Preface

The Internet's rapid diffusion and digitization of economic activities have led to the emergence of a new breed of criminals. Economic, political, and social impacts impacts of these cyber-criminals' activities have received considerable attention in recent years. Individuals, businesses, and governments rightfully worry about the security of their systems, networks, and IT infrastructures.

Looking at the patterns of cybercrimes, it is apparent that many underlying assumptions about crimes are flawed, unrealistic, and implausible to explain this new form of criminality. The empirical records regarding crime patterns and strategies to avoid and fight crimes run counter to the functioning of the cyberworld. The fields of hacking and cybercrime have also undergone political, social, and psychological metamorphosis.

The cybercrime industry is a comparatively young area of inquiry. While there has been an agreement that the global cybercrime industry is tremendously huge, little is known about its exact size and structure. Very few published studies have examined economic and institutional factors that influence strategies and behaviors of various actors associated with the cybercrime industry. Theorists are also debating as to the best way to comprehend the actions of cyber criminals and hackers and the symbiotic relationships they have with various players.

Our observations above highlight the emergent nature of the global cybercrime industry. Cybercrime is also a topic of considerable interest both theoretically and practically. This book aims to contribute to filling the research gaps discussed above and initiate further academic discussion on this topic. A major goal of the book is to examine economic processes associated with the cybercrime industry. The book would help us better understand cybercrime as a form of economic activity and could inform the development of strategies for crime prevention. A further goal of the book is to understand institutional processes in the cybercrime industry. More to the point, we analyze formal and informal institutions and associated feedback mechanisms influencing this industry. A third goal of the book is to provide insights into the entrepreneurial aspect of firms engaged in cyber-criminal activities. The book examines how criminal entrepreneurs in the cyberworld organize and manage essential ingredients needed for their businesses. We will also take a close look at cybercrime business models. A fourth goal of the book is to explain the global

variation in the pattern of cybercrimes. As we have demonstrated, economic factors facing cyber-criminal and cybercrime victims are significantly different in developing and developed countries. They include nature and quality of hardware, software, and infrastructure; targetability of victims; stock of cybercrime skills; and associated opportunity costs and benefits. Finally, the proposed book seeks to understand threats and countermeasures taken by key actors in this industry.

In sum, by providing a comprehensive overview of the ingredients, institutions, cost–benefit aspects, and modus operandi of different actors involved in cybercrimes, it is hoped that this book will aid in better understanding and analyzing the rapidly transforming cybercrime landscape. The book also provides research, managerial, and policy implications associated with cybercrimes.

This book is inter-disciplinary in focus, orientation, and scope. It crosses disciplines such as economics, law, business and management, international affairs, sociology, anthropology, cultural studies, and criminology to develop theory and provide information that could move theory and practice forward in the study of cybercrimes. This book is also theory-based, but practical and accessible to the wider audience.

This book is primarily targeted to academic specialists, practitioners, professionals, and policy makers interested in and concerned about the evolution of cybercrime industry. Undergraduate and graduate students are also target audience. More broadly, this book is expected to be useful to all members of the cyberworld to understand the nature of vulnerabilities from cyberattacks and develop appropriate defense mechanisms.

As for the ideas, concepts, content, and theories presented in this book, I am indebted and grateful to several people for comments, suggestion, support, encouragement, and feedbacks. Various papers related to this book were presented at scholarly meetings such as: (a) Fourth Annual CPP International Conference on Public Policy and Management, August 9–12, 2009, Bangalore, India; (b) Seventh International Business Week Conference, University of Minho, Braga, Portugal, April 26–May 1, 2009; (c) the 5th Annual Mason Entrepreneurship Research Conference, March 27, 2009 at Fairfax, Virginia; (d) The Workshop on Secure Knowledge Management, Dallas, Texas, November 3–4, 2008; (e) Third Annual Forum on Financial Information Systems and Cyber Security, Robert H. Smith School of Business at the University of Maryland, May 24, 2006; and (f) Sixth Annual International Business Research Forum, Philadelphia, April 1–2, 2005. This book benefited greatly from the comments and suggestions of anonymous reviewers and participants of these meetings.

My major debt is to my doctoral dissertation advisor Nikhilesh Dholakia, who has provided me with constant intellectual stimulation, support, and encouragement. I have also benefitted greatly from interacting with my colleagues Ralf Bebenroth, Nicholas Williamson, and David Bourgoin. Katharina Wetzel-Vandai, Senior Editor, Economics/Management Science, Springer has been constructive, supportive, helpful, and encouraging in guiding and managing this project. I also received help and support from my graduate assistant Jun (Johnny) Situ. I wish to express my

profound gratitude to my life's companion and best friend, Maya, for the patience and loving support during the endeavor to write this book. Finally, I'd like to dedicate this book to my mother Manamaya Kshetri, for her love, guidance, and support.

Greensboro, North Carolina Nir Kshetri

http://www.springer.com/978-3-642-11521-9

The Global Cybercrime Industry
Economic, Institutional and Strategic Perspectives
Kshetri, N.
2010, XXI, 252 p., Hardcover
ISBN: 978-3-642-11521-9