American Journal of Criminal Justice (2021) 46:837–842
https://doi.org/10.1007/s12103-021-09652-7

Cybercrime: Victimization, Perpetration, and Techniques

James Hawdon[1]

Received: 3 July 2021 / Accepted: 3 August 2021 /
Published online: 10 November 2021

The creation of the World Wide Web revolutionized communication. At the turn of the twenty-first century, roughly 413 million people used the internet (Roser & Ortiz-Ospina, 2015). A mere 21 years later, nearly 4.7 billion people, or about 60% of the world's population, actively use the internet (We Are Social, & DataReportal, & Hootsuite, 2021). The pace of innovation in information technology, from the introduction of email in the 1960s to the rise of multiple social media platforms in the early 2000s to the rise of the Internet of Things (Iot) and 5 g, has been astonishing. It is now almost inconceivable to imagine life without access to the internet. Yet the IT revolution, like all technological revolutions, has been a dual-edge sword. Indeed, the internet's many benefits and drawbacks have been discussed in numerous forums, and these discussions will undoubtedly continue as long as we remain dependent on this technology. This special edition of the *American Journal of Criminal Justice* contributes to those discussions by considering one of the drawbacks: cybercime.

Cybercrime, or the use of computer technology or online networks to commit crimes, ranges from fraud and identity theft to threats and intimidation. Cybercrime and its many manifestations has clearly increased over the past 20 years. For example, cybercrime costs increased from approximately $3 trillion in 2015 to more than $6 trillion in 2021, and these are expected to increase to over $10.5 trillion by 2025 (Morgan, 2020). In the U.S. alone, approximately 23 percent of households experience some sort of cybercrime annually (Reinhart, 2018; Hawdon et al., 2020). Indeed, in the same way that larceny characterized the twentieth century, cybercrime is characterizing the twenty-first century (Albanese, 2005). And these facts just reflect the economic costs of cybercrime and do not account for the non-monetary harms caused by cyberviolence. Cyberstalking, online sexual exploitation, cyberharassment and bullying, threats of violence, and online violent extremism are also commonly committed acts of cyberviolence (FBI, 2021).

In many ways, it is unsurprising that cybercrime has increased in recent years. As technology becomes more sophisticated, so do cybercriminals, and cybercriminals now target individuals, businesses, healthcare facilities, educational institutions,

✉ James Hawdon
hawdonj@vt.edu

[1] Virginia Tech, Blacksburg, VA, USA

and governments. As more people engage in an ever-increasing variety of online activities and more businesses conduct their affairs online, it is predictable that there would be a rise in cybercrime. To use the familiar language of Routine Activity Theory (Cohen & Felson, 1979), we have a lot more suitable targets in insufficiently guarded space being victimized by an increasing number motivated offenders. It is also unsurprising that there is a growing body of literature dedicated to cybercrime as scholars scramble to understand the ever-evolving phenomena. Entire journals are now dedicated to its study, and new academic disciplines have been created to try to prevent it. While our understanding of cybercrime has accumulated quickly and impressively, there is so much about cybercrime that we still do not know. This special issue of the A*merican Journal of Criminal Justice* offers nine new articles to help fill that knowledge gap.

The articles included in this issue reflect three broad areas of cybercrime research: cybercrime victimization, cybercrime perpetration, and techniques and facilitators of cybercrime. While there is some overlap, the issue includes three papers focused on each of these three areas.

The first area covered in the special issue focuses on cybercrime victimization. This area has generated the most research to date. In part because victims of cybercrime are relatively easy to find, considerable research has been conducted on cybervictimization across a variety of cybercrimes. Three of the articles in this special issue focus on cybervictimization, and they add to the literature in interesting ways by providing cross-national perspectives, building on theoretical traditions, or providing systematic summaries of the state of field at this time.

The first article in this section by Michelle Wright and a team of colleagues investigates how adolescent from China, Cyprus, the Czech Republic, India, Japan, and the United States explain being a victim of cyberbully. The investigation compares if how adolescents explain victimization varies by setting (private vs. public), medium (offline vs cyber), and severity and if cultural differences alter these relationships. Their findings suggest the need for prevention and intervention efforts to consider the role of setting, medium, severity, and cultural values if they are to be successful.

The second paper focusing on victimization builds on the frequent finding that problematic social media use is associated with negative life experiences and provides empirical support for a theoretical link between problematic social media use and cybervictimization. The analysis, conducted by colleagues Eetu Marttila, Aki Koivula, and Pekka Räsänen, is framed in Routine Activity Theory/Lifestyle-Exposure Theory. The results indicate that not only is problematic social media use strongly correlated with cybervictimization in a between-subject analysis, but within-subject analyses also reveal that problematic social media use has a cumulative effect on victimization.

The third paper bridges research on cybercrime victimization and cybercrime perpetration and provides a glimpse at the state of knowledge about a specific form of cyberviolence. Catherine Marcum and George Higgins conduct a systematic review of literature investigating both offending and victimization of cyberstalking, cyberdating abuse, and interpersonal electronic surveillance. Using a number of electronic databases, the authors focus on 31 studies to identify correlates of involvement in these cybercrimes. Victims are disproportionately female.

