American Journal of Criminal Justice (2019) 44:230–247
https://doi.org/10.1007/s12103-018-9457-3

Using Labeling Theory as a Guide to Examine the Patterns, Characteristics, and Sanctions Given to Cybercrimes

Brian K. Payne[1] · Brittany Hawkins[2] · Chunsheng Xin[1]

Received: 6 August 2018 / Accepted: 4 October 2018 /
Published online: 3 November 2018

Abstract

Over the past decade, reports of cybercrime have soared across the globe. Criminologists agree that the increase in cybercrime stems from technological advancements that have changed all facets of societal interactions. While it is agreed that technology has shaped cybercrime, there is less understanding about the dynamics of cybercrime. In particular, some researchers have explored whether these offenses are simply traditional types of crime that are now carried out through different strategies, while others have argued that cybercrimes are, in fact, new types of crime. This ambiguity potentially limits prevention and intervention strategies. In an effort to build our understanding about cybercrime within a criminological framework, in this study we use labeling theory as a guide to examine the patterns, characteristics, and sanctions associated with a sample of cybercrimes with an aim towards identifying how these offenses are socially constructed in comparison to traditional crimes, white-collar crimes, and international crimes. In doing so, our hope is to further determine how cybercrime can be understood within current criminological thinking.

Keywords Cybercrime · Cybersecurity

Introduction

A review of the history of crime shows that types of crime, definitions of crime, and responses to crime have changed over time. Cybercrime is perhaps the most recent evolution in the world of crime. Part of the reason for this evolution lies in the new types of technology that have made these offenses possible. These new technologies have

This research is supported in part by NSF under grant DGE-1723635 and grant CNS-1659795.

✉ Brian K. Payne
bpayne@odu.edu

[1] Old Dominion University, Norfolk, VA, USA

[2] Claflin University, Orangeburg, SC, USA

altered all types of behaviors individuals perform. In fact, recent research shows that individuals spend nearly 11 h a day using some form of technology (Howard, 2016).

Criminologists have debated how the evolution of cybercrime resulted from new types of crime being created as well as how this evolution new strategies for committing traditional forms of crime (Brenner, 2004; Wall, 1999; Yar, 2006). Building on these efforts to more broadly understand cybercrime, we use labeling theory as a guide, to consider whether cybercrime can be understood as a traditional crime, a white-collar crime, an international crime, and a socially constructed crime. Better understanding about how to classify cybercrime will inform appropriate prevention and intervention strategies. As well, accurately categorizing cybercrime provides insight into the causes and consequences of these offenses. Criminologist Peter Grabosky (2001) has asked whether cybercrime is "old wine in new bottles" or "new wine," while David Wall (1999) questions whether the behavior is "new wine" in "no bottles." Another question to ask is whether cybercrime is a "wine cellar," with various categories of crime (or wine) captured under the broader domain of cybercrime.

Review of Literature

Cybersecurity has escalated as an international concern. Interestingly, as a threat to our critical infrastructure, public safety, and overall homeland security, the scholarly response to cybersecurity has included a range of disciplines such as computer science, computer engineering, electrical engineering, and information technology. Research from these disciplines has been useful for developing computer hardware and software that enhances the security of various technological devices.

To a lesser degree, but in a worthwhile way, criminologists have begun to address cybersecurity. Generally speaking, these criminological studies focus on two topics: (1) explorations of specific types of cybercrimes and (2) theory tests of various cyber offenses. This first body of research has examined crimes such as digital piracy (Gunter, Higgins, & Gealt, 2010; Yu, 2011), cyber bullying (Antoniadou & Kokkinos, 2015; Marcum, Higgins, Freiburger, & Ricketts, 2012a), child pornography (Lollar, 2013; Seigfried-Spellar, 2013), and identity theft (Holt &Turner, 2012; Wall, 2013). One basic theme underlying these studies is that technological changes created new opportunities for criminal behavior.

In terms of theory tests on various cyber offenses, researchers have considered how theories such as self-control theory (Holt, Bossler, & May, 2012; Higgins, Marcum, Freiburger & Ricketts, 2012; Marcum, Higgins, Wolfe & Ricketts, 2011; Reyns, Fisher, Bossler & Holt, 2018), differential association/learning theory (Morris and Higgins, 2010), neutralization theory (Marcum et al., 2011), and routine activities theory (Leukfeldt and Yar, 2016; Williams, 2016) can be used to explain cyber offending. Perhaps the safest conclusion to make is that no criminological theory perfectly explains different types of cybercrime. Instead, as one author team recently wrote, "traditional theories tend to explain a particular aspect of cybercriminal activity" (Kethineni, Cao & Dodge, 2018, p. 143). In other words, while not fully explaining cyber offending, some criminological theories can be used to explain different aspects of the behavior.

Labeling theory is one such theory that can be used to understand the dynamics of cyber offending, especially the societal response to the behavior. This theoretical perspective is concerned with how behaviors come to be conceptualized as crime, the way members of society assign criminal labels, whether differences exist in the assignment of those labels, and the degree to which labels result in additional stereotypes.

