CRIME PREVENTION AND SECURITY MANAGEMENT

Cybercrime Prevention

Theory and Applications

Russell Brewer
Melissa de Vel-Palumbo
Alice Hutchings
Thomas Holt
Andrew Goldsmith
David Maimon

palgrave
macmillan

Crime Prevention and Security Management

Series Editor
Martin Gill
Perpetuity Research
Tunbridge Wells, Kent, UK

It is widely recognized that we live in an increasingly unsafe society, but the study of security and crime prevention has lagged behind in its importance on the political agenda and has not matched the level of public concern. This exciting new series aims to address these issues looking at topics such as crime control, policing, security, theft, workplace violence and crime, fear of crime, civil disorder, white collar crime and anti-social behaviour. International in perspective, providing critically and theoretically-informed work, and edited by a leading scholar in the field, this series will advance new understandings of crime prevention and security management.

More information about this series at
http://www.palgrave.com/gp/series/14928

Russell Brewer · Melissa de Vel-Palumbo ·
Alice Hutchings · Thomas Holt ·
Andrew Goldsmith · David Maimon

Cybercrime Prevention

Theory and Applications

palgrave
macmillan

Russell Brewer
School of Social Sciences
University of Adelaide
Adelaide, SA, Australia

Alice Hutchings
Department of Computer Science
and Technology
University of Cambridge
Cambridge, UK

Andrew Goldsmith
Centre for Crime Policy and Research
Flinders University
Adelaide, SA, Australia

Melissa de Vel-Palumbo
Centre for Crime Policy and Research
Flinders University
Adelaide, SA, Australia

Thomas Holt
School of Criminal Justice
Michigan State University
East Lansing, MI, USA

David Maimon
Department of Criminal Justice
and Criminology
Georgia State University
Atlanta, GA, USA

Crime Prevention and Security Management
ISBN 978-3-030-31068-4 ISBN 978-3-030-31069-1 (eBook)
https://doi.org/10.1007/978-3-030-31069-1

© The Editor(s) (if applicable) and The Author(s) 2019
This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Cover illustration: Przemyslaw Klos/EyeEm

This Palgrave Pivot imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Series Editor's Preface

Russell Brewer, Melissa de Vel-Palumbo, Alice Hutchings, Thomas Holt, Andrew Goldsmith, and David Maimon present a critique of seven different types of commonly deployed crime prevention interventions which they believe have the potential to be used in tackling cybercrimes (with a specific focus on cyber-dependent offences). Certainly, for this reader, these distinguished authors have fulfilled their aim 'to make a substantial original contribution' as to how their chosen crime prevention techniques can be used to tackle offending in the digital realm.

Running through their analysis are at least three issues. The first is that cyber-offending and cyber-offenders typically have different characteristics to traditional offline offenders/offences. This complicates the potential application of traditional crime prevention approaches when applied to the digital arena. Second, there is a paucity of research, and in particular evaluations of these prevention approaches in the online world. The third point is that where there is evidence, it often produces mixed results—sometimes interventions work as intended, sometimes not, sometimes their effect is neutral, and sometimes they can make things worse. This book charts a path through these issues by critiquing the available evidence in the offline world, identifying relevant overlaps with activities online, and then exploring the potential for them to be so applied—providing guidance at the same time as to how this might be undertaken most effectively.

Taking situational crime prevention as an example, and there is more research on this approach than any other they discuss, evaluations

suggest antivirus products are able at detecting and preventing malware attacks but are less positive about the effectiveness of warning messages in mitigating malicious hacking. The available evidence bars for other techniques such as firewalls, passwords, and security awareness programmes are far less developed.

Mass media messages such as awareness-raising campaigns are found wanting offline and have a limited applicability to online offending. Educational workshops may have potential although they will need a different orientation when applied in the cyber-world. Even good mentoring programmes can be thwarted by the difficulty of identifying relevant populations of both offenders and volunteers to help them. Targeted warnings and cautions by the police to warn potential offenders are deemed to have some potential where, for example, they focus on the wrongfulness of the act rather than the offender. Positive diversions that redirect offenders away from crime have some potential, for example, by transitioning malicious hackers to legitimate cybersecurity jobs. Restorative justice also has some appeal to victims and may help some offenders.

You will read more. The potential varies with offences and offenders and the context in which measures are introduced, but what is clear is that there is a need for more research. Offending has proliferated online because offences can generally be committed with more anonymity, where they have less chance of being identified, arrested, and successfully prosecuted and where victims are in plentiful supply. We know that policing generally and the security world specifically have struggled to keep up with changes, and this book suggests criminologists have too. Helpfully they outline in their final chapter ways of filling the knowledge gaps, both in terms of key issues to focus on and the positives and limitations of different evaluation methodologies.

