CATHERINE D. MARCUM, CYBER CRIME (Wolters Kluwer Law & Business, 1st ed. 2014)

Wolters Kluwer Law & Business (New York, United States of America: 2014)
ISBN: 9781454820338
Price: $74.64
Page Length: 145 Pages

Keywords: Cybercrime, Computers, Crime, Internet

Reviewed by Bayley Weese
Journal of High Technology Law
Suffolk University Law School

Cyber Crime: When Criminal Activity Extends Beyond the Physical World

"There will never be another generation that does not have constant accessibility to technology."[1]

Cyber Crime, by Catherine Marcum, examines eight new types of crime that occur exclusively on the Internet, and have only flourished due to the recent expansion of technology. This book review analyzes the entire book, which includes lengthy descriptions of all eight cyber crimes and the way prosecutors and law enforcement have attempted to combat them, and assesses the book as a basic reference allowing a reader with minimal knowledge on this subject to gain a better understanding of the general principles of cybercrime. The author, Dr. Catherine Marcum, is a professor at Appalachian State University, in the Department of Government and Justice Studies.[2] She is listed as an author on five additional books: *Social Networking and Criminality* (CRC Press/Taylor & Francis Group, 2014), *Sexual Victimization: Then and Now*

[1] CATHERINE D. MARCUM, CYBER CRIME 1 (1st ed. 2014) Wolters Kluwer Law & Business (New York, United States of America: 2014).
[2] *See Dr. Cathy Marcum*, APPALACHIAN STATE UNIVERSITY

(Sage Publications, 2014), *Prison Sex: Myths and Realities* (Lynne Rienner Press, 2013), *Digital Piracy: An Integrated Theoretical Approach* (Carolina Academic Press, 2011), and *Adolescent Online Victimization: A Test of Routine Activity Theory* (LFB Scholarly Publishing, 2009). Additionally, Marcum has published thirty-four articles in peer-reviewed journals ranging in topics from Internet facilitated cheating to sentencing practices for convicted cyber criminals. Her areas of interest and expertise include cybercrime victimization and offending, sexual victimization, and correctional issues.[3] Marcum has been a member of both the American Society of Criminology and the Academy of Criminal Justice Sciences since 2005.

Cyber Crime provides a brief overview of new crimes that have evolved due to the rapid increase of technology in recent years. Marcum addresses eight types of cybercrime, each in their own chapter, including digital piracy, child pornography, prostitution, sexual solicitation, scams and cons, cyberbullying and cyberstalking, hacking and malware, and cyberterrorism. The book begins with a chapter devoted to a general introduction to cyber crime.[4] In this chapter, Marcum discusses the history of the Internet, followed by a detailed description of the emergence of cyber crime and how cybercrime was not an "instantaneous act."[5] Marcum then mentions the public's perception of internet crime, and how the "fear of crime and expectations of criminal victimization affect a person's behavior," and then explores how cyber crime can be committed transnationally and the problems that subsequently arise with extraditing cyber criminals to the United States from foreign countries.[6]

Each chapter of *Cyber Crime* begins with a "case study" of the specific crime – a page long story of a highly publicized real-life example. For instance, in the child pornography

[3] *See id.*
[4] *See* MARCUM, *supra* note 1, at 1.
[5] *See* MARCUM, *supra* note 1, at 2-4.
[6] *See* MARCUM, *supra* note 1, at 4-7.

chapter, Marcum discusses a case where a pediatric clinical instructor at the Children's Hospital in Boston, Massachusetts, was found to have over 500 photographs and between 60 and 100 films of children involved in sexual acts.[7] If convicted, the defendant faced up to 20 years in prison.[8] In the final chapter of the book, cyberterrorism, Marcum uses the Iranian Cyber Army's takedown and control of the website Twitter as the case study of how cyberterrorists can fully utilize the Internet in their attacks.[9] After the case study, each chapter delves into the definition of the specific crime and the applicable statute that makes the act criminal. The middle of each chapter is different depending on the specific crime. For example, the sexual solicitation chapter explores the kinds of people who are both committing and falling victim to this crime.[10] In the chapter on scams and cons, Marcum discusses the myriad of Internet scams including retail scams, phishing, skimming, lottery schemes, and timeshare marketing – among many others.[11] Each chapter in the book ends with a small section containing reflective discussion questions and a list of all of the sources and authorities cited throughout the chapter for easy reference.

The second chapter of *Cyber Crime* focuses on digital piracy – the stealing of online material, such as books, movies, and music, without consent from the author or original creator.[12] The Copyright Act of 1976 is the prevailing statute providing legislative protections to intellectual property, including that of which is posted on the Internet.[13] Marcum accentuates that digital piracy is not a victimless crime and the economic costs associated with digital piracy crime are considerable.[14] Finally, Marcum explores the reasons why individuals engage in digital

[7] *See* MARCUM, *supra* note 1, at 25.
[8] *See id.*
[9] *See* MARCUM, *supra* note 1, at 131.
[10] *See* MARCUM, *supra* note 1, at 59-63.
[11] *See* MARCUM, *supra* note 1, at 75-87.
[12] *See* MARCUM, *supra* note 1, at 12.
[13] *See* MARCUM, *supra* note 1, at 17-18.
[14] *See* MARCUM, *supra* note 1, at 13-14.

piracy and offers two theories of explanation: the Self-Control Theory and the Social Learning Theory.[15]

Chapter three centers around child pornography – what Marcum describes as a hybrid crime.[16] A hybrid crime is that which "falls between traditional and true cybercrimes. These are traditional crimes that are expanded through the use of the Internet."[17] Marcum points out how child pornography has substantially risen since the advent of the Internet, and examines all of the legislative action to try and combat it.[18] Unfortunately combating child pornography has not been an easy road for Congress, as there have been numerous First Amendment claims against censoring these images and videos.[19]

