International Journal of Cybersecurity Intelligence & Cybercrime

Volume 6 | Issue 1 Article 1

3-31-2023

New Knowledge, Better Decisions: Promoting Effective Policymaking Through Cybercrime Analysis

Hackers; Profiling; Cyberterrorism; Cybe

Recommended Citation
Givens, A. D. (2023). New knowledge, better decisions: Promoting effective policymaking through cybercrime analysis. International Journal of Cybersecurity Intelligence & Cybercrime, 6(1), 1-4.

New Knowledge, Better Decisions: Promoting Effective Policymaking Through Cybercrime Analysis

Austen D. Givens*, Ph.D., Utica University, U.S.A.

Keywords: Hackers; Profiling; Cyberterrorism; Cyberbullying

Abstract:
This editorial introduction will present an overview of the four articles contained in this issue of the *International Journal of Cybersecurity Intelligence and Cybercrime*. The articles examine the profiling of hackers, the role of the media in shaping public perceptions of cyberterrorism, research trends in cybersecurity and cybercrime, as well as the impacts of cyberbullying.

Introduction

Given the persistence of cybercrimes today, it is difficult to imagine a future in which threats like online predation, attacks against industrial control systems (ICS), and the laundering of funds through cryptocurrency exchanges slows or declines. Yet new data can potentially illuminate previously hidden patterns and methods among cybercriminals. And that information holds out the promise of both contributing to scholarly knowledge of cybercrime and providing a basis from which government and private sector leaders can forge sound, data-driven policies to reduce cybercrime.

Consider, for example, the broken windows theory of policing, which focuses on enforcing low-level, non-violent offenses to reduce community fears of crime and deter other, more violent types of crimes. First posited by George Kelling and James Q. Wilson in the early 1980s, broken windows policing was embraced by law enforcement officials in locations such as New York City (Kelling & Wilson, 1982). While the merits and drawbacks of the broken windows theory of policing have attracted scholars' attention for many years, at its inception, broken windows policing became one crime reduction strategy within a constellation of possible approaches to improving community safety (Harcourt & Ludwig, 2006; Hinkle & Weisburd, 2008; Howell, 2016).

But with advances in research, scholars have since developed serious doubts around the effectiveness of broken windows policing strategies (Harcourt & Ludwig, 2006). In New York City, for example, broken windows policing drove drug offense-related arrests to extraordinary levels, and this contributed to crowded prison conditions. Broken windows policing affects communities of color at levels disproportionate to those of other demographic groups (Howell, 2016). Broken windows policing continues to be defended by some senior law enforcement leaders, and it is important to highlight that scholarly interest in this strategy continues (Bratton & Kelling, 2015; Kelling, 2015).

*Corresponding author
Austen D. Givens*, Ph.D., School of Business & Justice Studies, Utica University, 600 Burrstone Road, Utica, NY 13502, U.S.A.
Email: adgivens@utica.edu

The creation and evolution of broken windows policing presents us with a living example of how focused scholarly inquiry can lead to new enforcement strategies, as well as refinements and adjustments to those strategies over time. In a similar manner, new understandings of cybercrime can contribute to the creation of future strategies and approaches to reduce cybercrime. This issue features four articles that treat cybercrime phenomena from diverse perspectives. Individually and collectively, these studies shed light on cybercrimes and their effects.

Overview

Wu, Peng, and Lemke's (2023) article, titled "Research trends in cybercrime and cybersecurity: a review based on Web of Science core collection database," traces the arc of scholarship on cybercrime and cybersecurity from 1995-2021. In conducting their analyses, the authors visualized data on thousands of publications about these topics, and in so doing, were able to sift out and identify key themes and trends among researchers. There has been a pronounced growth in the number and variety of journals publishing articles about cybercrime and cybersecurity over time. In addition, Wu, Peng, and Lemke (2023) were able to identify how classical criminological theories like routine activity and self-control have been revisited by scholars interested in cybersecurity and cybercrime. They observe a convergence, too, of various keywords over time. For example, cybercrime and hacking, victimization, and deterrence are increasingly found in the same publications.

The second article in this issue, "Threat Construction and Framing of Cyberterrorism in the U.S. News Media," uses quantitative and qualitative analyses of survey data to assess how the media shape perceptions of malicious cyber activity. This study finds that, for American adults, consuming news coverage of incidents like data breaches, attacks on critical infrastructure, and ransomware is a significant predictor of fear of cyberterrorism. The article also notes that the term "cyberterrorism" itself appears to be conflated in media coverage with other types of actions, such as distributed denial of service (DDoS) attacks. This lack of precision in vocabulary results in an overuse of the term "cyberterrorism" in media coverage. And that overuse itself may be contributing to fear of cyberterrorism among the general population within the United States. To address this, the authors suggest that an increase in public awareness of the different types of cyber threats which exist may help to reduce irrational and unnecessary fears.

