Routledge Handbook of International Criminology

Edited by
Cindy J. Smith, Sheldon X. Zhang,
and Rosemary Barberet

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

Contents

<i>List of plates</i>	xiii
<i>List of figures</i>	xv
<i>List of tables</i>	xvii
<i>List of boxes</i>	xix
<i>Notes on contributors</i>	xxi
<i>Foreword</i>	xxix
<i>Acknowledgments</i>	xxxci

1 Progress of international criminology	1
<i>Cindy J. Smith, Sheldon X. Zhang, Rosemary Barberet</i>	

PART I

Methods and theories	9
-----------------------------	----------

2 Introduction to international research challenges	11
<i>Cindy J. Smith</i>	
3 Doing criminology in the "semi-periphery" and the "periphery": in search of a post-colonial criminology	13
<i>Juanjo Medina</i>	
4 International criminology: qualitative research on polluted actors	25
<i>Martha K. Huggins</i>	
5 Quantitative criminology: crime and justice statistics across nations	38
<i>Jan van Dijk</i>	
6 The Campbell Collaboration Crime and Justice Group: a decade of progress	53
<i>David P. Farrington, David L. Weisburd and Charlotte E. Gill</i>	

revention	64	20 Trafficking of "conflict diamonds" <i>Dina Siegel</i>	200
isitive	77	21 Conceptualizing and studying organized crime in a global context: possible? indispensable? superfluous? <i>Jana Arsovska</i>	211
iminology	87	22 Hong Kong triads <i>Yiu Kong Chu</i>	226
research	98	23 Ants moving houses – cross-border drug trafficking in the Golden Triangle <i>Sheldon X. Zhang and Ko-lin Chin</i>	237
	107	24 The production of ecstasy in the Netherlands <i>Melvin R. J. Soudijn and Matthijs F. J. Vijlbrief</i>	248
	109	25 Drug violence in Colombia <i>Gipsy Escobar</i>	260
national	112	26 The basics of terrorism and counterterrorism <i>Mustafa Cosar Unal</i>	274
	125	27 The ambivalent role of Italian prosecutors and their resistance to 'moral panics' about crime <i>Riccardo Montana and David Nelken</i>	286
	134	PART III	
		Criminology and criminal justice in context	297
	142	28 Introduction to country assessments <i>Rosemary Barberet</i>	299
	153	29 Australia: the state of criminology <i>Judy Putt and Jade Lindley</i>	302
	166	30 Brazil: the state of criminology <i>Corinne Davis Rodrigues</i>	313
	178	31 Canada: the state of criminology <i>André Solecki, Nicole Crutcher, and Stephen Mihorean</i>	324
	192	32 Cambodia: a criminal justice system in transition <i>Roderic Broadhurst and Chenda Keo</i>	338

7	A question of good governance? Developments in crime prevention internationally	64	Jacqui Karn
8	Transferring Western theory: a comparative and culture-sensitive perspective of crime research in China	77	Lening Zhang
9	The legacy of INTERPOL crime data to cross-national criminology	87	Rosemary Barberet
10	Research methods overview: the missing pieces of rigorous research	98	Cindy J. Smith
PART II			
Special topics			
11	Introduction to special topics in international criminology	109	Sheldon X. Zhang
12	The impact of United Nations crime conventions on international cooperation	112	Matti Joutsen
13	The United Nations and criminology	125	Stawomir Marek Redo
14	International criminal courts	134	Harry M. Rhea
15	International identity crime	142	Russell G. Smith
16	Cybercrime and online safety in cyberspace	153	Roderic Broadhurst and Kim-Kwang Raymond Choo
17	Immigration and criminology	166	William F. McDonald
18	Trafficking in persons	178	Kristina Kangaspunta
19	Trafficking in antiquities	192	Blythe Bowman Proulx
PART III			
Criminology and			
20	Trafficking of "commodities" in crime prevention	64	Dina Siegel
21	Conceptualizing and operationalizing	77	Jana Arsovska
22	Hong Kong triads	87	Yin Kong Chiu
23	Ants moving houses	98	Sheldon X. Zhang
24	The production of crime	107	Melvin R. J. Soudry
25	Drug violence in	109	Gipsy Escobar
26	The basics of terrorism	112	Mustafa Cosar Ulu
27	The ambivalent	125	Ricardo Montano
28	Introduction to	134	Rosemary Barberet
29	Australia: the state	142	Judy Pitt and Jacqui Karn
30	Brazil: the state	153	Corinne Davis R
31	Canada: the state	166	Andre Solecki, N
32	Cambodia: a cr	178	Roderic Broadhurst

Contents

33	Chile: a criminological approach <i>Joanna Heska</i>	349
34	Colombia: crime trends, criminal justice, and criminology in a society in turmoil <i>Gipsy Escobar</i>	360
35	Estonia: crime, criminal justice, and criminology in a changing socio-economic context <i>Anna Markina</i>	376
36	Ghana: the state of criminology in a changing society <i>Obi N. I. Ebbé</i>	390
37	Great Britain: criminology and criminal justice <i>Anne Brunton</i>	400
38	Hong Kong: the state of criminology <i>Jianhua Xu</i>	411
39	India: the state of criminology in a developing nation <i>Prasanna Poornachandra</i>	419
40	Italy: an overview of criminology <i>Rosemary Serra</i>	429
41	South Korea: current trends and issues in crime and criminal justice <i>Joon Oh Jang and Kyung-shick Choi</i>	440
42	Mexico: the state of criminology and public safety <i>Mario Arroyo Juarez and Veronica Martinez Solares</i>	452
43	Nigeria: social structure, criminal justice and criminology <i>Innocent Chukwuna</i>	463
44	The Netherlands: the state of criminology <i>Melvin R. J. Soudijn</i>	475
45	People's Republic of China: the state of criminology <i>Liu Xiu and Jiang Tingyao</i>	486
46	Russia: an overview of crime and criminology <i>Yakov Gillsnitsky</i>	497

Index

47	Sierra Leone: the q <i>Christopher E. S. W</i>	
48	Turkey: the state o <i>Ali Ozdoğan</i>	

349	47 Sierra Leone: the quest for justice and social cohesion <i>Christopher E. S. Warburton</i>	509
360	48 Turkey: the state of criminology <i>Ali Özdoğan</i>	520
	<i>Index</i>	531
376		
390		
400		
411		
419		
429		
440		
452		
463		
475		
486		
497		

Foreword

Knowledge in international and comparative criminal justice and criminology has grown considerably since Gerhard O. W. Mueller and I first started teaching at Rutgers in 1974. In the early days, the publisher of our textbook, *Criminology* (1991), thought it was unnecessary to devote a whole chapter to comparative and international criminology. When Elmer H. Johnson edited the *International Handbook of Contemporary Developments in Criminology* in 1983, world criminology and comparative criminal justice were struggling for their place among other disciplines. Johnson described the field as being handicapped by "ethnocentricity." His two-volume text provided seven chapters on the state of criminology throughout the world (e.g. the United Nations, international organizations, feminist and radical criminology perspectives) and forty country chapters. The authors were invited to focus on, "What is criminology?" The responses varied widely based on contributors' placement in education and in the field.

