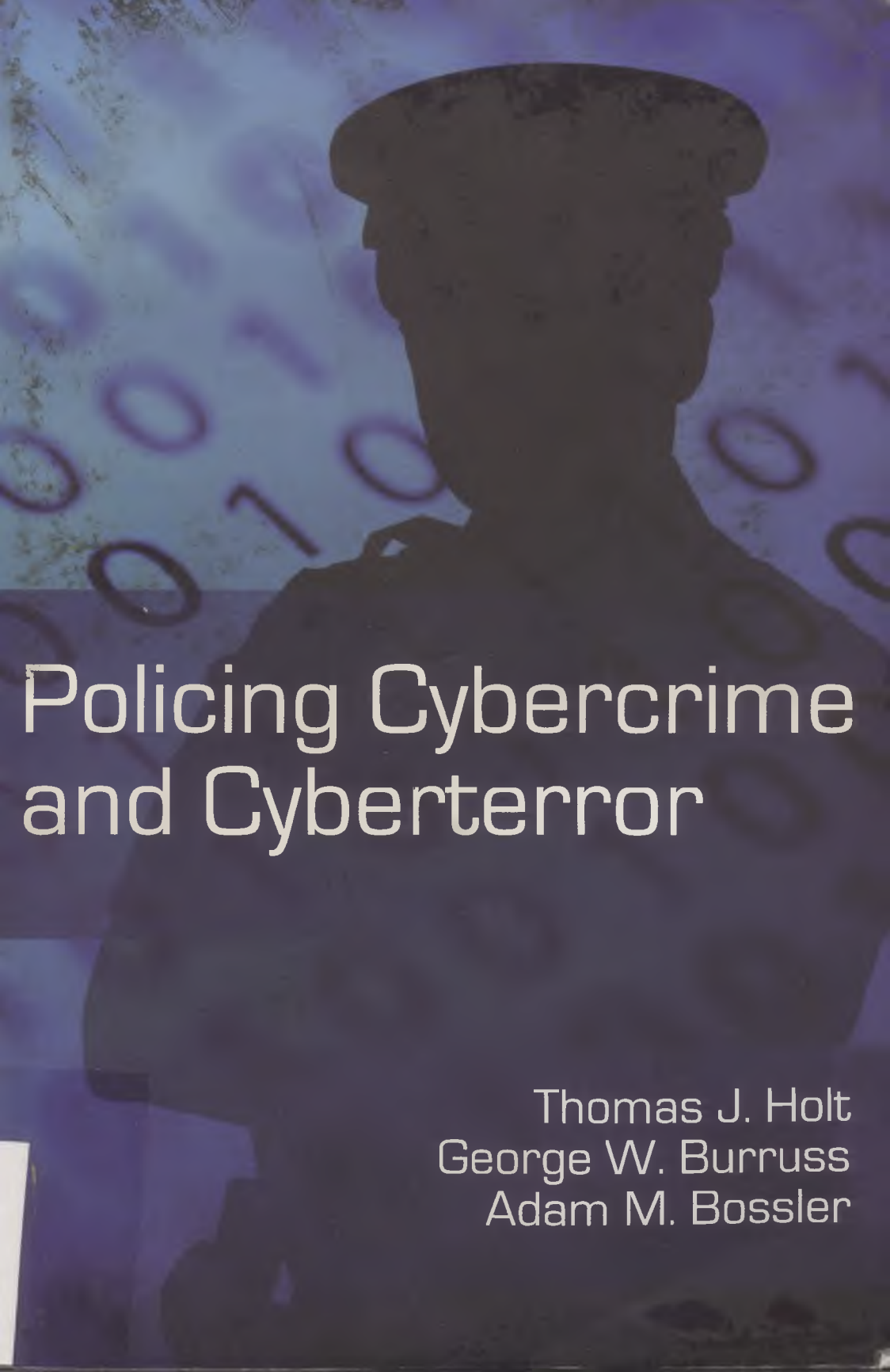

Policing Cybercrime and Cyberterror

Thomas J. Holt
George W. Burruss
Adam M. Bossler

Policing Cybercrime and Cyberterror

Thomas J. Holt
Michigan State University

George W. Burruss
Southern Illinois University Carbondale

Adam M. Bossler
Georgia Southern University

BIBLIOTEKA
Nr ewid. .....
Akademii Sztuki Wojennej

Carolina Academic Press
Durham, North Carolina

Copyright © 2015
Carolina Academic Press
All Rights Reserved

Library of Congress Cataloging-in-Publication Data

Holt, Thomas J., 1978-
Policing cybercrime and cyberterror / Thomas J. Holt, George W. Burruss, and Adam M. Bossler.
pages cm
Includes bibliographical references and index.
ISBN 978-1-61163-256-9 (alk. paper)
1. Computer crimes. 2. Cyberterrorism. 3. Police. I. Burruss, George W. II. Bossler, Adam M. III. Title.