Chapters four and five explain prostitution and sexual solicitation, respectively. In the prostitution chapter, Marcum discusses all the different ways that one can advertise for sex online and how people who sell sexual services on the Internet can evaluate their customers before the transaction occurs in the real world.[20] In the sexual solicitation chapter, Marcum details the general characteristics of online predators as the complete opposite of the public's general perception of a pedophile.[21] Almost no sexual solicitation offenders have a previous criminal record or any known sexual contact with minors, rather they are people who have had a hard time forming meaningful relationships with other adults, a history of abuse, and a sense of entitlement among other characteristics.[22]

---

[15] *See* MARCUM, *supra* note 1, at 15-16.
[16] *See* MARCUM, *supra* note 1, at 27.
[17] *See id.*
[18] *See* MARCUM, *supra* note 1, at 26, 31-32, 36-39.
[19] *See* MARCUM, *supra* note 1, at 36-39.
[20] *See* MARCUM, *supra* note 1, at 45-49.
[21] *See* MARCUM, *supra* note 1, at 61-63.
[22] *See id.*

Chapter six reviews scams and cons, while chapter eight addresses hacking and malware. Marcum describes a few of the numerous methods of identity theft and other Internet schemes like product counterfeiting, lottery schemes, and work from home scams.[23] Anti-identity theft legislation is mentioned briefly, but there is no mention of any other legislation to combat the other kinds of crime that fall under the category of scams and cons.[24] In chapter eight, Marcum defines what exactly it means to "hack" and she reviews some of the general characteristics the hacking community shares – most notably their high intelligence.[25] Marcum then delves into the subculture of and the motivations behind hacking.[26]

Chapter seven focuses on cyberbullying and cyberstalking – specifically the gray area that exists when prosecuting these kinds of cases, due to their recent emergence. Marcum briefly introduces the ideas of both cyberstalking and cyberbullying and then quickly transitions to all of the pending legislation right now in all fifty states for both cyberstalking and cyberharassment.[27] Lastly, chapter nine discusses exclusively the idea of cyberterrorism and all of the benefits the Internet provides terrorists. This last chapter is concise due to cyberterrorism being one of the newest of all cybercrimes, but Marcum does mention there could be advantages to counterterrorism being conducted through the Internet, because Internet users always leave an electronic trial of their steps.[28]

Marcum explicitly states the purpose of her book is "to provide the reader with a thorough overview of the different types of cybercrime present online"[29] – and she does just that. Marcum takes an exceptionally objective approach to her analysis and descriptions of the

[23] *See* MARCUM, *supra* note 1, at 75-87.
[24] *See* MARCUM, *supra* note 1, at 80-81.
[25] *See* MARCUM, *supra* note 1, at 110-12.
[26] *See* MARCUM, *supra* note 1, at 112-18.
[27] *See* MARCUM, *supra* note 1, at 94-101.
[28] *See* MARCUM, *supra* note 1, at 137.
[29] *See* MARCUM, *supra* note 1, at 7.

cybercrimes. Never once can her personal opinions on the crime, sentencing, legislative efforts to combat the crime, or the victim/offender relationships be discerned from reading her book. The definitions and descriptions of each crime are very clearly arranged, with no allowance for any bias from Marcum. That being said, while there is no specific style or type of voice, the piece is readable.

While there is no mention the audience Marcum intends to read this book, it would serve as a remarkable resource for anyone with basic to minimal knowledge of cybercrime. *Cyber Crime* does a skillful job of breaking each crime down to explain what exactly the crime is and the policy and reasoning as to why it is illegal in a clear and organized fashion. The case studies at the beginning of each chapter assist the reader to understand how these crimes play out in the real world – as often times the case study is a highly reported and well known example. The reader, now familiarized with a real world example of the specific crime, can easily begin comprehensive study of the crime. Marcum utilizes basic terms throughout her book, further facilitating a reader with no knowledge of cybercrime the ability to comprehend the material. *Cyber Crime*'s biggest strength is its readability and ability to explain concepts in such a clear, basic, format – again, ideal for the reader who may previously have next to no knowledge about cybercrime.

A criticism of *Cyber Crime* would be that Marcum devotes too much of the book to child pornography, prostitution, and sexual solicitation and not enough necessarily to white collar cybercrimes that affects both businesses and consumers, such as hacking, virus dissemination, phishing etc. While the book does address these crimes briefly, it doesn't spend as much time on them as it could considering how prevalent they are. Not everyone knows someone who has troves of child pornography on their computer, but almost everyone is familiar with someone

who has had their credit card numbers stolen or received a suspicious email part of a phishing attempt. Marcum does a satisfactory job addressing that these types of crimes do exist, as there are small descriptions for each of the kinds of scams and cons, but there is less than a page devoted to anything other than just these descriptions of the crimes. There is brief mention of anti-identity theft legislation, but with how prevalent this kind of cybercrime is, it would be more informative had Marcum chose to expand even further about what the government is doing to combat these specific kinds of Internet crimes.

Overall, *Cyber Crime* was both an informative and enjoyable read. As someone who knows very limited amounts about technology this book helped me connect the increase in technology to criminal justice, and begin to understand how these two worlds intersect. I would highly recommend *Cyber Crime* to anyone interested in learning about cybercrime who knows next to nothing about it already, whether that be the average citizen, a law professor, etc. Marcum truly does a fantastic job breaking down and explaining all of the different kinds of cyber crime.