Change, however, has occurred over the last thirty years since Johnson's text. Criminology and criminal justice have moved into the spotlight in many ways. In the United States, the international divisions of both the Academy of Criminal Justice Sciences and the American Society of Criminology have grown from a handful to one of the largest divisions of each organization. The luncheons that provide the networking opportunities for academics have grown from a table of close friends to a reception of over one hundred. In Europe, the British Society of Criminology (1985) and the European Society of Criminology (2000) were founded. In similar fashion, other countries and regions developed professional societies, including the Indian Society of Criminology (1970) and the Asian Criminological Society (2009). Articles on comparative or international research, virtually impossible to publish in the past, now appear in a growing number of internationally focused journals. Criminologists are increasingly being consulted on policy issues. The change started to become visible in the 1970s in the United Nations where Mueller served as the Chief of the Crime Branch, reaching out to academics and non-governmental organizations for knowledge building and assistance and in the American Society of Criminology's work with the United States Attorney General Janet Reno during my presidency. Yes, we have made great strides, but we have not moved along rapidly enough to keep up with the globalization of crime. Other academic and practitioner fields, such as business, economics, and health care, have been racing forward. Unfortunately, Johnson's ethnocentricity is still very much alive in many countries and many universities in the field of criminology and criminal justice. Only a handful of universities have degree programs in international criminology or criminal justice and many universities around the world do not recognize criminology as a field of study.

International criminology can no longer be seen as a luxury for those who have achieved sufficient status to enable them to travel or as a perk given as a reward for some other activity. Rather, changes need to be made in this growing area of concern. It requires retooling to meet

Foreword

the needs of those who have not had the good fortune to be mentored by international criminologists. It requires that students seek out an international mentor and take advantage of international educational opportunities, such as the study abroad semester, the summer course abroad, an international internship, a placement at the United Nations, or the Fulbright program. Universities across the country are rapidly including these overseas opportunities in their curriculum offerings to ensure that their students are given an advantage in obtaining future career goals.

This text is an important step in this preparatory process. The book is divided into three parts. The first part, *Methods and theories*, introduces the reader to the challenges of research and theory building in comparative/international settings. The progress and problems are well documented and thought provoking. Part II, *Special topics*, offers a comprehensive insight into the broad range of our rapidly increasing transnational crime problems and the attempt on the part of international bodies to deal with them. The third part, *Criminology and criminal justice in context*, offers a unique discussion of worldwide criminology. Here we get a most intriguing look at the state of the art of criminology in twenty countries spread around the globe (with the authors' wise caution that definitions and cultural contexts dictate the need for careful comparison). Each of the chapters ends with five research questions that will guide the readers to areas of research that will enable them to move forward in our pioneering efforts in this challenging new perspective. The foremost scholars in the field of international/comparative criminology have assembled chapters that, when taken together, yield a comprehensive update and thorough analysis of the globalization of crime. It answers many questions, but it raises more. It calls on us to further assess international criminology and to map out its future directions.

Freda Adler
Director, Master of Science in Criminology, University of Pennsylvania
Visiting Professor, Department of Criminology, University of Pennsylvania
Professor Emeritus, Rutgers University

Printed and bound in Great Britain by
CPI Antony Rowe, Chippenham, Wiltshire

First published 2011 by Routledge
2 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN
Simultaneously published in the USA and Canada
by Routledge
711 Third Avenue, New York, NY 10017
Routledge is an imprint of the Taylor & Francis Group, an informa business

© 2011 Cindy J. Smith, Sheldon X. Zhang, and Rosemary Barbaret; individual chapters,
the contributors

The right of Cindy J. Smith, Sheldon X. Zhang, and Rosemary Barbaret to be identified as
editors of this work has been asserted by them in accordance with the Copyright, Designs
and Patents Act 1988.

All rights reserved. No part of this book may be reprinted or reproduced or utilised in any
form or by any electronic, mechanical, or other means, now known or hereafter invented,
including photocopying and recording, or in any information storage or retrieval system,
without permission in writing from the publishers.

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library
Library of Congress Cataloguing in Publication Data

Routledge Handbook of International Criminology / edited by Cindy J. Smith,
Sheldon X. Zhang, and Rosemary Barbaret.

1. Criminology. 2. Crime. I. Smith, Cindy J. II. Zhang, Sheldon.
III. Barbaret, Rosemary. IV. Title: Handbook of International Criminology.
HV6025.R68 2011
364 – dc22
2010040654

ISBN: 978-0-415-77909-8 hbk
ISBN: 978-0-203-86470-8 ebook
Typeset in Bembo
by Keystroke, Station Road, Codsall, Wolverhampton

In his memory

We dedicate this col-
to the man who star-
with his *International
Contemporary Develop*
Elmer H. Johnson

Notes on contributors

Editor biographies

Cindy J. Smith, Ph.D., is a retired faculty member of the University of Baltimore, Maryland, USA. She is the former Chief of the International Center at the National Institute of Justice (2006–8), a Senior Fulbright Research Scholar in Turkey (2005–6), Director of the Master's in Criminal Justice Program (2001–5), and Chair of the International Division of the American Society of Criminology (2005–9). Her research interests include terrorism, human trafficking, corrections, sex offenders, and comparative methodology.

Sheldon X. Zhang, Ph.D., is Professor of Sociology at San Diego State University. His research interests include community corrections and reintegration, and transnational organized crime. His works have appeared in such journals as *Criminology*, *British Journal of Criminology*, and *Crime and Delinquency*. He has published two books on human smuggling topics: *Chinese human smuggling organizations – families, social networks, and cultural imperatives* (Stanford University Press, 2008) and *Smuggling and trafficking in human beings: all roads lead to America* (Praeger, 2007).