Collectively, this past body of literature on types of cybercrime and theory tests of cyber offending shows the breadth of cybercrime. From this research, it seems that cybercrime has been labeled (or defined) as a traditional crime, as white-collar crime, as international crime, and as socially constructed crime. In the following section, we expand on these conceptualizations and provide a basis for using labeling theory as a guide to better understand cyber offending.

Cybercrime as a Traditional Crime

Most introductory criminology courses devote significant attention to defining crime. Common typologies for defining crime focus on whether the behavior is *illegal* (Brenner, 2007), *harmful* (Friedrichs, 2009), or *deviant* (Inderbitzin, Bates & Gainey, 2016). Each of these frameworks can be used to define different types of cybercrime. For instance, *legal definitions of cybercrime* would point to cybercrime as "the use of computer technology to commit crime; to engage in activity that threatens a society's ability to maintain internal order" (Brenner, 2007, p. 386). Addressing cybercrime as illegal acts means that offenders would be punished and sanctioned in ways consistent with the criminal law.

Defining cybercrime as a *harmful behavior* would focus on the specific and general harms that arise from cyber offending. It is widely accepted that cybercrime costs far more than other crimes. Data from the Internet Crime Complaint Center (2017) shows $4.63 billion in total losses to Internet crime in 2016. In comparison, data from the FBI shows a total of 465 million in total losses to robberies that same year (FBI, 2017). To be sure, costs of cybercrime are not isolated to economic costs. Certain types of cybercrime (e.g., bullying, harassment, stalking, and revenge porn) harm victims emotionally. The point here is not to suggest that the consequences of cybercrime are worse than other crimes; rather, the basic point is that cybercrime is similar to other crimes in that it can (and does) harm victims.

Traditional definitions of cybercrime might also focus on the *behavior as a deviant construct*. From this perspective, cybercrime is behavior that breaks societal norms, whether it is illegal or not. Consider instances when individuals are verbally aggressive online. It is not illegal to make mean comments in a web forum. This behavior, however, can be seen as against societal norms and standards. The same goes for cyber harassment. Certain types of harassment (e.g., "sending excessively needy or disclosure messages") are not illegal, but would certainly be deviant (see Wick et al., 2017). Likewise, Internet addiction is not criminal, but it may be seen as deviant, and it is certainly a topic of interest to cyber criminologists (Ineme, Ineme, Akpabio & Osinowo, 2017).

Some types of cybercrime might also be defined as *immoral*. Internet child pornography is the clearest example. Societal values dictate that this behavior is immoral. Regardless of religious or cultural background, most individuals agree that child

pornography is immoral. Other types of cybercrimes that might be defined as immoral include public displays of terrorism on the Internet and spying through a computer user's web camera.

This review is not meant to be exhaustive. Our intent is to simply show that traditional strategies for defining crime can be used to define cybercrime. From this perspective, cybercrime is "old wine in a new bottle."

Cybercrime as a White-Collar Crime

Some criminologists have explored cybercrime as a type of white-collar crime. Using Edwin Sutherland's concept and definition (e.g., white-collar crime is "a crime committed by a person of respectability and high social status in the course of his occupation"), it has been argued that certain types of cybercrimes are white-collar offenses (Payne, 2016). Obviously, not all cybercrimes are white-collar crimes; however, it is not clear the degree to which white-collar crimes comprise all forms of cybercrimes. Indeed, few studies have considered cybercrime solely as a form of white-collar crime.

Despite this lack of research on "cyber white-collar crimes," countless examples have been provided in the media. Consider the following example:

> A contract security guard at the North Central Medical Plaza on North Central Expressway in Dallas, pleaded guilty . . . to felony offenses related to his compromising and damaging the hospital's computer system . . . [the defendant], a/k/a "Ghost Exodus," 25, of Arlington, Texas pleaded guilty to an indictment charging two counts of transmitting a malicious code. . . . [The defendant] gained physical access to more than 14 computers located in the North Central Medical Plaza, including a nurses' station computer on the fifth floor and a heating, ventilation and air conditioning (HVAC) computer located in a locked room. (U.S. Department of Justice, 2010).

Two elements of this example make it a white-collar crime: (1) it was committed at work and (2) the offender committed the offense as part of his employment role.

While researchers rarely explore cybercrime as a white-collar crime, the Ponemon Institute conducts an annual study exploring how businesses experience cybercrime. This annual study recently found that one-third of the cyber victimizations were attributed to malicious insiders (Ponemon, 2015). The Ponemon findings showed that these offenses take longer to address than cybercrimes by outsiders. Specifically, once an inside attack was identified, it took 54 days to address while other attacks could be addressed in less than half the time. Ponemon's research also shows that the costs from insider attacks were much higher (at $144,542 in comparison to $1900 for viruses and worms).