Other correlates of victimization include overall social media use, risky online behavior, and negative external factors such as being attached to abusive peers. Correlates of perpetration provide support for a number of leading criminological theories as perpetrators tend to have low levels of self-control, associate with delinquent peers, and have low levels of parental supervision. As more research is conducted, there is a great need for more systematic literature reviews so we can begin to better refine our understanding and identify the theoretical approaches that provide the most insight into the world of cybercrime.

There are another three articles included in this special issue that focus on cybercrime perpetration. All three articles test traditional criminological theories and find support for them. In the first, Adam Bossler uses Sykes and Matza's (1957) techniques of neutralization to examine the effects of techniques of neutralization on college students' willingness to commit cybercrime, specifically hacking websites to deface them or compromise foreign and domestic financial and government targets. An overall techniques of neutralization scale significantly predicts being willing to commit cyberattacks even after controlling for other relevant factors. In addition to the theoretical implications of finding strong support for Sykes and Matza's framework, the findings also have implications for situational crime prevention efforts aimed at removing excuses for offenders.

In another article focusing on perpetration, Thomas Dearden and Katalin Parti use a national online sample of 1,109 participants and find strong support for social learning theory as measures of both online and offline social learning correlate with a measure of cyber-offending. However, the authors also argue that self-control will interact with social learning variables to further influence the likelihood of cyber-offending. Overall, they find that both social learning and self-control, individually and as an interaction, are good predictors of cyber-offending.

In the final article dedicated to investigating the perpetration of cybercrime, Ashley Reichelmann and Matthew Costello use a nationally representative sample to explore how various dimensions of American national identity relate to producing online hate materials. The analysis reveals that higher levels of salience and public self-regard are weakly related to producing online hate. However, the findings suggest that understanding the nuances of "what it means to be American" is important for fully understanding the phenomenon of cyberhate, especially in this polarizing time when what it means to "be American" is frequently questioned.

Another three articles deal with perpetrating cybercrimes or "pseudo-cybercrimes," but their focus is on how these crimes are committed. That is, the investigations deal with using the Dark Web or the surface web to make illegal or pseudo-legal purchases of illegal or quasi-legal substances. In the first paper in the section, Eric Jardine provides a crime script for purchasing drugs on the Dark Web. The script involves four generic stages (i.e. Informational Accumulation; Account Formation; Market Exchange; Delivery/Receipt) and provides an opportunity to review known law enforcement interventions that have effectively targeted each stage of the script to reduce the use of these online markets. The paper highlights numerous steps that law enforcement could take to effectively reduce the illegal selling and purchasing of drugs on the Dark Web.

Next, Robert Perdue engages in green criminology and focuses on the illegal trade of endangered species. Noting that regulating this trade is a critical, and very difficult, challenge for conservationists and law enforcement agents, Perdue examines the role the Internet plays in critically endangered plant transactions, but instead of focusing on the Dark Web, he investigates eBay to understand the extent to which such trades occur in plain sight. He finds that nearly a third of the critically endangered plant species examined were for sale in some form on eBay. Yet, despite the evidence that there is a high degree of open trading in these species, the complexity of the international legal frameworks regulating these transactions makes it difficult to ascertain their legality. Nevertheless, at least a subset of these sales are probably unlawful.

Finally, J. Mitchell Miller and Holly Ventura Miller provide insight into the computer-facilitated gray market of pseudo-legal marijuana sales in Los Vegas, Nevada. The ethnographic study reveals how various cannabis products are illegally diverted from legal markets to the gray market, and how brokers use the Internet in clever ways to advertise their products and services to a public that is likely unaware that they are engaging in illegal activities by skirting the regulations and tight control of the legal market.

Taken together, these three papers highlight the tremendous difficulties with regulating e-commerce. While the Dark Web provides an environment to conduct illegal transactions with minimal risk, it turns out that the Dark Web may be unnecessary for many illegal cyber-purchases. Given the surface web is convenient, widely available, and scarcely policed, many cybercriminals simply commit their crimes in the open. Using the language of Routine Activity Theory again, the internet—Dark or Surface—is an environment largely devoid of capable guardians.

Cybercrime: Victimization, Perpetration, and Techniques

As a whole, I believe these nine papers speak to the current state and future promise of cybercriminology. Currently, we are building a large body of empirical studies that speak to patterns of victimization and perpetration. With respect to victimization, we have learned a lot about who is likely to be victimized and how the patterns of victimization vary by type of cybercrime. We also have a good understanding of the activities that increase the likelihood of victimization, the emotional and financial costs of being a victim, and how people view victims depending on the setting and type of victimization. The body of evidence supporting a slightly modified version of Routine Activity Theory/Lifestyle-Exposure Theory is increasingly impressive, and the papers by Marttila, Koivula, and Räsänen as well as the article by Marcum and Higgins offer additional support for aspects of this theoretical approach.