Rosemary Barberet, Ph.D., is an associate professor in the Sociology Department of John Jay College of Criminal Justice in New York City, USA., and directs the Master's Program in International Crime and Justice. She has spent most of her academic career in Europe (Spain and England) and is fluent in Spanish and French. Her publications have dealt with youth crime, victimology, crime indicators, and comparative methodology. From 2001–5 she chaired the International Division of the American Society of Criminology (ASC). In 2006 she received the Herbert Bloch Award of the ASC, as well as the Rafael Salillas Award of the Sociedad Española de Investigación Criminológica.

Contributor biographies

Freda Adler, Ph.D. is a visiting professor and the Director of the Master of Science Program in Criminology at the University of Pennsylvania, and Professor Emeritus at Rutgers University. She is a world renowned leader of international criminology. The Freda Adler Distinguished International Scholar Award of the Division of International Criminology of the American Society of Criminology is named in honor of her work in advocating for an international perspective in all work and her knowledge building to internationalize criminology around the world. Her publication list is extensive with over 130 books and papers.

Mario Arroyo Juarez, Ph.D., is an expert in security and crime reduction. He holds a Ph.D. in Sociology from the National Autonomous University of Mexico (UNAM), and an MSc. in

criminal justice policy from the London School of Economics and Political Science, UK. Currently, he is a researcher on strategic intelligence at the Tecnológico de Monterrey in Mexico.

Jana Arsovska, Ph.D., a native of Macedonia, is an assistant professor at the Sociology Department at John Jay College of Criminal Justice (CUNY) in New York City, USA. She holds a Ph.D. degree in criminology from the Catholic University of Leuven in Belgium where she studied ethnic Albanian organized crime. She has published widely on Balkan criminal networks.

Roderic Broadhurst, Ph.D., is Professor at the Australian Research Council Centre of Excellence in Policing and Security (CEPS), School of Regulation, Justice and Diplomacy, College of Asia and the Pacific, Australian National University. He is currently engaged in research for CEPS on "illicit organizations" and "investigative practices" as well as on crime in Cambodia, Hong Kong, and China.

Anne Brunton, Ph.D., has professional qualifications in law and a background in social policy. She has experience of working with vulnerable groups such as care leavers, drug users, and young offenders. Until recently she was Director of the British Society of Criminology and an associate lecturer in criminology at the London School of Economics and Political Science. She is now a senior lecturer in criminology and policing at Buckinghamshire New University.

Ko-jin Chin, Ph.D., is Professor II (Distinguished) at the School of Criminal Justice at Rutgers University-Newark. He is the author of *Chinese subculture and criminality: non-traditional crime groups in America; Chinatown gangs: extortion, enterprise, and ethnicity; Smuggled Chinese: clandestine immigration to the United States; Heijun: organized crime, business, and politics in Taiwan; and Golden triangle: inside Southeast Asia's drug trade.*

Kyung-shick Choi, Ph.D., is an assistant professor in the Criminal Justice Department at Bridgewater State University, USA. He also facilitates the UN Virtual Forum against Cybercrime as a lecturer. He received his Ph.D. in criminology from Indiana University of Pennsylvania, USA. His scholarly interests focus on the study of cybercrime and theory testing.

Kim-Kwang Raymond Choo, Ph.D., is a senior research lecturer at the University of South Australia, and the recipient of a number of awards including the 2010 Australian Capital Territory Pearcey Award, 2010 Consensus IT Professional Award, a 2009 Fulbright Scholarship, and the 2008 Australia Day Achievement Medallion. He was nominated as one of 100 Emerging Leaders in *The Weekend Australian Magazine/Microsoft's Next 100 series.*

Yiu Kong Chu, Ph.D., is an honorary assistant professor in the Department of Sociology of the University of Hong Kong. He is one of the founding members of the Asian Association of Police Studies and the Hong Kong Juvenile Delinquency Research Society. He is conducting research on organized crime and policing.

Innocent Chukwuma is a leading researcher on police, policing, and criminal justice reform in Nigeria, having served as a consultant to the United Nations Office on Drugs and Crime (UNODC), the European Union (EU), and many other agencies, as well as the founder of CLEEN Foundation in West Africa. He is currently the William H. Bloomberg Visiting Lecturer in Public Management at the Harvard Kennedy School, USA.

Cybercrime and online safety in cyberspace

Roderic Broadhurst and Kim-Kwang Raymond Choo

Introduction

Information and communications technologies (ICT) have become a crucial element in our day-to-day activities. This is hardly surprising as the proliferation of ICT and connectivity of the Internet in today's information age open the door to increased productivity, faster communication capabilities, and immeasurable convenience. Unfortunately, our increased dependence on ICT and the pervasive interconnectivity of our ICT infrastructure also expose us to an evolving spectrum of cyber-threats.

Cybercrime is essentially a transnational crime with a "modus operandi" that exploits interstate differences in the capacity to respond to such crime, and appears in the same company as such powerful global concerns as civil war, genocide, and poverty (United Nations, 2004). This transnational characteristic provides cybercriminals, especially organized crime, with the ability to avoid countermeasures even when implemented by capable actors (Brenner, 2002, 2006; Council of Europe, 2004). Although some have questioned the existence of organized criminal activities in cyberspace, several studies have noted the potential and actual synergy between organized crime and cyberspace in recent years. McCusker (2006, p. 257), for example, suggested that "cybercrime has become an integral part of the transnational threat landscape, and conjures up pressing images of nefarious and increasingly complex online activity."

Choo (2008) outlined three categories of organized groups in cyberspace:

1. Traditional organized crime groups which make use of ICT to enhance their terrestrial criminal activities;
2. Organized cybercriminal groups which operate exclusively online; and
3. Organized groups of ideologically and politically motivated individuals who make use of ICT to facilitate their criminal conduct.

These forms of organized crime look to exploit cyberspace in a number of different ways by committing a wide range of crimes that may be conducted or enhanced by computer and digital devices.

Cybercrime offenses

Although there is no definitive list of what constitutes cybercrime or computer-related crime, the following presents the typical scope of offenses that occur in cyberspace.