Cybercrime as an International Crime

The very nature of cyber technology is that cybercrimes are not tied to any country borders. As a result, these offenses can potentially be defined as international crimes. The way that the crimes travel across international borders can result in jurisdictional

issues (Speer, 2000). Who has jurisdiction over cybercrimes that cross country borders – the location where the crime originated or the location where the victim resides? One legal expert notes that in some cybercrimes, it could be that no government has jurisdiction or multiple countries might claim jurisdiction for the same offense (Brenner, 2006). Taken together, the international nature of cybercrime makes it harder to respond to the behaviors (Smith, 2015).

The "transnational implications" of cybercrime have been hailed as among the most "remarkable developments relating to crime in the digital age" (Grabosky, 2001, p. 243). In the words of one legal expert, "Determining which country has jurisdiction for purposes of a criminal prosecution may establish whether conduct will be a crime, how the crime will be defined, and how it will punished" (Podgor, 2004, p. 97). This same scholar concludes that some cybercrimes "will fall into national jurisdiction, others to transnational, and others might be designated 'international crimes'" (p. 108).

Cybercrime as a Socially Constructed Crime

It is also important to question whether and how cybercrime can be characterized as socially constructed offenses. Specifically, the notion of social construction refers to the possibility that certain crimes are socially constructed as illegal acts. Drug crimes are frequently cited as an example of socially constructed offenses (Goode, 2014). For instance, Goode notes that drugs are essentially substances that society defines as drugs and that illegal drugs are those drugs that society chooses to label as illegal.

Criminologists have demonstrated how various other types of crimes can be seen as social constructions. Few criminologists have explored the social construction of cybercrimes, but those who have shed some light on the way that some cybercrimes can be seen as socially constructed. For example, one researcher has defined cyber identity theft as a "social construction" rather than a "legal construction" based on the fact that the behaviors are not new (Wall, 2013). Elsewhere, this same researcher has noted that the "concept of cyberspace has developed from science fiction into a socially constructed reality" (Wall, 1999, p. 105).

The social construction of crime occurs through various communication efforts. The media/news is perhaps one of the most prominent strategies to communicate about crime. In fact, a branch of criminology known as "newsmaking criminology" explores interactions between the news media and criminology (Barak, 1988). Some criminologists have explored how cybercrimes are portrayed in the media (Williams, Bengert, & Ward-Caldwell, 2016) and how politicians construct cybersecurity issues (Hill & Marion, 2016). An examination of 535 news articles focused on cyberterrorism found that "news items with an international focus and concentrating primarily on cyberterrorism also appear to demonstrate an exaggerated conception of the cyberterrorism threat" (Jarvis, Macdonald & Whiting, 2017). One study attributed an increase in the use of the word cybersecurity in the U.S. to the election of President Barack Obama in 2008 (Reijmer & Spruitt, 2014). Indeed, the news often reports on the comments made by politicians. Not surprisingly, reviews of presidential speeches by recent U.S. presidents found that the speeches constructed cybersecurity from a fear-based perspective rather than a policy-based perspective (Hill & Marion, 2016).

Using Labeling Theory to Understand Cyber Offending

From our perspective, the tenets of labeling theory offer a framework which can be used to guide our understanding about cybercrime. Three specific themes in labeling theory are relevant in this study: (1) variations in how labels are assigned, (2) the consequences of labeling, and (3) the distribution of labels after they are initially applied. Regarding variations in how labels are assigned, criminologists have recognized that demographic characteristics, particularly gender and race, impact the assignment of criminal and deviant labels. On the one hand, the way that gender identity is assigned may alter criminal justice responses to offenses by females. On the other hand, many researchers have concluded that labeling processes contribute to disparate treatment of racial minorities in the justice system (Goode, 2014). While labeling theory has rarely been applied in this context to cybercrime, one can't help but draw attention to the distinction between "White Hat" hackers and "Black Hat hackers." The former refers to hackers who engage in hacking behaviors as a strategy to help businesses protect their network. Black hat hackers, in turn, are the more nefarious hackers who engage in criminal behaviors. While this study is not able to specifically explore race, attention is given gender and nationality status in relation to the assignment of a criminal label for cyber offenders.

A second labeling theory theme relevant to this study has to do with the consequences of labeling. Derived from the notion of "self-fulfilling" prophecy, this theory assumes that labels result in subsequent behaviors by offenders that may promote wrongdoing. More immediately, though, the application of the criminal label results in criminal sanctions for offenders. The question in this study is whether sentences vary across types of cybercrime.

A third theme labeling theory theme surfacing in this study centers around the distribution of criminal labels. More specifically, once a label is assigned by justice officials, how do others, such as the media, apply the criminal label. A basic assumption of labeling theory is that secondary deviance occurs after the deviant individual has gone through a process of labeling by both primary and secondary contacts. Whether the media – as a secondary contact – applies criminal labels across offenders and offense types differently in cybercrime cases is addressed in this study.

The Current Study

Tying together these themes, the current study explores how cybercrimes prosecuted by federal authorities in the United States can be conceptualized. To provide a framework for understanding cybercrime, in this study the following questions are addressed:

- What are the characteristics of cybercrimes prosecuted by federal authorities in the United States?
- Are criminal labels assigned differently to male and female cyber offenders?
- Are criminal labels assigned differently to domestic and international cyber offenders?
- Does the criminal label result in different types of sentences based on gender and country of origin?