Similarly, our understanding of cybercrime perpetration has expanded exponentially in recent years. While finding samples of cybercriminals is always a challenge, the growing body of evidence suggests that the behavior of cybercriminals is largely explained by the same set of factors that can account for the behavior of more traditional criminals. That is, cybercriminals tend to have low levels of self and social control, are largely unsupervised, experience strains, and learn the how, when, and

why of their crimes from their associates. The papers in this issue offer additional support for techniques of neutralization, social learning theory, and self-control theory. While there are nuanced differences in how some criminogenic factors play out in the virtual and offline worlds, our existing theories appear to be robust as many of our theories apply to both online and offline criminal behavior. A number of the differences that exist largely relate to the asynchronous nature of many online interactions. The fact that online interactions can occur synchronously as well as asynchronously expands our networks and provide additional opportunities for others beyond our immediate environment to influence us and for us to commit crimes. The full ramifications of these changes in social networks, criminogenic forces, and criminal opportunities are not understood; however, we understand these far better today than we did even just a few years ago.

We also have a far greater understanding of the techniques of committing cybercrimes. We know considerably more about the use of the Dark Web to find and purchase illegal goods and services, and we have learned that the Surface Web plays a significant role in computer-dependent crimes. Moreover, as the article by Miller and Miller highlights, information technology has helped blur the line between legal, pseudo-legal, and illegal behaviors. What work in this area really highlights is how difficult it is to monitor and police the internet. While there is certainly social control exercised on the internet, there are limits to the effectiveness of this control (see Hawdon et al., 2017). Yet, by understanding the patterns of victimization, the underlying causes of perpetration, and the techniques that facilitate cybercrime, we become better armed in designing strategies to prevent it, defend against it, mitigate its adverse effects, and prosecute those who commit it. All of the articles included in this issue further that understanding.

The Special Issue

The process of selecting the articles for this special issue was perhaps unusual but also rather intensive. The process began by me inviting a group of scholars to submit manuscripts for the special issue. I selected these scholars because I knew of their work and was confident they would submit quality papers that covered a wide range of topics in the area of cybercrime. After discussing their planned submissions with the authors to assure there would be good topic coverage, the authors submitted their paper. An anonymous scholar and I reviewed these initial submissions (the anonymous scholar served as a typical double-blind reviewer). Each contributing author also reviewed one or two of the included articles. Authors then revised their work based on the reviewers' comments and resubmitted the papers. Each contributing author was then asked to read all nine revised papers. Then, the authors and I took advantage of the brief pause in the COVID-19 pandemic and gathered for a two-day workshop in Asheville, North Carolina as part of the Center for Peace Studies and Violence Prevention's annual research workshop program. The lone exception to this was our Finnish colleagues who were unable to get a special visa to visit the U.S. at that time. These colleagues joined the workshop via Zoom. The authors/workshop participants then discussed and provided feedback on all of the articles.

The authors then made final revisions to their papers based on these discussions. Thus, these papers have been through three rounds of revisions. As the editor of the special edition, I am proud of the finished product.

References

Albanese, J. S. (2005). Fraud: The characteristic crime of the 21st Century. *Trends in Organized Crime, 8*, 5–16.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608.

Federal Bureau of Investigation. (2021). *2020 Internet crime report*. U.S. Government Printing Office.

Hawdon, J., Costello, C., Ratliff, T., Hall, L., & Middleton, J. (2017). Conflict management styles and cybervictimization: An extension of routine activity theory. *Sociological Spectrum, 37*(4), 250–266.

Hawdon, J., Parti, K., & Dearden, T. E. (2020). Cybercrime in America amid COVID-19: The initial results from a natural experiment. *American Journal of Criminal Justice, 45*, 546–562.

Morgan, S. (2020). Cybercrime to cost the World $10.5 Trillion Annually by 2025. *Cybercrime Magazine*, November 13, 2020. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Reinhart, R. J. (2018). One in four Americans have experienced cybercrime. *Gallup Politics*. https://news.gallup.com/poll/245336/one-four-americans-experienced-cybercrime.aspx

Roser, M. H. R. & Ortiz-Ospina, E. (2015). "Internet". *Published online at OurWorldInData.org.* Retrieved from: 'https://ourworldindata.org/internet' [Online Resource]

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review, 22*(6), 664–670.

We Are Social, & DataReportal, & Hootsuite. (2021). Global digital population as of January 2021 (in billions) [Graph]. In *Statista*. Retrieved September 24, 2021, from https://www.statista.com/statistics/617136/digital-population-worldwide/

James Hawdon is a professor of sociology and Director of the Center for Peace Studies and Violence Prevention at Virginia Tech. Dr. Hawdon's research focuses on how communities influence the causes and consequences of violence. He is currently researching how online communities influence online hate, extremism, political polarization, and cybercrime. Since 2013, he and his colleagues have collected multiple waves of data on online hate speech and extremism in the Finland, France, Germany, Poland, Spain, the United Kingdom, and the United States. His recent work has been funded by the National Institute of Justice, the National Science Foundation, and The Commonwealth Cyber Initiative. He has published eight books and over 130 articles, books chapters, and technical reports.