1. Telecommunications theft and illegal interception
2. Piracy copyright theft
3. Cyber stalking
4. Electronic money laundering and tax evasion
5. Electronic vandalism, cyber-terrorism, denial of service, extortion
6. Sales and investment fraud, forgery (classic pyramid schemes)
7. Electronic funds transfer fraud and counterfeiting (carding, identity theft and misrepresentation)
8. Content crime – offensive materials
9. Espionage
10. Resource theft – illegal use of personal computers (PCs) or other digital devices

Cybercrime ranges across a wide spectrum of activities and behaviors: at one end are crimes that involve fundamental breaches of personal or corporate privacy, such as assaults on the integrity of information held in digital depositories, identity theft, and the use of illegally obtained digital information to blackmail a firm or individual. Midway along the spectrum are transaction-based crimes such as fraud, trafficking in child pornography, digital piracy, money laundering, and counterfeiting. These are specific crimes with specific victims, but the offender hides in the relative anonymity provided by the Internet. Another aspect of this type of crime involves those that deliberately alter data for either profit, or personal or political objectives. At the other end of the spectrum are those crimes that involve attempts to disrupt the actual workings of the Internet. These include spamming, hacking, and denial of service attacks against specific sites to acts of cyber-terrorism by non-state actors – that is, the use of the Internet to affect a nation's economic and technological infrastructure and cause public disorder or disturbances and even death (Broadhurst and Chandler, 2006).

The threat environment

Cyberspace provides criminal actors a safe haven that enhances their organizational and operational capabilities. Information security and associated laws and policy are also less well developed in emerging economies, thus providing an environment in which criminal activities can be conducted at lower risk but still have an impact on advanced economies (Choo *et al.*, 2007). Such threats are increasingly important and strategically relevant (Rudd, 2008). For example, a 2008 report of the Centre for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency began with a central finding: "The United States must treat cyber-security as one of most important national security challenges it faces" (CSIS, 2008). A 2009 Australian Defence white paper also voiced similar concerns.

ICT advances have undeniably changed the way criminals conduct their activities, and policing also needs to adapt enforcement strategies that reflect changes in society. With the increasing digitalization of information, "policing will be carried out over a borderless community, rather than within the confines of national boundaries" (Sim, 2000, p. 116).

Data breaches

Almost every business in developed economies makes use of the Internet. As businesses continue to engage in electronic commerce, they will become increasingly globalized and interconnected and the level of data being created by society is set to increase. In terms of the future threat landscape, it is argued that the increased variety and volume of attacks are inevitable given transnational crime networks' desire to obtain personal and confidential information. Not all criminal misuse of computers or digital devices involves hacking, since passwords, PIN (personal identification numbers), and other protective codes can be obtained by "social engineering"¹ to gain access then erase, modify, or copy the information to suit the needs of their attack (Guenther, 2001). Non-physical data breaches (e.g. due to computer or network intrusions) are a cause for concern. According to the data breach investigations conducted by Verizon Business from 2004 to 2008, for example, only 9 percent of the 90 data breaches (involving 285 million compromised records) were attributed to physical attacks. In the Verizon investigations, hacking is one of the leading causes of data breaches (64 percent of cases) and reportedly a favored technique of cybercriminals, and "unauthorized access via default, shared, or stolen credentials constituted more than a third of the entire Hacking category and over half of all compromised records" (Verizon, 2009, p. 16).

The involvement of organized crime groups in computer or network intrusions such as hacking and unauthorized access to obtain sensitive information now emphasizes the importance of large-scale profit-driven incentives. As noted by Peretti (2009, p. 379), a Senior Counsel with the United States Department of Justice's Computer Crime and Intellectual Property Section, "compromise of credit and debit card account information most often results in the type of identity theft referred to as 'account takeover,' which involves fraud on existing financial accounts." For example in a recent case in the United States, two accused persons were indicted on charges of "unlawfully, intentionally, and knowingly, acting in interstate and foreign commerce," via access of a computer and "thereby obtaining information from a protected computer for the purposes of commercial advantage and private financial gain." According to court documents, both accused persons (and others known and unknown) "allegedly participated in a scheme to steal funds from bank and brokerage accounts by hacking into those accounts through the Internet, using personal financial information obtained through computer viruses" (*United States of America v. Alexander Bobnev and Alexey Mineev*).² The accused persons subsequently sent a portion of the stolen funds to their associates in Russia using money-remitting services after keeping a portion of the fraud proceeds for themselves.

Internet frauds, scams, and phishing

In online or Internet scams, cybercriminals approach potential victims across the globe by sending unsolicited messages purporting to originate from legitimate organizations in order to deceive individuals or organizations into disclosing their financial and/or personal identity information. Information obtained from "phishing"³ and other illegal means is often for the purpose of using it to commit or facilitate crimes such as financial fraud and identity theft. A 2008 Gartner survey of 4,988 American adults, for example, indicated that top causes for financial fraud against consumers and payment card frauds are data breaches at a retailer, government agency or other, and third party phishing (Litan, 2009). The biennial KPMG fraud survey of 420 organizations in Australia and New Zealand reported similar findings. Within the financial services sector, credit card fraud accounted for 39 percent of the value of fraud attributable to external parties. Fraudulent access to financial services' accounts (by adopting the identity of the account holder

by "phishing" or "Trojan horse" attacks over the Internet) amounted to 31 percent of the total value attributable to external parties (KPMG Forensic, 2009, p. 13). Several researchers and security practitioners have also suggested the involvement of organized crime groups in phishing scams and messages are increasingly targeting top company executives – also known as "spear phishing" or "whaling" in reference to bigger "fish" (Choo and Smith, 2008).

Organized crime groups have also been known to use identity fraud to either conceal their identities to evade detection and protect their assets from confiscation or as an enabler to commit various frauds and other crimes. Internet frauds and scams include "advance fee" frauds (also known as "419" cases named after the relevant section of the Nigerian Criminal Code), online auction frauds, and identity and payment card frauds. These take many forms but include enticements to use your bank account to deposit the plunder of a former despot in Africa, administrative fees to transfer a huge lottery pay-out (for which you strangely cannot remember buying a ticket), or the bond money and advance rent for a non-existent but reasonably priced apartment suitable for an international student, and so on. Out of 275,284 complaints to the Internet Crime Complaint Centre in 2008, 26.5 percent or 72,940 cases were reported to US law enforcement; online auction fraud accounted for 25.5 percent of the reported cases and 16.3 percent of the total loss; payment card fraud accounted for 9 percent of cases and 4.7 percent of the total loss; and Nigerian advance fee scam accounted for 2.8 percent of cases and 5.2 percent of the total loss. The total monetary loss from all reported cases of Internet fraud and scams to United States law enforcement agencies in 2008 was \$264.6 million USD – an increase of 10 percent from 2007 (NW3C, 2009).