- Are there offense, gender, and country of origin differences in the way labels are assigned in press releases and news articles?

Expanding our understanding of cybercrime will help to identify appropriate prevention, intervention, and response strategies. The degree to which traditional crime-prevention strategies can be utilized with cybercrime is not yet fully understood. By determining how cybercrime can be characterized, steps that are needed to better address these offenses will become apparent.

Methods

To expand our understanding about the characteristics of cybercrime, its patterns, and the criminal justice system's response to cyber offending, we content analyzed 119 cybercrime cases prosecuted by the U.S. Department of Justice between 2013 and June 2017. The content analysis used was manifest content analysis rather than thematic content analysis (see Berg & Lune, 2011). In particular, words and patterns were analyzed focusing on the commonly accepted meanings of those words. The cases were located on the DOJ's website. The DOJ periodically publishes press releases of ongoing cases on their website. In summer 2017, the second author content analyzed all cases that were included on the website by filtering the "cybercrime" topics on the website. For this study, we included only those offenses where a sentence was announced in the press release. For the 2013 and 2014 years, we culled cases from the DOJ's Computer Crime and Intellectual Property Section website because those years were not included on the main page of DOJ press releases.

A coding sheet was developed to assist in the coding. The coding sheet included information about the offender, offense, sentence, and press release. Variables related to the offender included gender, age, and nationality. Variables related to offense included number of offenders, type of offense, and location of the offense. Variables related to the sentence included type of sentence given to the offender (prison/jail, probation, fine, restitution) and length or amount of each sentence. Variables related to the press release included number of words in the press release and number of news articles published about the case. This latter variable was coded by searching in Google by name of offender. It provides a superficial indication of the degree to which offenses were socially constructed in the media.

Findings

What Are the Characteristics of Cybercrimes Prosecuted by Federal Authorities in the U.S.?

Table 1 shows the characteristics of the cases appearing on the cybercrime link on the Department of Justice's press release website. The most common offenses were hacking, fraud schemes, and trafficking counterfeit goods. Regarding the counterfeit goods offenses, many of them did not have a direct connection to cybercrime, but were presumably included in the cybercrimes press releases on the DOJ website because of

Table 1 Sample characteristics

	n	%
Type of Crime (Legal Label)		
Hacking	24	20.3
Fraud Scheme	23	19.5
Conspiracy	7	5.9
Cyberstalking	5	4.2
Identity Theft	4	3.4
Trafficking Counterfeit Goods	21	17.8
Cyber Attacks	2	1.7
Money Laundering	1	.8
Wiretapping	1	.6
Theft	1	3.4
Other	26	22.6
Gender		
Male	108	91.5
Female	10	9.5
Co-Defendants		
Yes	63	53.8
No	54	46.2
White-Collar Crime		
Yes	34	29.3
No	92	70.1
Country of Origin		
U.S.	83	70.3
Foreign	35	29.7
Offender Country		
U.S.	83	70.3
China	8	6.7
Nigeria	5	4.2
Romania	5	4.2
Canada	2	1.7
Russia	2	1.7
Vietnam	2	1.7
Cameroon	1	.8
Estonia	1	.8
Germany	1	.8
Iran	1	.8
Kosovo	1	.8
Moldova	1	.8
Philippines	1	.8
Senegal	1	.8
South Korea	1	.8
Turkey	1	.8

Table 1 (continued)

	n	%
Ukraine	1	.8
Sanction		
Prison	109	91.6
Restitution	47	39.5
Fine	12	10.1
Probation	7	5.9
	x	s.d.
# of news articles about case	9.44	4.61
# of words in press release	540.23	286.03
Prison length (months)	80.57	175.14

the digital nature of counterfeiting goods and labels. As well, the fact that the same section that prosecutes cybercrime also addresses intellectual property offenses explains why these cases appeared in the search for cybercrimes in DOJ press releases.

Like most other types of crimes, the vast majority of offenders were males. The average age of the male cyber offenders was 35.6 years (s.d. = 12.58), while the average age of female offenders was higher at 51.5 (s.d. = 10.95) ($t = 3.85$, $p < .001$). Unlike many other offenses, more than half of the cases involved situations where more than one offender was involved in the case. Also unlike other types of traditional offenses, the offenders were much more diverse in terms of nationality. While the majority of offenders were from the U.S., roughly 30% were from other countries. In fact, seventeen other countries were represented, with China ($n = 8$), Nigeria ($n = 5$), and Romania (n = 5) having the most convicted cyber offenders. The international offenders tended to be younger than U.S. offenders. Their average age was 30.32 (s.d. = 14.38), while the average age of U.S. cyber offenders was 39.12 (s.d. = 12.51) ($t = 3.32$, $p < .01$).

Nearly a third of the offenses were characterized as white-collar offenses. For these cases, a legitimate occupation held by the offender or victim was a primary factor in the crime. Cases in which offenders used an illegal or illegitimate occupation to perpetrate the offenses were not included in this count.

