BOOK REVIEW

The Psychology of Cyber Crime: Concept and Principles

Reviewed by Maximiliano E. Korstanje, University of Palermo, Buenos Aires, Argentina

The Psychology of Cyber Crime: Concepts and Principles
Gráinne Kirwan and Andrew Power
© 2012 by IGI Global
372 pp.
$156.00
ISBN 978-161350350-8

A philosophical debate has been posed over last decades in industrial societies, where the cyber-world not only modified peoples´ life-styles, but taking attention to the advance of cyber-space which was originally consigned as a prolongation of reality. Cyberspace is defined as a network or shared enviroment in which communication goes through. The global network facilitated by internet allows a rapid connection for people to engage with others, selling and buying (exchanging) commodities. In recent years, some philosophers paid heed on the negative effects of cyberspace for individual behavior. This led to Jean Baudrillard to announce that the principle of reality sets the pace to a hyper-reality where events remained unreal. Hollywood echoed this concern by starring the film *Matrix*, a fictional saga that denotes a much deeper philosophical problem formulated by Plato in the Cavern; which means the connection of pleasure with displeasure or "the real and perceived enviroment". Though this dilemma is not new, it was aggravated by the appearance of cyberspace. To put this in bluntly, all of a sudden we are in a different world and one that we must face up to. In a globalized economy, all resources to protect civil populations from cyber-attacks should be taken by government. Although social sciences and scientists have widely focused on the problems and benefits of cyber-world, a marginal attention was given to the psychology of cyber-criminals or those persons who take the virtual to violate citizens 'rights.

As the previous backdrop, in this book, G. Kirwan & A. Power set forward 13 chapters which are based on the sociology of cybercrime as the main topic. Taking their cue from the consolidated legacy of forensic psychology in criminal behavior, authors understand that goals and motive of cyber-criminals (which range from specific examples as theft towards child pornography and

Copyright © 2015, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

malware) are still unclear. The lack of a solid theoretical framework to classify crimes committed in cyberspace is legally one of the most difficult limitations researchers face when they enter in the fieldwork. There are typical forms of cyber-crimes as cyber-bullying, inappropriate child exhibition or websites offering children pornography, thefts, swindle, and attacks perpetrated by terrorists to disable the system of defense of developed-nations. Therefore, the endless efforts of governments to prevent these cyberattacks pave the ways for the advent of newfound risks that sometimes vulnerates the smooth functioning of the system. To what extent, cyber security, which is associate to the implementation of efficient software performances, seems to be a fertile ground to cyber-attacks are widely addressed throughout chapter one. Rather, second chapter is oriented to explore the benefits or limitation offer forensic psychology to prevent cyber-crime. We start from the premise that this discipline is more interested in studying real cases of crime where victims are harassed or their commercial rights violated. In this respect, chapter third offers a good opportunity to readers to expand their current understanding on why these cyber-crimes occur. Exhibiting an erudite review of the already existent theories of crime, this section explores the contribution of a well-read scholar as Eysenck who has strongly evinced not only how crime evolved in certain periods of time, but incorporated the thesis it is culturally created and accepted by peer-groups. In XIXth century, medicine believed that criminality corresponded with a biological explanation. Eysenck´s theory of criminal personality argued that a great dispersion of individual personalities can be observed reducing involving factors into two dimensions, a person´s degree of extraversion and neuroticism. Quite aside the criticism on EPQ – Eysenck Personality Questionnaire, he amply shows that criminality is socially constructed by the convergence of self with enviroment. Because of its robustness in handling meanings and concepts, this is the best section of the book.

Complementarily, the second section, which is formed by chapter 4 and 5, shows a continued interest for studying the convergence of crimes with internet. It examines not only the psychological motivations of hackers and other cyber-criminals but attempts to draw a psychological profile of virus-writers, which turns out very interesting and useful for policy makers, police and agents of governments. Beyond their popularity as rebels, a clear distinction should be done; hackers are not the same than virus writers simply because both follow different goals and motives. While the former signals to manipulate knowledge in favor of some private interests, the former one is oriented to create indiscriminate damage to users and their respective networks. In view of the reputation of cyber-criminals in their groups, some deviant behaviors are more popular than others. For example, a hacker who violates the Pentagon´s security may very well gains further recognition than a pedophile network taking advantage of cyberspace to coordinate its criminal acts. The section third focused on the conditions where our systems are vulnerable to cyber-attacks. Other crimes as cyber-bullying and online child pornography are interesting topics that take part of chapters integrated in this section. Last but not least, those restant chapters which crystalize the fourth part are seminal texts dealing with the complexity of crime in an online networking platform. The problem of online governance after Jullian Assange´s WikiLeaks scandals represented one of the main priorities of states. This begs a more than interesting point, is digital technology based on the desire of control, or can be vulnerated in favor of peoples, what happens when state is the agent that violate rights to privacy?

The main thesis of this book is that though there is a lot of material published on cyber-crime, less attention was given to the psychology of cyber-criminals as well as the effects on victims. The fact is that if crime is culturally determined, the ethical borders between good and wrong are blurred. What is a cyber-crime? The produced material is certainly intended to discuss tech-

Copyright © 2015, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

nically forms of protection, and software anti-malware, but this does not suffice to understand the world of those who perpetrate these attacks, their attitude and reasons. The vast experience of authors as fieldworkers is conjoined to a foundational review of the literature to make a text that surely will pass the time proof. The logic of cybercrime and the reaction of society to this is one of the themes explored in this pungent research. Obviously, this reviewed work has not offer answers for all our questions formulated in this review, but shows a platform to start a much smarter discussion in regards to cyber-security.

Copyright © 2015, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.