Malware creation and dissemination

McAfee (2008)'s virtual crime report indicated that cybercriminals are increasingly exploiting vulnerabilities in software and applying social engineering to spawn a broad range of threats including spyware, phishing, adware, rootkits,⁴ and botnets. In 2008, Symantec (2009, p. 15) reported that new malicious code had increased by 265 percent since 2007 and 60 percent of all current malicious code was detected in 2008.

Malware⁵ is software designed to infiltrate, compromise security, or damage a computer system, without the owner's informed consent and includes viruses, worms,⁶ backdoors, keyloggers, and trojans. The 2008 UK Threat Assessment report observed that "most new malware is designed to steal financial data (such as credit card details, bank account details, passwords, and PINs) as a precursor to various frauds and other deceptions" (SOCA, 2008, p. 9). An example of information stealing malware is keylogging programs that are designed to monitor user activity including keystrokes. This can then be used by cybercriminals to steal passwords or credit card details, which can then be used for malicious purposes such as identity/online fraud. An example of a "keylogger" case was the attempted theft of more than £229m from Sumitomo Matsui Banking Corporation in London. Three individuals were extradited to the UK from Belgium and Spain and £1.5m in assets was (reportedly) restrained (SOCA, 2009).

McAfee (2005) estimated that the number of potentially malicious threats emerging each month increased from roughly 300 to 2,000 between 2003 and 2005, largely due to the growth of bot-malware.⁷ Sophos (2006), an IT security company, noted that an unpatched computer without antivirus protection or a firewall would have a 50 percent chance of becoming a zombie within 30 minutes of being connected to the Internet. Bot malware are often surreptitiously forwarded to victims by various means, such as via email attachments, peer-to-peer (P2P) networks, and visits to an infected website. Building botnets requires minimal levels of expertise

(Ianneli and Hackworth, 2005; Choo, 2007). Bot malware typically takes advantage of system vulnerabilities and software bugs or hacker-installed backdoors that allow malicious code to be installed on computers without the owners' consent or knowledge.

Compromised computers (also known as bots) are then turned into zombies. The shift in motivation from curiosity and fame seeking to illicit financial gain has been marked by a growing sophistication in the evolution of bot malware, as illustrated by recent examples of detected bot malware such as Conficker. Conficker has received a considerable amount of media attention, and has been reported to have successfully infiltrated government networks, home PCs, critical infrastructure, and universities (Porras *et al.*, 2009). According to analysis of the Conficker and its variants (Conficker B and C) by Sophos and the Malware Threat Centre at SRI International, Conficker was designed to provide a secure binary updating service that effectively allows the bot malware designer instant control of millions of PCs. The design included sophisticated defensive mechanisms such as binary encryption methods and compiler-level code obfuscation to hinder detection by anti-malware software. Reverse engineering was made more difficult for investigators analyzing the malware (Porras *et al.*, 2009; Fitzgibbon and Wood, 2009).

Compromised computers – zombies – can then be used as remote attack tools or to form part of a botnet under the control of the botnet controller. According to Symantec (2009), bot networks accounted approximately 90 percent of all spam email in 2008. A 2008 report by McAfee also stated that:

the number of compromised zombie PCs in botnets has quadrupled in the last quarter alone and that these are capable of flooding the Internet with more than 100 billion spam messages per day . . . [and] are increasingly switching to phishing, distributed denial of service (DDoS) and website attacks which are capable of causing a huge amount of damage and are a growing threat to the security of nations, the national information infrastructure, and the economy
(McAfee, 2008, p. 5)

Although malware are still disseminated using conventional tools such as email, cybercriminals have turned recently to exploiting browser plug-in and webserver vulnerabilities. A large number of commercial, government, university, and other high-profile and high-traffic websites worldwide apparently may have been successfully compromised to allow "infection" of unwitting visitors with malware. For example in May 2009, the UK regional director of Finjan, an IT provider of secure web gateway solutions, noted that a botnet discovered by the company in February 2009 contained 1.9 million infected computers including 73 government domains (Raywood, 2009). Similarly in the first quarter of 2009, McAfee (2009, p. 3) reported an increase in the number of malicious websites created and "sites that host malware— with thousands of new sites appearing daily." They also discovered a search-engine-optimization ring that targeted the top Google search terms to enable the installation of anti-virus software. Business, government, and individual householders need to be aware of risk mitigation strategies and implement and update them because search engine optimization will continue to be one of the most sought after attack vectors by criminals.

Responses and countermeasures

The threat of cybercrime has given rise to a demand for strategies for prevention and control, particularly in the area of organized crime in cyberspace. Some of the key approaches reduce opportunities for the commission of cybercrime, making such activities more difficult to commit, increasing the risks of detection, enhancing the level and certainty of sanctions, and reducing the

to be obtained concerning each of the thousands of computers that have been compromised – a gargantuan task. Thus a new offense category, such as creating a network for illegal purposes and selling/renting established botnets (networks of compromised computers) to commit or facilitate criminal activities, could be developed to deal with these threats.

The true impact of cybercrime is unknown due to poor detection and under-reporting, but cybercrime prosecutions involving multiple jurisdictions will be an essential response (Broadhurst and Grabosky, 2005; Choo *et al.*, 2007). Because online offending easily transcends borders, numerous territories can simultaneously assert jurisdiction, particularly when an attack transits multiple jurisdictions with different regimes for preserving evidence. Timely access to evidence located in one or more foreign jurisdictions may be difficult or impossible, as it would normally require the assistance of authorities in the foreign jurisdiction(s), who may be unwilling or unable to assist. When the suspect is located abroad, these difficulties are compounded. Countering the risks of cybercrime is a multi-dimensional challenge and requires effective coordination and collaborative efforts on the part of a wide range of government and private sector entities. Achieving some uniformity will be an essential strategy to minimize the risk of so-called safe havens and “jurisdiction shopping,” in which offenders seek out countries from which to base their activities that have the least severe punishments or which have currently no extradition treaties.

