institutional responses to cyber bullying.

The book ends with some reflections by Jaishankar on the future of cyber criminology as an independent discipline. The big question, as he points out, is, "Will it evolve as a separate discipline?" In this regard, he states that there are many such criminologies that have not become separate disciplines (citing green criminology, biocriminology, environmental criminology) but, in his opinion, "cyber criminology has the potential to become an independent discipline because of its dynamic expansion of exceptional interdisciplinary content in teaching and research" (p. 411). He analyses the main challenges for modern-day cyber criminologists –i.e. issues in teaching, research and professionalization of the discipline.

However, in my view, Cyber Criminology lacks a solid structure or, at least, an academic structure. If cyber criminologists claim to create a new discipline, some could argue that much more structure would be needed. However, what does it mean to become a discipline? And, moreover, would the so-called cyber (space) criminology be the opposite discipline to real (space) criminology? Should not the real and virtual dimensions of crime be included within the same research and teaching purposes? It is no doubt that cyber crimes and cyber victimization have their own particular patterns. One could also claim that human beings act and commit crimes quite different while online. There is a sort of schizophrenia or dissociative identity disorder that might justify different approaches. But, can we absolutely separate both worlds without missing something relevant?

For research and crime policy purposes, it is also debatable if we should build up separate research and policies to cope with the both sides of a phenomenon, for instance, bullying and cyber bullying. Again, there is no doubt that we need updated and suitable knowledge about the particular features regarding any particular type of crime in cyber space. We do need to adapt our instruments and strategies to each space. But the question is if such a particular strategy should not be defined along with its counterpart in real space. Probably, in a not so far future, both realities will come naturally together or, even, they will be so mixed in our lives that there will make impossible to separate them one another. However, this is not the case for the time being. Meanwhile, the creation of a separate academic and research discipline should be absolutely needed. As for the current and future needs in forensics and digital evidence, there will always be technical issues that will demand a specialized expertise.

To conclude, the greatest asset of this book is its focus on a broad sample of topics and its significant contribution to previous research in the field. The reader is able to gain better knowledge on the state of the art global cyber crime by analyzing in detail a bunch of cyber crimes from different perspectives. Thereby, *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* is an excellent resource for providing a general overview of the field of cyber crime that would be of interest to those in criminal justice, law, psychology and sociology.

References

Felson, M. (2003). The Process of Co-Offending. In M. J. Smith & D. B. Cornish (Eds), *Theory for Practice in Situational Crime Prevention. Crime Prevention Studies* (pp.149-168), 6. Monsey, NY: Criminal Justice Press.

Jaishankar, K. (2008). Space transition theory of cyber crimes. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 283–301). Upper Saddle River, NJ: Prentice Hall.

Suler, J. (2004). The Online Disinhibition Effect. *Cyberpsychology & Behavior*, 7(3), 321-326.