This book is more than about cybercrime. It provides a critique and a review of crime prevention approaches and charts a way of better identifying how a much-neglected area of enquiry can be better understood, and, as importantly, how we can best target future prevention efforts. These alone make it an enticing read.

July 2019 Martin Gill

Acknowledgements

This work has its origins in a programme of research funded through the Home Office, which studied cybercrime prevention, knowledge, and practice. The book itself is an outgrowth from a symposium hosted by the University of Cambridge in late 2017, where the findings from this programme were presented by the authorship team. In bringing this research together here in this volume, we hope to contribute to the extensive work already being done by those within the cybersecurity community, law enforcement, and the criminal justice system, who contend with cybercrime and its impact every day.

The authors would like to acknowledge the contributions of several individuals, without whom this book would not have been possible. First and foremost, we would like to thank Catherine Schubert for her editorial and research support over the life of this project. Her patience, diligence, and good humour were greatly appreciated by all. We are also grateful to Ross Anderson, Alistair Beresford, Robert Clarke, Samantha Dowling, Richard Clayton, Sergio Pastrana, Daniel Thomas, and Julie-Anne Toohey for their inputs on earlier drafts of this work. In addition, we would also like to acknowledge the numerous scholars cited throughout the book, whose high-quality scholarship formed the basis of our evaluations and discussion. Finally, we would like to express our gratitude to Liam Inscoe-Jones, Josie Taylor, and the production staff at Palgrave for their dedication to bringing this book together.

In closing, the authors would like to acknowledge and thank the Home Office for funding the original programme of research, as well as the Centre for Crime Policy and Research at Flinders University for subsequent financial support in the preparation of the manuscript for this book.

Contents

List of Tables

CHAPTER 1

Setting the Scene

Abstract The book begins with an introductory chapter that sets the scene: providing an overview of the core principles associated with crime prevention targeting that will be drawn upon throughout. It chronicles the unique aspects of offending within digital contexts, and in particular, explicates offending lifecycles, and flags significant points of divergence from what is broadly accepted for offline forms of offending. Next, it provides a methodological account of the approach taken in researching this book, before concluding with an overview of chapters to come.

Keywords Cybercrime · Cyber-dependent crime · Cyber-offender · Crime prevention · Cybercrime prevention · Intervention

Introduction

Criminological research has made significant advances in the development, deployment, and evaluation of the myriad crime prevention strategies designed to identify and target individuals at various stages of the offending life cycle. This work, however, is principally rooted in understandings of what may be loosely called 'traditional' crime settings (Newman and Clarke 2003). Cybercrime is a relatively new crime type, and there has been little systematic attention given to the specific digital settings and contexts in which it occurs. As a result, many cybercrime prevention

© The Author(s) 2019

R. Brewer et al., *Cybercrime Prevention*,
Crime Prevention and Security Management,
https://doi.org/10.1007/978-3-030-31069-1_1

recommendations are not necessarily evidence-based. Such initiatives also tend to ignore the role of the offender (who can often displace to new targets or methods) and place the onus on victims to protect themselves. Scholars, practitioners, and policymakers are now seeking more effective ways to prevent cyber-offenders from attacking certain targets and to practically facilitate desistance from serious forms of cybercrimes. At present, they face a largely undeveloped theoretical and empirical body of literature.

Identifying and articulating evidence-based approaches to cybercrime prevention is critical due to the increasingly serious economic, national security, and political harms associated with the now-routine reports of compromised computer systems that have been used to access, reveal, or resell sensitive data (Franklin et al. 2007; Holt et al. 2016; Hutchings and Holt 2016; Motoyama et al. 2011). This book addresses this knowledge gap by investigating the applicability of evidence-based interventions to prevent cyber-dependent crimes. That is, crimes that can *only* be committed using a computer or network and include such acts as spreading viruses, malware, spyware, malicious hacking, and distributed denial of service attacks (DDoS) (McGuire and Dowling 2013).[1] These attacks have become a common global problem: in 2015, more than 1600 data breaches targeting governmental and private organisations exposed over 707 million records around the world (Gemalto 2015). Moreover, users of private computers, smartphones, and even medical devices increasingly report infiltration of their devices by illegitimate users (Storm 2015). This book adopts a broad definition of cyber-dependent crime that includes both 'illicit intrusions into computer networks', as well as the 'disruption or downgrading of computer functionality and network space' (McGuire and Dowling 2013, p. 4). Accordingly, the term 'cyber-offender' used throughout this book is also to be construed broadly—denoting those who use their knowledge to cause harm to, or directly damage, computer software, hardware, and data. This may include the use of malware (whether created by the individual or purchased/acquired from others) or exploits, or the manipulation of human actors to achieve said goals. This breadth is merited due to the range of interests and attack techniques that can be, and have already been,