A recent report by the Commission of the European Communities (2008), for example, highlighted the need to enhance cross-border law enforcement and judicial cooperation in the fight against transnational payment fraud, and improve the response of the UN, INTERPOL, and other international agencies efforts (Dandurand *et al.*, 2007). Nevertheless a review by Microsoft of the criminalization of cybercrime in several Asian jurisdictions⁸ showed that serious gaps continue to exist in the “seamless web” of cyber laws needed to counter cybercrime (Microsoft, 2007). The review applied the CoE Cybercrime Convention bench-mark adopted by Japan and the Philippines and also influential in the development of laws in Thailand and Indonesia (Broadhurst, 2006b). The review noted the poor compliance with model privacy laws. Even for core offenses such as the criminalization of unauthorized access to computers, systems, programs and data some Asian countries had yet to enact laws or provide for civil remedy. Despite widespread public alarm only one jurisdiction met the model laws for online child safety and six countries did not have adequate laws.

Theoretical problems

The absence of settled theory about the interaction of organized crime with cyberspace is an impediment to the development of sound countermeasures. At present, crime prevention practices based on actor choice (cf. neo-classical deterrence theory) are usually applied with variable effect (Grabosky *et al.*, 2001; Newman and Clarke, 2003). Routine activity theory draws on rational exploitation of “opportunity” in the context of the regularity of human conduct (Felson, 1998; Yar, 2005) to design prevention strategies, especially where terrestrial interventions are possible – for example in the transit of goods. This approach assumes criminals are rational and appropriately resourced actors that operate in the context of high-value, attractive targets protected by weak guardians (e.g. ill-managed ISPs and jurisdictions with weak legal enforcement of the Internet). An assumption is that organized crime consists of profit-focused enterprises that seek out opportunities provided by cyberspace, and acquire the necessary resources for cybercrime by (inter alia) using delinquent IT professionals and targeting weakly protected computers/networks or other digital devices. Consequently, deterrence (increased penalties and detection) is the preferred policy response enhanced by appropriately trained police (capable guardians) and target “hardening.”

The myriad motivations of offenders requires no elaboration in the rational-choice model, and prevention strategies should be as effective against terrorists using the Internet as they would be for individual "hackers" seeking reputation, or organized crime seeking illicit gain. However, such an assumption in respect to some forms of cybercrime may be misplaced. There is an absence of evidence-based research about offender behavior and recruitment in cyberspace, although learning and imitation play important roles (Broadhurst, 2005). Hence, organized crime groups cannot be understood from just their illicit activities alone, that is – as rational profit-driven networks of criminal actors, since socio-cultural forces play an important role in the genesis and sustainability of such groups.

Alternative theoretical approaches that posit particular offender motives or pathologies, or the role of social conflict, have not featured widely in explanations of cybercrime. Early accounts of "hackers" emphasized individuality and a non-profit orientation, but also observed the likely shift to profit-oriented misuse as the Internet developed (Chandler, 1996). Indeed the role of social learning and offender pathology has been neglected but may play a significant role in predisposing some actors to criminal activity and risk-taking in cyberspace, where anonymity reduces social surveillance and self-control (Jayawardena and Broadhurst, 2007; Jones, 2007). Hate and so-called "content" crimes perpetrated via the Internet may reflect social or individual pathologies, and less the exercise of rational choice – although it may be "rational" to adopt Internet strategies of dissemination (Broadhurst, 2006a).

Functional approaches assume crime is a normal adaptation to change, and indeed represents a creative response to adversity (usually experienced as different forms of social exclusion) – cybercrime in this sense is normal, although novel in its form. Thus, the cost of suppression of cybercrime may only be achieved by curtailment of the Internet's natural advantages, such as low-cost connectivity. Another approach is to see the rise of certain forms of crime as a result of conflict within society and disputes about what constitutes "real" crime: here, the criminalization of an act represents the exercise of power by elites. Thus, defining behavior as deviant or criminal may represent only sectional interests with little real community support. For example, the practice of illegally copying digital media without paying the copyright holders has only been recently "criminalized," with attendant changes to community attitudes, opportunities for criminals, and policing practice.

Wikström and Treiber (2007, p. 244) noted that in order "to advance criminological theory we need a developed theory of action through which we can address causal mechanisms." Functional, learning, and conflict explanations, as well as choice theories, are often applied to explain organized crime. In the context of cyberspace, we have limited understanding and empirical sources about these "causes" with respect to profit and content forms (e.g. hate crime, child pornography, etc.) of cybercrime. We therefore propose the following:

1. The extent of profit-oriented cybercrime will index organized crime activity in cyberspace, and the more lucrative, the more likely organized crime rather than individual offenders will dominate, and – the corollary that – content-related cybercrime will reflect "pathology" and be dominated by individuals rather than organized crime.
2. Criminal networks operating in cyberspace will tend to be new forms of organized crime rather than traditional "mafia"-like groups. Traditional organized crime will have limited operations and focus on precursor offenses such as identity theft or money laundering.
3. Organized crime operating in cyberspace will trade primarily in the protection of illicit data and information (e.g. compromised credit card and identity details) and will be less likely to be engaged in systematic fraud/deception-related cybercrimes.

Future trends

These propositions use the Internet.

The use of "bots" involved in more sophisticated hacker attacks (Choo, 2008).

The introduction of pumps, ATMs) and this will be the target of includes routers, becoming a major (Instant Messaging) credit card information of-service attacks. that technological a profit-motivated a

Research agenda

A 2007 inquiry in concerns about organized crime & illicit activities in Commission "call" research information (PjCACC, 2007), The importance highlighted by Sin environment was rude shock when of the cybercrime involvement in c factors. Such research designed to address

These propositions offer challenging research questions and are conditioned by the way we see cybercrime evolving with the advent of technological and behavioral changes among those who use the Internet.

Future trends

The use of "bots" is expected to increase in the near future. Botnets are expected to become involved in more sophisticated, targeted attacks and reflect a general trend toward more focused hacker attacks (Choo, 2007). While "syntactic" attacks such as worms and viruses were previously spread to cause disruption and inconvenience, the use of "semantic" or social-engineering methods such as "pharming" are used to steal personal information that may be used to access bank accounts (Choo *et al.*, 2007). Therefore organized crime is expected to adopt this activity and take a more active role in future cyber crime. There will be a shift in targets from desktop computers to smart devices (i.e. cellular phones, Blackberrys) and other such Internet-linked personal organizers partly due to the ordinary user's inclination to store confidential information such as bank PINs on such devices. These are expected to become the next prime target for attacks (Chantler and Broadhurst, 2008; Choo *et al.*, 2007).