The third article in this issue, "Prevalence and Trends of depression among cyberbullied adolescents—Youth Risk Behavior Survey, United States, 2011-2019," illuminates both the scope and growing impacts of cyberbullying. Using data from the U.S. Centers for Disease Control and Prevention (CDC), this study shows that there are linkages between instances of depression and cyberbullying across gender and racial/ethnical lines among youths. This has significant implications for law enforcement officials, educators, as well as the healthcare profession. Each of these actors are stakeholders in addressing cyberbullying behaviors and their attendant consequences among juveniles.

The final article is by Gerstenfeld (2023) and examines data from the U.S. Department of Justice (DOJ) to assess whether there are relationships between the age, gender, and nationality of hackers and the types of electronic attacks in which they engage. This article makes several contributions to the literature on hackers and hacking that are worth emphasizing. One of the most persistent challenges with research on hacking is a lack of researcher access to those who perpetrate hacks—the hackers themselves. Gerstenfeld's work addresses this problem by utilizing publicly available information on hacks from DOJ to discern and analyze patterns of behavior from hackers. Importantly, this analysis strives to determine if the specific targets or methods used to hack can be leveraged to predict a hacker's age, gender, and location.

The results of the analysis offer fascinating insights into the ways in which different types of hackers employ an array of techniques to perpetrate attacks. For example, Gerstenfeld finds that the use of social engineering tends to be associated with younger hackers. Relatedly, the creation of software tools to execute attacks is associated with hackers who are older, and presumably have more specialized knowledge and experience with building such tools, than their younger counterparts. Findings such as these suggest that scholars can construct profiles of hackers that could potentially be used by policymakers to develop deterrence and enforcement strategies.

Concluding Remarks

While the studies presented in this issue contain important caveats, they nonetheless work to advance our knowledge and comprehension of cybercrime today. By gaining further insights into the techniques employed by different types of hackers, how media coverage of cyber threats influences perceptions of those threats, emerging trends in cybercrime research, and the health effects of cyberbullying, scholars and policymakers alike come further to grips with the evolving nature of cybercrime. In so doing, a window of opportunity opens for the scholarly community as well as law enforcement practitioners to deter and reduce cybercrime. One hopes that the insights presented in this issue will also fuel other cybercrime scholars to seek answers to the pressing questions we confront.

References

Bratton, W. J., & Kelling, G.L. (2015). why we need broken windows policing. *City Journal, Winter.* https://www.city-journal.org/html/why-we-need-broken-windows-policing-13696.html.

Gerstenfeld, J. (2023). Understanding the connection between hackers and their hacks: Analyzing US DOJ reports for hacker profiles. *International Journal of Cybersecurity Intelligence and Cybercrime. 6*(1), 59-76.

Harcourt, B. E., & Ludwig, J. (2006). Reefer madness: broken windows policing and misdemeanor marijuana arrests in New York. john m. olin program in law and economics working paper no. 317. https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1412&context=law_and_economics.

Hinkle, J. C., & Weisburd, D. (2008). The irony of broken windows policing: A micro-place study of the relationship between disorder, focused police crackdowns and fear of crime. *Journal of Criminal Justice, 36*(6), 503–512.

Howell, K. B. (2016). The costs of broken windows policing: twenty years and counting. *Cardozo Law Review, 37.* 1059–1073.

Kelling, G. (2015, August 11). Don't blame my 'Broken Windows' theory for poor policing. *Politico Magazine.* https://www.politico.com/magazine/story/2015/08/broken-windows-theory-poor-policing-ferguson-kelling-121268/

Kelling, G. L., & Wilson, J.Q. (1982). Broken windows: The police and neighborhood safety. *The Atlantic, March, 249*(3). https://www.theatlantic.com/magazine/archive/1982/03/broken-windows/304465/.

Mehmet F. Bastug, M. F., Onat, I., & Guler, A. (2023). Threat construction and framing of cyberterrorism in the U.S. news media. *International Journal of Cybersecurity Intelligence and Cybercrime. 6*(1), 29-44.

Nicholson, J., Marcum, C., & Higgins, G. E. (2023). Prevalence and trends of depression among cyberbullied Adolescents – youth risk behavior survey, United States, 2011 – 2019. *International Journal of Cybersecurity Intelligence and Cybercrime. 6*(1), 45-58.

Wu, L., Peng, Q., & Lemke, M. (2023). Research trends in cybercrime and cybersecurity: A review based on web of science core collection database. *International Journal of Cybersecurity Intelligence and Cyber crime. 6*(1), 5-28.