Book Review of Crimes of the Internet

Stephen M. Marson¹
University of North Carolina at Pembroke, USA


Crimes of the Internet is an edited monograph whose intended audience is criminal justice undergraduate and graduate students. It includes 31 chapters divided into five sections which include:

- Online Predatory Child Victimization and Exploitation
- Emerging Global Crimes of the Internet
- Criminological Perspectives on Cyber Crimes
- Investigating and Prosecuting Cyber Crimes
- Cyber Terrorism: The “New” Face of Terrorism

Historically and chronically, edited monographs have two major flaws. First, chapters in edited volumes have an uneven quality; some chapters possess significantly greater quality and substance than others. This emerges because editors of such monographs cannot consistently attract the best chapter authors. This is not the case for Crimes of the Internet. The editors were able to attract distinguished authors within highly specialized areas of cyberspace crime. In itself, this was a Herculean task, executed by the editors with great success. Second, edited monographs generally have very weak transitions from one chapter or section to the next. Typically, monographs have weak, choppy or nonexistent linkages. Apparently, the editors gave specific guidelines to the authors and as a result the entire volume smoothly moves from one chapter and section to the next. This is a critically important characteristic for a textbook.

I have read and seen many books on Internet crimes and social mores’. One aspect of the identification, understanding, and prevention of these troubling activities is the fleeting nature of technology. Several years ago, Rules of the Road for the Information Superhighway: Electronic Communications and the Law was published. This non-edited and very expensive book created an accurate portrayal of the cyberspace legal environment at that time. Within less than a year, the volume possessed a great deal of outdated and inaccurate material! The author and publisher needed to write a second edition. Although a second edition was desperately needed, they did not pursue it. Why? Because of the

¹ Professor, Social Work Program, University of North Carolina at Pembroke, NC 28372-1510, United States of America. Email: steve.marson@uncp.edu
lightening fast changes in cyberspace, writing a second edition would require the author to start from scratch. Generally speaking, past work on cyberspace cannot be used as a foundation for an update. Technology changes with such speed, it is likely that some technological analysis can be outdated prior to going into print. I have reviewed other recently published books on cyber law and crime. They, too, will become rapidly outdated. The distinct advantage of *Crimes of the Internet* over other books on this topic is that updates promise to be much more manageable over time. The format will enable the current and future authors to update the material to be an accurate reflection of current realities of cyber crime. Thus, professors who adopt the book and future editions will have fewer problems with syllabus construction and other issues related to academic presentation.

Generally speaking monographs addressing cutting edge technology are best evaluated or assessed within the framework of “understanding/action.” By “understanding,” the central theme within a book would be guidance to offer the reader a theoretical basis on which to comprehend technological interaction. In the case of *Crimes of the Internet*, the authors would examine crime and explain how and why it exists. The authors would be required to offer a coherent platform for the reader to comprehend the existence of the crimes, identify those who commit the crimes (i.e. a prototype), damages that occur from the crimes and the unique process by which the crimes have been perpetrated. This theoretical understanding is absolutely essential for all undergraduate and graduate students. By “action,” the central theme within the book offers guidance to the reader as to what actions to take in order to apprehend, rehabilitate and adjudicate the criminal. In other words, an “action” book informs the reader as to what to do.

The common path for books intended for a student audience is the “understanding” framework. Within the context of law and crime, these authors pursue an unusual path. Normally, assessment of cyberspace crime and law emphasizes the negative dimension. That is, authors stress what the laws are, what crimes are being committed and what the law enforcement response should be. Although the authors engage this path, they also pursue the positive aspects of cyberspace. With many unprincipled and illegal activities taking place on the Internet, the authors hold the position that many positive aspects of the Internet have emerged. In any society, law enforcement and understanding of criminal activities may lack behind the actions of the offender. As we reap the benefits of cyberspace (or any other social activity), criminal activities emerge. Although the response to criminal activity seems insurmountable, the authors provide guidance on how to protect ourselves and citizens, while the legislation and law enforcement catch up to the technological advances of the criminal element.

Although the intended audience is undergraduate and graduate criminal justice students, it is likely that others will have an interest. Students and practitioners of law, psychology, social work and sociology would have an intensive interest in most of the chapters. I recommend that every academic librarian within these programs adopt this book. In addition, a college educated adult who has an interest in learning more about self preservation in cyberspace will have an intense interest in the subject matter. In that respect, public libraries should seriously consider adoption of this valuable book.