The introduction of commercial appliances linked to the Internet (e.g. vending machines, gas pumps, ATMs) and the increased usage of mobile phones to pay for such products suggests that this will be the target of malware in the future. Other non-PC devices will also be targeted. This includes routers, switches and backup devices. Furthermore, real-time programs such as IM (Instant Messaging) are likely to be increasingly targeted in the near future and are rapidly becoming a major risk vector (Choo *et al.* 2007). There appears to be a trend towards a greater emphasis on the development of semantic/human intelligence methods rather than the syntactic measures. This is due to semantic methods placing value on particular types of information (i.e. credit card information) rather than the use of syntactic methods to release viruses and denial-of-service attacks. Human-based social engineering is able to obtain information in many cases that technological methods are unable to. This further illustrates the changing trend towards profit-motivated attacks and the involvement of organized crime (Chantler and Broadhurst, 2008; Choo, 2008).

Research agenda

A 2007 inquiry into the future impact of serious and organized crime on Australian society raised concerns about "the increasing use of technology, transnational connections and fluidity of organized crime groups [that] will make law enforcement's task of policing organized crime's illicit activities more difficult" (PJCACC, 2007, p. 28). In the inquiry, the Australian Crime Commission "called for a greater involvement and contribution by academia to the body of research informing Australia's policy and operational choices in fighting organized crime" (PJCACC, 2007, p. 78).

The importance of looking ahead to future offending in the online environment was highlighted by Smith *et al.* (2004, p. 156) who, only seven years ago, noted that crime in the digital environment was prone to rapid change and "those who fail to anticipate the future are in for a rude shock when it arrives." An urgent research project would be to launch region-wide studies of the cybercrime threat environment that aim to address the impact of organized crime involvement in cybercrime, the nature of new variants of cybercrime and the response of regulators. Such research would need to entail an extensive multi-method approach to data collection designed to address the future research questions identified in the next section. Such an agenda

- Brenner, S. W. (2002) Organized cybercrime? How cyberspace may affect the structure of criminal relationships. *North Carolina Journal of Law & Technology*, 4(1): 1–50.
- (2006). Cybercrime jurisdiction. *Crime, Law and Social Change*, 46: 189–206.
- Brenner, S. W. and Frederiksen, B. A. (2002). Computer searches and seizures: some unresolved issues. *Michigan Telecommunications & Technology Law Review*, 8: 39–114.
- Broadhurst, R. G. (2005). International cooperation in cyber-crime research. Paper presented at the 11th UN Congress on Crime Prevention and Criminal Justice, Workshop 6: Measures to Combat Computer Related Crime, Bangkok, April.
- (2006a). Content cybercrimes: criminality and censorship in Asia. *Indian Journal of Criminology*, 34(1&2): 11–30.
- (2006b). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies and Management*, 29(3): 408–33.
- Broadhurst, R. G. and Grabosky, P. (2005). Computer-related crime in Asia: emergent issues. In R. Broadhurst and P. Grabosky (Eds.), *Cybercrime: the challenge in Asia*, pp. 347–60. Hong Kong: University of Hong Kong Press.
- Broadhurst, R. G. and Chandler, A. (2006). Cybercrime update: trends and developments, In *Expert Group Meeting on the development of virtual forum against cybercrime report*, June 28–30, 2006, Seoul Korea, KICJP and UNODC, pp. 21–56.
- Center for Strategic and International Studies (CSIS). (2008) *Securing cyberspace for the 44th presidency*. Washington, DC: Center for Strategic and International Studies.
- Chantler A. (1996). *Risks, the profile of computer hackers*. PhD thesis. Curtin University, unpublished.
- Chantler A. N. and Broadhurst, R. (2008). Social engineering and crime prevention in cyberspace. Paper presented to the Korean Institute of Criminology, October 30, Seoul.
- Choo, K. K. R. (2007). Zombies and botnets. *Trends & Issues in Crime and Criminal Justice*, 333. Canberra: Australian Institute of Criminology. Online at <http://www.aic.gov.au/publications/current%20series/tandi/321-340/tandi333.aspx> (accessed July 31, 2009).
- (2008). Organized crime groups in cyberspace: a typology. *Trends in Organized Crime*, 11(3): 270–95.
- (2009). *Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences*. Research and public policy series no. 103. Canberra: Australian Institute of Criminology. Online at <http://www.aic.gov.au/en/publications/current%20series/rpp/101-20/rpp103.aspx> (accessed July 31, 2009).
- Choo, K. K. R. and Smith, R. G. (2008). Criminal exploitation of online systems by organized crime groups. *Asian Journal of Criminology*, 3(1): 37–59.
- Choo, K. R. R., Smith, R. G., and McCusker, R. (2007). *Future directions in technology-enabled crime: 2007–09*. Research and public policy series no. 78. Canberra: Australian Institute of Criminology. Online at <http://www.aic.gov.au/publications/current%20series/rpp/61-80/rpp78.aspx> (accessed July 31, 2009).
- Cooke, E., Jahanian, F., and McPherson, D. (2005). The zombie roundup: understanding, detecting, and disrupting botnets. In *SRUTY'05 Workshop Proceedings*, pp. 35–44. Berkeley CA: USENIX Association.
- Council of Europe. (2004). Summary of the organized crime situation report: focus on cybercrime. Octopus Interface conference: challenge of cybercrime, September 15–17, Strasbourg.
- Dandurand, Y., Colombo, G., and Passas, N. (2007). Measures and mechanisms to strengthen international cooperation among prosecution services. *Crime, Law and Social Change*, 47(4–5): 261–89.
- Felson, M. (1998). *Crime and everyday life*. New York: Pine Forge Press.
- Fitzgibbon N. and Wood, M. (2009). *Conficker C: a technical analysis*. Online at http://www.sophos.com/sophos/docs/eng/marketing_material/conficker-analysis.pdf (accessed July 31, 2009).
- Grabosky P. (2007). Requirements of prosecution services to deal with cyber crime. *Crime, Law and Social Change*, 47(4–5): 201–23.
- Grabosky, P. and Broadhurst, R. G. (2005). The future of cyber-crime in Asia. In R. G. Broadhurst and P. Grabosky (Eds.), *Cybercrime: the challenge in Asia*, pp. 347–60. Hong Kong: University of Hong Kong Press.
- Grabosky, P., Smith, R. G., and Dempsey, G. (2001). *Electronic theft: unlawful theft in cyberspace*. Melbourne: Cambridge University Press.
- Guenther, M. (2001). Social engineering – security awareness series. UK: Information Warfare Site. Online at <http://www.iwar.org.uk/comsec/resources/sa-tools/Social-Engineering.pdf> (accessed December 20, 2006).
- Ianelli, N. and Hackworth, A. (2005). *Botnets as a vehicle for online crime*. Pittsburgh: CERT Coordination Center.