What Patterns Appear in the Types of Crimes Perpetrated by Cyber Offenders?

To explore the patterns surrounding the cybercrimes considered in this study, we explored the gender dynamics, international dynamics, and age dynamics of the crimes. Tables 2, 3, and 4 show the findings from this analysis. Regarding gender dynamics, while females were not as likely to be involved in offending, two statistically significant findings were uncovered and one finding that approached significance is noteworthy. First, a portion of the analysis focused on specific types of crime and gender patterns, with comparisons made between each specific crime type and the other types as a group. When comparing fraud to all other offenses, females are more likely to be accused of cyber fraud (Chi square = 9.29,

Table 2 Gender by legal classification of crime

	Male	Female
Hacking	24 (22.4)	0 (0.0)
Fraud	18 (16.8)	5 (50.0)
Conspiracy	7 (6.5)	0 (0.0)
Cyberstalking	5 (4.7)	0 (0.0)
Identity theft	3 (2.8)	1 (10.0)
Trafficking	18 (16.8)	3 (30.0)
Cyber attacks	2 (1.9)	0 (0.0)
Money Laundering	1 (0.9)	0 (0.0)
Wiretapping	1 (0.9)	0 (0.0)
Theft	3 (2.8)	0 (0.0)
Other	25 (23.4)	1 (10.0)

$p < .01$). Half of the females committed fraud, in comparison to less than one in six male offenders. Second, when comparing specific types of computer hacking and all other offenses, statistically significant differences were found (Chi Square = 4.42, $p < .028$). None of the female offenders were convicted of hacking offenses, while more than one in five male offenders were. Third, while not statistically significant (due to low cell sizes), it is noteworthy that 8 of the 10 females were involved in offenses with co-defendants, while just over half of the male offenders had co-conspirators. This result approached significance (Fisher's exact = .078). While not statistically significant, the finding points to theoretical significance.

Regarding international dynamics and cybercrime, five differences were found, each suggesting that international offenders were more prone to commit monetary offenses than U.S. offenders. Note that cyber offenders could commit multiple types of monetary offenses and these types may overlap with one another. First, offenders from the

Table 3 Country of origin by legal classification of crime

	U.S.	Foreign
Hacking	16 (19.5)	8 (22.9)
Fraud	14 (17.1)	9 (25.7)
Conspiracy	5 (6.1)	2 (5.7)
Cyberstalking	5 (8.1)	0 (0.0)
Identity theft	3 (3.7)	1 (2.9)
Trafficking counterfeit goods	15 (18.3)	6 (17.1)
Cyber attacks	2 (2.4)	0 (0.0)
Wiretapping	1 (1.2)	0 (0.0)
Theft	3 (3.7)	1 (2.9)
Other	18 (22.0)	8 (22.9)

Table 4 Gender by sanction

	Male	Female
Prison/Jail		
Yes	100 (92.6)	9 (90.0)
No	8 (7.4)	1 (10.0)
Fine		
Yes	10 (9.3)	2 (20.0)
No	98 (90.7)	8 (80.0)
Restitution		
Yes	43 (39.8)	4 (40.0)
No	65 (60.2)	6 (60.0)
Probation		
Yes	7 (6.5)	0 (0.0)
No	101 (93.5)	10 (100.0)
Community Service		
Yes	8 (7.4)	0 (0.0)
No	110 (92.6)	10 (100.0)

United States were less likely to commit cyber theft offenses than offenders from other countries. In all, 14.5% of the U.S. offenders were convicted of cyber theft while 28.6% of offenders from outside the U.S. were convicted of theft (Chi Square = 3.23, $p < .05$). Second, offenders from outside the U.S. were more likely to be convicted of wire fraud than U.S. offenders. Nearly a third of non-U.S. offenders were convicted of wire fraud, in comparison to 13% of U.S. offenders (Chi Square = 5.36, $p < .05$). Non-U.S. offenders were also more likely to be convicted of fraud (as a general crime type) than U.S. cyber offenders. Nearly 30% of non-U.S. offenders were convicted of fraud, in comparison to just under 10 % of U.S. offenders (Chi Square = 6.82, $p < .01$). Non-U.S. offenders were also more likely to commit money laundering, with one-fifth of them committing this offense, and just one of the U.S. offenders being convicted of money laundering (Fisher's Exact Test = .001). Finally, non-U.S. offenders were more likely to commit bank fraud than U.S. offenders. One-fifth of the non-U.S. offenders committed bank fraud while none of the U.S. cyber offenders were convicted of bank fraud (Fisher's Exact Test = .000).

What Sanctions Are Given to Cyber Offenders?

Perhaps not surprisingly, prison was the most common sentence given to the cyber offenders, with 100 of the offenders being sentenced to prison. The average prison sentence was 80.57 months (s.d. = 175.14). Restitution was the most common sanction, with nearly 40% of the offenders being ordered to pay restitution. Fines ($n = 10$), community service ($n = 8$), and probation ($n = 7$) were less frequently imposed.