HV6773.H653 2015
363.25'968--dc23

2015000194

Carolina Academic Press
700 Kent Street
Durham, NC 27701
Telephone (919) 489-7486
Fax (919) 493-5668
www.cap-press.com

Printed in the United States of America

For my wonderful wife Dr. Karen Holt, and our spectacular daughter Scarlett.
TJH

For my mother, Linda.
GWB

For my amazing wife Jordan and our two wonderful children,
Kate and Bennett.
AMB

Contents

Acknowledgments ix

Chapter 1 • Introduction to Cybercrime and Cyberterror 3
- Defining Cybercrime and Cyberterror 6
  - Cybercrime 6
  - Cyberterror 9
- Situating Local Law Enforcement in the Management of Cyberspace 10
  - Internet Users 11
  - Internet Service Providers 12
  - Corporate Security and Industry 13
  - Non-Governmental Non-Police Organizations 14
  - Governmental Non-Police Organizations 14
  - Public Policing Agencies 15
- Local Law Enforcement and Cybercrime Investigation 17

Chapter 2 • Cybercrime Statistics and Officer Perspectives 21
- Data Sources for Cybercrime and Cyberterror 22
  - UCR and NIBRS 22
  - NCVS 24
  - IC3 24
  - Business Estimates 26
- Officer Perceptions of Cybercrime 27
  - Officer Perceptions of Typical Cybercriminals and Victims 28
  - Perceptions of Cybercrime Uniqueness, Seriousness, and Frequency 29
  - Assessing Specialized Officers' Perceptions of Cybercrime 34
- Summary and Conclusion 38

Chapter 3 • Examining the Attitudes of Local Law Enforcement toward Cybercrime Training 39
- Investigative Resources for Cybercrime Cases 40
- Officer Interest in Cybercrime Training 43

Officer Attitudes toward Training 48
Summary and Conclusion 58

Chapter 4 • Police Officer Attitudes toward the Law Enforcement Response to Cybercrime 59
Perceptions of Traditional Strategies to Combat Cybercrime 60
Support of Cybercrime Investigations within Police Departments 63
Innovative Strategies 66
Interest in Working with High-Tech Industries and Service Providers 71
Summary and Conclusions 88

Chapter 5 • Stress, Strain, and Satisfaction among Cybercrime Investigators 89
Job Stress in Policing 90
Occupational Experiences in Law Enforcement 90
Cybercrime, Forensic Investigation, and Stress 91
Assessing Stress, Satisfaction, and Coping Mechanisms 94
Exploring the Predictors of Stress and Satisfaction 98
Coping Mechanisms Reported By Digital Forensic Investigators 103
Exploring Trauma among Digital Forensic Investigators 105
Summary and Conclusions 109

Chapter 6 • Implications for Policing Policy and Practice 115
Implications of Findings for CJ Policy 115
1) Public Awareness 115
2) Data Reporting 117
3) Uniform Training and Certification Courses 118
4) Onsite Management Assistance for Electronic Crime Units and Task Forces 119
5) Updated Laws 120
6) Cooperation with the High-Tech Industry 122
7) Special Research and Publications 123
8) Management Awareness and Support 124
9) Investigative and Forensic Tools 126
10) Structuring a Computer Crime Unit 126
Limitations and Conclusions 130

References 133
Index 149

Acknowledgments

As the field of criminological research on cybercrime continues to evolve, we are grateful to the many individuals whose assistance and contributions facilitated its creation. We are extremely grateful to April Wall-Parker, Deputy Director Mark Gage, Gerry Cliff, and all of the trainers of the National White Collar Crime Center. This study would not have been possible without their creativity and assistance in allowing the researchers to survey trainees in their various courses. We would also like to thank the Charlotte Mecklenburg Police Department and the Savannah Chatham County Metropolitan Police Department for their willingness to allow the researchers to survey line officers in both agencies. They provided us with an opportunity few have had in researching cybercrime; we are greatly appreciative. We would also like to sincerely thank the publishing team at Carolina Academic Press, especially Beth Hall for her encouragement and flexibility throughout the creation and submission of this work. There were times I am sure we tried your patience. It is also important that we thank the faculty and staff of the Department of Criminology and Criminal Justice at the University of Missouri–Saint Louis. Dr. Scott Decker is still a mentor despite our having graduated many years ago. Finally, we would like to thank our families and friends for all of their support throughout this process.

Biblioteka Główna
Akademii Sztuki Wojennej
26662/III (CB)
03-026662-000-0

The purpose o
in-depth discussic
law enforcement agencies in dealing with cybercrime and cyberterror. The themes for this book include the challenges that cybercrime and digital evidence handling pose for local and state agencies, the jurisdictional and investigative hurdles that hinder the response capabilities of police agencies, and the complexities of the actual investigation of these offenses and their impact on officers.

This text analyzes data collected from local law enforcement agencies in the United States in order to understand officer perceptions of and responses to cybercrime and cyberterrorism, along with samples from digital forensic examiners, to understand their stress, satisfaction, secondary trauma, and coping mechanisms in response to work experiences. The findings demonstrate the realities of policing cybercrime and those involving digital evidence processing relative to traditional offenses. *Policing Cybercrime and Cyberterror* addresses a gap in the policing literature by examining the various technological and policy changes needed to increase the investigative response of police agencies, along with various internal policies to improve support for forensic investigators.

Thomas J. Holt is an Associate Professor in the School of Criminal Justice at Michigan State University.

George W. Burruss is an Associate Professor in the Department of Criminology and Criminal Justice at Southern Illinois University Carbondale.

Adam M. Bossler is an Associate Professor in the Department of Criminal Justice and Criminology at Georgia Southern University.

ISBN 978-1-61163-256-9

Cover photograph © caracterdesign/iStockPhoto