Book Review

Policing cybercrime and cyberterror

Thomas J. Holt, George W. Burruss and Adam M. Bossler
Carolina Academic Press, Durham, NC, 2015, 174pp., $27.00, ISBN: 978-1611632569

Security Journal (2016) **29,** e13–e15. doi:10.1057/sj.2015.47; published online 21 December 2015

In *Policing Cybercrime and Cyberterrorism*, Thomas J. Holt, George W. Burruss and Adam M. Bossler provide an especially timely and informative discussion of the important role that local law enforcement should play in addressing cybercrime and cyberterrorism. The book is organized into a total of six chapters and covers topics such as the current state of cybercrime data, police officer attitudes toward cybercrime training, officer attitudes regarding the response to cybercrime, stress and satisfaction among investigators, and implications of the findings for cybercrime policy and practice. The book is very well structured and organized, contributing to its accessibility for a variety of audiences. The book is written so that both policymakers and practitioners will find the material practical and easily digestible, as readers are not overwhelmed with heavy academic and statistical language. At the same time, the information provided in the footnotes regarding the authors' statistical approaches will appeal to scholars who may seek a more detailed explanation of the particular tests used. Given the lack of literature that currently exists regarding the perceptions of and role of local law enforcement in addressing cybercrime and cyberterrorism, this book clearly fills a gap and contributes to both the criminology and cybercrime research. It offers not only appropriate recommendations for how cybercrime can be prevented, but also important suggestions for how future research can attempt to untangle the uncertainties currently present in our understanding of the issue.

In the book's Chapter 1, the authors provide an overview of cybercrime and cyberterrorism along with the unique challenges local law enforcement face in combatting such offenses. They highlight how advances in technology play a role in assisting criminal activity, as the Internet allows for terrorists and other extremists to disseminate information about their ideology and weapons-making materials. In addition, since important infrastructures such as electricity and water are supported by Internet-based systems, these resources are increasingly susceptible to attacks by terrorists, nations or other groups that seek to inflict widespread damage. When it comes to successfully investigating cybercrimes, law enforcement agencies are at a disadvantage considering the variety of challenges they face. Such hurdles include the lack of incident reporting that characterizes many cyber offenses, along with the jurisdictional confusion that exists among agencies since offenses can be local or international in scope. Cyber offenders are also able to hide their locations and identities through the use of proxies. Finally, law enforcement agencies require costly technological resources to adequately investigate these crimes.

In Chapter 2, the authors discuss the issues present in the availability of sufficient cybercrime data. They note that individuals often do not report their cybercrime victimization to the police because they think that the police cannot help them. As a result of this lack of reporting, there is a very large 'dark figure of cybercrime', where the true scope of the problem is unknown. Cybercrime data from official sources are very limited, consequently making research on the topic difficult. For example, cybercrime data are not recorded in the FBI's Uniform Crime Report, and several limitations exist with the data contained in the FBI's National Incident Based Reporting System. Another data resource, the Internet Crime Complaint Center (IC3), which individuals can use to report their victimization, is limited in that it contains mostly reports of financial cybercrime incidents. In response to the lack of data available, the authors administered a survey to 1701 law enforcement officers that completed the National White Collar Crime Center's (NW3C) computer training program in order to gain an understanding of their perceptions of cybercrime. Notably, results show that officers ranked child pornography and cyberterrorism as the most serious offenses compared with other forms of cyber and street crime. This finding signifies that officers recognize the importance and severity of cybercrime and cyberterror.

Holt, Burruss and Bossler discuss their survey findings in Chapter 3. In the survey data administered to NW3C trainees, the authors found that some demographic and agency factors such as, officer age, race and agency size affected whether or not individuals received more cybercrime investigation training. In order to examine what factors may influence officer willingness to receive computer and cybercrime training, the authors collected additional survey data from patrol officers in Charlotte, North Carolina and Savannah, Georgia. They discovered that there are distinct attitudes impacting officers' desires to investigate cybercrimes, which may influence their success if they participate in a case. For example, officers who saw value in addressing cybercrime were more likely to be interested in developing and improving their skills, while officers who thought that cybercrime investigations should be dealt with at the federal and state levels were less likely to be interested in computer training. Also in this chapter, Holt, Burruss and Bossler discuss how task forces are one potential avenue for combatting cybercrime since they promote resource sharing and investigative coordination among different branches of the criminal justice system. They point to the Internet Crimes Against Children as an example of a successful task force, while also acknowledging that not all law enforcement agencies have the resources needed to adequately contribute to these types of task forces.

Chapter 4 provides an informative discussion of officer attitudes toward the law enforcement response to cybercrime. The authors emphasize that cybercrime programs designed to coordinate law enforcement efforts with outside organizations and citizens must have support from officers in order to be successful at reducing offenses. They note that researchers have found that law enforcement can effectively reduce cybercrime by working with outside partners such as Internet users, Internet Service Providers and other law enforcement and non-public policing agencies. In response to this research, the authors recommend that one avenue for obtaining a successful collaborative cybercrime program could be through applying the tenets of traditional community-oriented policing. In fact, their findings reveal that officers who support traditional community policing, as well as officers who value computer-based investigations, are more likely to support working with outside groups (that is, the business community and service providers). Officers who view cybercrimes more seriously than other officers are also more wiling to work with outside

groups, and officers who believe that cybercrime investigations drain resources are less likely to support working with outside partners. One noteworthy finding is that computer proficiency and skill is not related to officers believing that it is important to work with outside groups. Thus, officers possessing computer skills are not necessarily the best suited for working with collaborative cybercrime programs.

The authors discuss the issues of stress and satisfaction among cybercrime investigators in Chapter 5. In order to examine the stressors posed by cybercrime offenses, they administered a new survey to investigators who completed digital forensic investigation training provided by the NW3C. They find that investigators who are exposed to child pornography report higher degrees of stress and secondary trauma. They also find that individuals potentially rely more on their personal relationships to help cope with this stress instead of clinicians. These results underscore the need for agencies to be aware of the unique stressors investigators face and provide these individuals with the necessary resources for effectively coping with these issues.

In the final chapter, the authors detail the implications of their findings for policy and practice. They emphasize that until law enforcement agencies improve their documentation of cybercrime calls for service, we will continue to have an inadequate picture of cybercrime. They argue that one way to address this issue is to develop a public awareness campaign of the IC3 so more people can seek it out to file reports. The authors also support the idea of introducing cybercrime training and recognition early in police officer careers (that is, at the police academy) in order to improve their awareness of the importance of cybercrime investigations. One notable recommendation they offer is the creation of an online tip service to assist individuals in reporting of suspicious online behavior directly to law enforcement. The authors conclude this chapter by acknowledging that their data is limited as their samples are derived from Charlotte and Savannah, and thus the results are not necessarily applicable to the entire country. They also acknowledge that their samples of forensic investigators are limited because of the fact that they are convenience samples.

Despite the limitations regarding the data, this book certainly provides a valuable addition to the research literature on cybercrime. Considering the lack of research on this topic and inadequate official sources of data, the authors offer an informative discussion of the role local law enforcement can play to effectively reduce cybercrime incidents, as well as the steps that can be taken to improve data collection. The book provides practical recommendations for improving not only the response of law enforcement to cybercrime but also officer attitudes toward such investigations. Policymakers, practitioners and scholars can all learn from and apply these findings to formulate successful prevention measures and improve cybercrime investigations.

Marissa Mandala
Department of Criminal Justice,
John Jay College of Criminal Justice/CUNY Graduate Center, New York, USA