We examined patterns surrounding the sanctions (see Tables 4, 5, 6 and 7). No gender differences were found in how often the sanctions imposed. Some differences were found between U.S. and international offenders. U.S. offenders were more likely to be ordered to pay restitution. Among U.S. offenders, 46% were ordered to pay

Table 5 Country of origin by sanction

	U.S.	Foreign
Prison/Jail		
Yes	74 (89.2)	34 (97.1)
No	9 (10.8)	1(2.9))
Fine		
Yes	6 (7.2)	6 (17.1)
No	77 (72.6)	29 (82.9)
Restitution		
Yes	38 (45.8)	9 (25.7)
No	45 (54.2)	25 (75.3)
Probation		
Yes	7 (8.4)	0 (0.0)
No	76 (91.6)	35 (100.0)
Community Service		
Yes	8 (9.6)	0 (0.0)
No	75 (90.4)	35 (100.0)

restitution, while one-fourth of international offenders were imposed a sentence of restitution. In addition, the average prison length for international offenders was much higher at 159 months in comparison to average prison length of 43 months for U.S. offenders ($t = -2.29$, $p < .05$). The average was inflated with a handful of long sentences for international offenders.

How Are these Offenses Socially Constructed in the Media?

Our focus on how the cyber offenses are socially constructed in the media focused on two variables: the number of words included in the DOJ press release and the number of times the case described in the press release appeared in online news outlets. The average press release included 540 words (s.d. = 286.03). The average number of news articles about each case was 9.44 (s.d. = 4.61) articles.

To identify gender, international, and offense-type dynamics in relation to their social construction, we conducted a series of cross-tabulations (see Tables 6, 7 and 8). Several differences were found. These included:

Table 6 Gender by prison length, age, and newsmaking

	Male x (s.d.)	Female x (s.d.)	t
Age	35.61 (12.58)	51.5 (10.95)	3.85***
Prison/Jail	84.02 (181.23)	41.44 (22.38)	−.70
Number of articles about case	9.68 (4.65)	6.8 (3.61)	−1.9*
Number of words in press release	550.45 (296.50)	418.2 (98.9)	−3.1**

*p < .05, **p < .01, ***p < .001

Table 7 Country of origin by prison length, age, and newsmaking

	U.S. x (s.d.)	Foreign x (s.d.)	t
Age	39.12 (12.51)	30.32 (14.38)	3.22**
Prison/Jail	43.2 (43.5)	159.41 (293.93)	−2.29*
Number of articles about case	8.35 (3.22)	11.97 (6.24)	−3.25**
Number of words in press release	482.83 (228.55)	671.43 (357.04)	−2.88*

*p < .05, **p < .01, ***p < .001

- Cybercrime press releases were longer for males than for females. The average press release for males was 550 words, in comparison to an average of 418 words for females ($t = -3.1$, $p < .01$).
- A higher number of news articles were published about the male cybercrime offenders. For each male cyber offender, an average of 9.68 articles were published, in comparison to an average of 6.8 articles for female offenders ($t = -1.9$, $p < .05$).
- Cybercrime press releases for international offenders were longer than the press releases were for U.S. offenders. The average length of press releases for international offenders was 671 words, in comparison to an average length of 482 words for U.S. offenders ($t = -2.88$, $p < .05$).
- A higher number of articles were published about international cybercrime offenders than U.S. cybercrime offenders. For each international cyber offender, an

Table 8 Newsmaking by cybercrime types

	x	s.d.
Average number of words in press release		
Hacking	634.17	409.55
Fraud	573.57	225.48
Conspiracy	523.0	346.63
Cyberstalking	601.2	226.8
Identity theft	603.5	186.17
Counterfeit goods	406.29	198.53
Theft	523.0	137.32
Other	511.46	287.17
Average number of news articles published		
Hacking	10.63	5.31
Fraud	10.96	5.48
Conspiracy	11.67	5.16
Cyberstalking	10.8	2.38
Identity theft	10.00	4.08
Counterfeit goods	6.20	3.57
Theft	9.34	2.5
Other	9.46	3.38

average of nearly 12 articles were published, in comparison to an average of 8.35 articles for U.S. offenders ($t = -3.25$, $p < .01$).
- Hacking press releases were the longest at 634 words, while trafficking on counterfeit good were the shortest press releases at 406 words.
- Conspiracy cybercrime cases led to the highest number of news articles while trafficking in counterfeit goods led to the fewest articles. Hacking, fraud, and cyberstalking cases led to a comparatively high number of news articles.

Discussion

Our research shows the complexities of cybercrime. It is similar to traditional crimes in that they tend to be committed by males and younger offenders. At the same time, many of the offenses are, in fact, white-collar crimes and many can also be characterized as international crimes crossing international borders. More than half of the crimes involved co-defendants. Also, there is significant variety in the specific types of cybercrimes and the U.S. government responds somewhat aggressively to these offenses by issuing prison sentences somewhat routinely, with international offenders receiving longer prison sentences than U.S. offenders. In addition, the social construction of cybercrimes (defined by number of news articles and length of press release) varied across offense and offender types with cybercrimes involving males, international offenders, and hacking offenses having more news articles and longer press releases. Collectively, these findings can be tied to past cybercrime research. After discussing the connections to past cybercrime research, the implications for policy, theory, and research arising from these findings are considered.