[1] Such activities can be distinguished from cyber-enabled crimes which are regarded as 'traditional' crimes that are augmented through the use of computers or networking technologies (e.g. fraud) (McGuire and Dowling 2013).

used by individuals to successfully complete a cyberattack. Additionally, researchers have noted the overlapping interests and skills needed in order to write malware, engage in DDoS attacks on a fee-for-service basis, or complete malicious hacks more generally (Décary-Hétu and Dupont 2012).

Overall, the book aims to make a substantial original contribution to how the discipline of criminology understands and can reasonably apply longstanding, tried and tested, traditional crime prevention techniques to the digital realm, particularly for cyber-dependent crimes. In doing so, it breaks new ground and articulates the ways that crime prevention research and practice needs to be reimagined for an increasingly digital world.

This introductory chapter sets the scene for the book, providing an overview of the core principles associated with crime prevention targeting that will be drawn upon throughout. It chronicles the unique aspects of offending within digital contexts, and in particular, explicates offending lifecycles, and flags significant points of divergence from what is broadly accepted for offline forms of offending. Next, it provides a methodological account of the approach taken in researching this book, before concluding with an overview of chapters to come.

Approaches to Crime Prevention

In crafting any sort of preventative measure, be it on- or offline, it is important to first consider the point at which (i.e. when) an intervention is most suitable. Taking cues from an established public health literature, crime prevention scholars acknowledge that interventions can be designed to target different points (in this case, of the offending life cycle). These can broadly occur at one of three stages (Brantingham and Faust 1976). First, interventions can be designed to target the *primary prevention* stage, whereby they are intended to target and prevent criminal behaviour before it occurs. Interventions appearing at this stage are considered to be the most universal, being largely undiscriminating and targeted at wide populations. Such interventions tend to focus upon the earliest stages of the offender life cycle, before potential offenders begin engaging in criminal behaviours. Typically, interventions occurring at this stage involve reducing opportunities for crime, or enhancing social factors that reduce an individual's likelihood of becoming involved in crime. The next stage, classed as *secondary prevention*, is targeted

towards people *at risk* of embarking on a criminal career, such as children who show some signs of delinquent behaviour. Such interventions, therefore, devote effort and resources towards those who may have an increased proclivity for criminal conduct, but before they graduate into more serious offending. Finally, the *tertiary prevention* stage focuses on treating individuals after they have become involved in crime. The focus at this stage is to prevent individuals reoffending. This is the most targeted level of intervention, by which individuals are formally referred to programming by the criminal justice system following a criminal conviction.

Determining the appropriate stage at which an intervention is to be directed can be based on several factors, including characteristics of the crime and the offender group, as well as more practical considerations such as resources. In particular, much research suggests the development of effective interventions relies on the accurate identification of factors known to contribute to offending (e.g. Bonta and Andrews 2017; Andrews and Bonta 2010; Andrews et al. 1990; Dowden and Andrews 1999; Koehler et al. 2013). Considerable research has been done to explicate such factors—particularly in offline settings. While criminogenic factors vary somewhat across different criminal populations (e.g. sexual offenders versus others), there is substantial overlap between categories, and correlates for criminal behaviour show many similarities for specific forms of criminal deviance (Bonta and Andrews 2017). The best-validated risk factors for criminal behaviour include: *individual factors*, such as being male and young, substance abuse, low educational achievement/unemployment, lack of structured prosocial leisure activities, antisocial personality patterns (i.e. impulsivity, poor problem-solving), antisocial cognition (i.e. attitudes/values/beliefs that promote criminal behaviour such as lack of empathy, pro-crime justifications, and anti-law attitudes); *family factors*, including coming from a low socio-economic status home, abuse and neglect, poor parental mental health, parental criminal history, parenting style, and parent–child relationship (i.e. harsh, lack of affection and supervision); and *social* factors, including urban environments, unstable living arrangements, and exposure to delinquent peers (for reviews see Cottle et al. 2001; Gendreau et al. 1996; Lipsey and Derzon 1998; Murray and Farrington 2010).