- Jayawardena, K. and Broadhurst, R. (2007). Online child sex solicitation: exploring the feasibility of a research "sung." *International Journal of Cyber Criminology*, 1(2), pp. 228-48.
- Jones, B. (2007). Comment: virtual neighborhood watch: open source software and community policing against cybercrime. *Journal of Criminal Law & Criminology*, 97(2), 601-29.
- KPMG Forensic. (2009). *Fraud survey 2008*. Australia: KPMG.
- Litan, A. (2009). 2008 data breaches and financial crimes scare consumers away. Stamford: Gartner.
- McAfee (2005). *McAfee virtual criminality report*. Santa Clara: McAfee.
- (2007). *Cybercrime: the next wave*. Santa Clara: McAfee.
- (2008). *McAfee virtual criminality report: cybercrime versus cyberlaw*. Santa Clara: McAfee.
- (2009). *McAfee threats report: first quarter 2009*. Santa Clara: McAfee.
- McCusker, R. (2006) *Transnational organized cyber crime: distinguishing threat from reality*. *Crime, Law and Social Change*, 46(4-5): 257-73.
- Microsoft (2007). *Asia Pacific legislative analysis: current and pending online safety and cybercrime laws*. A study by Microsoft. November. Online at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/microsoft.asia.pacific_legislative_analysis.pdf (accessed July 31, 2009).
- Morris, S. (2004). The future of netcrime now: part 1 - threats and challenges. UK: Home Office. Online at <http://www.homeoffice.gov.uk/rds/pdfs04/rds046204.pdf> (accessed July 31, 2009).
- National White Collar Crime Center (NW3C). (2009). *2008 Internet crime report*. Online at http://www.nw3c.org/downloads/2008_IC3_Annual%20Report_3.27.09_small.pdf (accessed July 31, 2009).
- Newman, G. and Clarke, R. (2003). *Superhighway robbery: preventing e-commerce crime*. Devon: William Publishing.
- Parliamentary Joint Committee on the Australian Crime Commission (PJACC). (2007). *Inquiry into the future impact of serious and organized crime on Australian society*. Canberra: Parliament House.
- Pereira, K. K. (2009). Data breaches: what the underground world of "carding" reveals. *Santa Clara Computer and High Technology Law Journal*, 25(2): 375-414.
- Portas, P., Saidi, H., and Yegneswaran, V. (2009). *An analysis of Conficker C*. Online at <http://mtc.sri.com/Conficker/addendumC/> (accessed July 31, 2009).
- Raywood, D. (2009). Botnet discovered by Finjan contained 73 government domains. Online at <http://www.scmagazineuk.com> (Accessed 31 July, 2009).
- Rudd, K. (2008). Address by the Prime Minister of Australia The Hon. Kevin Rudd MP, 4 December.
- Serious Organized Crime Agency (SOCA). (2008). *The United Kingdom threat assessment of serious organized crime*. Online at <http://www.soca.gov.uk/assessPublications/downloads/UKTA2008-9NPM.pdf> (accessed July 31, 2009).
- (2009). *Serious organized crime. Agency annual report 2008/9*. Online at http://www.soca.gov.uk/assessPublications/downloads/SOCA_AR_2009.pdf (accessed July 31, 2009).
- Sim, S. H. (2000). Effective countermeasures against economic crime and computer crime. Resource material series no. 55. Tokyo, Japan: United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders. pp: 103-16.
- Sheptycki, J. (2004). Organizational pathologies in police intelligence systems: some contributions to the lexicon of intelligence-led policing. *European Journal of Criminology*, 1(3): 307-32.
- Smith, R. G., Grabosky, P., and Urbas, G. (2004). *Cyber criminals on trial*. Cambridge: Cambridge University Press.
- Sophos. (2006). *Stopping zombies, botnets, and other email-borne threats*. Abingdon: Sophos.
- Symantec. (2009). *Symantec global Internet security threat report trends for 2008*. Vol. XIV. Mountain View, CA: Symantec.
- Thomas, N. (2009). Cyber security in East Asia: governing anarchy. *Asian Security*, 5: 1-23.
- Raywood, D. (2009). Botnet discovered by Finjan contained 73 government domains. *SC Magazine*, 1 May. Online at <http://www.scmagazineuk.com/botnet-discovered-by-finjan-contained-73-government-domains/article/135953> (accessed July 31, 2009).
- United Nations (2004). A more secure world: our shared responsibility: report of the high-level panel on threats, challenges and change. Online at <http://www.un.org/secureworld/report2.pdf> (accessed July 31, 2009).
- Verizon. (2009). *2009 data breach investigations report*. Online at http://www.verizonbusiness.com/resources/security/reports/2009_databreach_report.pdf (accessed July 31, 2009).
- Walker, D., Brock, D., and Stuart, I. (2006). *Accesses-oriented policing: traditional policing theories are not adequate in a cyber world*. *The Police Journal*, 79(2): 169-76.

- Wall, D. (2007). Policing cybercrimes: situating the public police in networks of security within cyberspace. *Police Practice and Research: An International Journal*, 8(2): 183–205.
- White, M. and Fisher, C. (2008). Assessing our knowledge of identity theft: the challenges to effective prevention and control efforts. *Criminal Justice Policy Review*, 19(1): 3–24.
- Wikström, P. and Treiber, K. (2007). The role of self-control in crime causation. *European Journal of Criminology*, 4(2): 237–64.
- Yar, M. (2005). The novelty of “cybercrime”: an assessment in light of routine activity theory. *European Journal of Criminology*, 2(4): 407–27.