One finding from our study that is consistent with past research is the finding that the vest majority of cyber offenders were male offenders rather than female offenders (Bachmann, 2010). As Bachmann has noted, the low number of female hackers makes it difficult to draw conclusions about patterns among this population. One conclusion that can be drawn, however, is that computer hacking appears to be dominated by male offenders. However, it is plausible that our results are driven by the fact that our sample includes offenders who had received a criminal label. Other types of cyber offending (such as cyber bullying) may actually have higher numbers of female offenders, particular when considering self-reported offending rather than official conviction reports (Marcum et al., 2011).

Finding that many of the offenses involved multiple offenders is also consistent with past research on cyber offenders. An earlier review of Department of Justice cases found that more than who of the cybercrime cases involved multiple offenders (Lusthaus, 2012). One expert even suggested the presence of "cybergangs" to describe cybercrimes perpetrated by multiple offenders (Smith, 2015). These cybergangs come together because of their expertise, communicate online, maintain online reputations, cover the entire globe, and are typically driven by profit (Smith, 2015). While our research did not identify the presence

of specific "cybergangs," the fact that the majority of cases involved multiple offenders lends credence the earlier research showing the interactive nature of the cybercrimes.

The international nature of cybercrime we found in our study is consistent with prior research (Kigerl, 2013; Li, 2015). Research by Kigerl (2065) suggests that types of cybercrime may vary across countries. Similarly, our findings suggested that certain types of theft-related offenses were more likely to originate from outside the U.S. What's not clear, though, is whether our patterns reflect patterns of behavior on the parts of offenders or law enforcers. Labeling theorists would question whether labels are being assigned differently to international offenders.

One of our findings in the area of sentencing severity is inconsistent with past research. A study by Marcum, Higgins, and Tewksbury (2012b) found that longer prison sentences were given to female cyber offenders than male cyber offenders. The differences in our two studies is potentially due to a sampling effect. The Marcum study focused on state level offenses, while the current study focused on federal offenses (which tend to include more serious offenses across all types of offenses). We agree with Marcum and her research team who point to the need for more research on sentencing of cybercrime offenders in general and on convicted female offenders specifically.

Based on our findings, we can point to four different policy implications. First, given the high number of co-conspirators, cybercrime law enforcement investigations would be bolstered by searching for multiple offenders. Others have called for investigations of multiple offenders in white-collar crime cases, with investigators searching for the "least culpable" offender initially in order to get them to share information about co-offenders with authorities (see Payne, 2016). It would seem that the same recommendation can be made for cybercrime investigations.

Second, given the international nature of cybercrime, and the fact that even domestic cases will involve multiple criminal justice agencies, it is imperative that law enforcement and prosecution officials be prepared to collaborate across jurisdictions. Collaboration, particularly across national borders, can be challenging. These challenges, however, must be addressed and overcome in order to effectively deal with cybercrime cases.

Third, the nature of press releases by government officials requires some attention. In particular, if the goal of the press releases is to garner additional attention in the news, government officials would be advised to develop longer press releases (given that longer releases seemed to produce more news articles). In addition, if the purpose of the high number of prison sentences given to cyber offenders is to deter others from committing crime, then officials should make sure that members of the public are receiving information about these prison sentences.

Fourth, cyber criminologists should work with law enforcement and prosecutors to shape awareness about cybercrime. It has only been in the past decade that we have seen an increase in academic understanding about cybercrime. At the same time, more law enforcement efforts have been devoted to cybercrime. Cyber criminologists can play a central role in helping to socially construct accurate definitions and conceptualizations of cybercrime.

Labeling theory principles can be used to understand these findings. First, consider the low number of women involved in cyber offending. It is well

established in education literature that women are assigned negative labels that dissuade them from seeking STEM career. This theory would suggest that the low number of women in STEM careers can be traced to the way young girls are dissuaded from taking STEM classes. A parallel argument could be made about cybercrime. In particular, the lower interest in computing among girls reduces the likelihood of offending. So, labels preventing opportunities to learn techniques for offending reduce opportunities for offending.

Second, labels assigned in the media potentially paint a picture of cybercrime that exacerbate these differential labeling. Recall that women had fewer words in their press releases and fewer news articles about their cases while foreign offenders had more words and more articles. On the surface, this suggests that cases involving women are labeled as less serious while those involving foreign offenders are defined as more serious. Interestingly, no differences in number of words or number of articles were found when considering the type of cybercrime. This at least tacitly suggests that decisions to label are driven more by offender characteristics than offense characteristics.

This research is not without limitations. First, the dark figure of cybercrimes is not included as we only focused on cybercrimes resulting in convictions at the federal level in the U.S. government. Crimes that were not detected or reported were not included in our sample. Second, the amount of data included in each press release was determined by those officials releasing the information. Third, cybercrimes prosecuted at the state level or in other jurisdictions were excluded. Finally, our sample represents those offenses that the federal authorities issued press releases about. While a limitation, our understanding about social construction is bolstered by focusing on those offenses that are distributed to the media.

Despite these limitations, our findings point to a number of questions for future cyber criminologists. For example, the role of gender in cyber offending should be further explored. In addition, researchers should further explore those factors that impact sentencing decisions in cybercrime cases. Also, researchers should further examine how to best address cyber white-collar crimes and whether cyber white-collar crimes are substantively different from other forms of cybercrime. Finally, researchers should continue to explore the way that cybercrime is conceptualized and socially constructed across the globe with an aim of determining whether cultural forces shape definitions of cybercrime.

As noted earlier, cybercrime researchers have explored whether cybercrime is "old wine in new bottles," "new wine in old bottles" or something else (Grabosky, 2001; Wall, 1999). Depending on one's perspective, arguments can be made either way – that these are old crimes done with new tools, or that – in some ways – these are new crimes done with new tools. In this study, our findings point to the breadth of cybercrimes –old and new alike. Cybercrimes are similar to traditional crimes; many are international crimes; many are socially constructed offenses; and many are white-collar crimes. Based on these findings, we conclude that rather than characterizing cybercrimes as a type of wine bottle, perhaps it is appropriate to characterize cybercrime as a wine cellar – it includes all types of crimes (wine bottles), some that are old and some that are new. The task at hand for cyber criminologists is to expand their expertise as cyber sommeliers and better understand cybercrimes in its many forms.

References

Antoniadou, N., & Kokkinos, C. (2015). Cyber and school bullying. *Aggression and Violent Behavior, 25*, 363–372.

Barak, G. (1988). Newsmaking criminology. *Justice Quarterly, 5*, 565–587.

Berg, B., & Lune, H. (2011). *Qualitative research methods for the social sciences* (8th ed.). New York: Pearson.

Brenner, S. W. (2007). "At light speed": Attribution and response to cybercrime/terrorism/warfare. *The Journal of Criminal Law & Criminology, 97*(2), 379–475.

Brenner, S. W. (2006). Cybercrime jurisdiction. *Crime, Law, and Social Change, 46*, 189–206.

Brenner, S. W. (2004). Cyber crime metrics: Old wine in new bottles? *Virginia Journal of Law and Technology, 9*(13), 1–52.

Federal Bureau of Investigation. (2017). Crime in the United States, 2016. https://ucr.fbi.gov/crime-in-the-u.s/2016/crime-in-the-u.s.-2016/topic-pages/robbery

Friedrichs, D. (2009). *Trusted criminals*. Belmont, CA: Wadsworth.

Goode, E. (2014). *Drugs in American society* (9th ed.). McGraw Hill.

Grabosky, P. (2001). Virtual criminality: Old wine in new bottles? *Social and Legal Studies, 10*, 243–249.

Gunter, W., Higgins, G., & Gealt, R. (2010). Pirating youth. *International Journal of Cyber Criminology, 4*, 657–671.

Higgins, G., Marcum, C., Freiburger, T., & Ricketts, M. (2012). Examining the role of peer influence and self-control on downloading behavior. *Deviant Behavior, 33*, 412–423.

Hill, J., & Marion, N. (2016). Presidential rhetoric on cybercrime. *Criminal Justice Studies, 29*, 163–177.

Holt, T., Bossler, A., & May, D. (2012). Low self-control, deviant peer associations, and juvenile cyberdeviance. *American Journal of Criminal Justice, 37*, 378–395.

Howard, J. (2016). Americans devote more than 10 hours a day to screen time, and growing. CNN.com. http://www.cnn.com/2016/06/30/health/americans-screen-time-nielsen/index.html

Holt, T., & Turner, M. (2012). Examining risks and protective factors of online identity theft. *Deviant Behavior, 33*, 308–323.

Internet Crime Complaint Center. (2017). 2016 Annual Internet Crime Report. https://pdf.ic3.gov/2016_IC3Report.pdf.

Inderbitzin, M., Bates, K., & Gainey, R. (2016). *Deviance and social control*. Thousand Oaks, CA: Sage.

Ineme, M., Ineme, L., Akpabio, G., & Osinowo, O. (2017). Predictive roles of depression and demographic factors in Internet addiction. *International Journal of Cyber Criminology, 11*(1), 10–23.

Jarvis, L., Macdonald, S., & Whiting, A. (2017). Unpacking cyberterrorism discourse: Specificity, status and scale in news media constructions of threat. *Journal of International Security*, cambridge.org.

Kethineni, S., Cao, Y., & Dodge, C. (2018). Use of bitcoin in darknet markets. *American Journal of Criminal Justice, 43*, 141–157.

Kigerl, A. (2013). Infringing nations. *International Journal of Cybecriminology, 7*, 62–80.

Leukfeldt, E., & Yar, M. (2016). Applying routine activity theory to cybercrime. *Deviant Behavior, 37*, 263–280.

Li, X. (2015). Regulation of cyber space. *International Journal of Cyber Criminology, 9*, 185–204.

Lollar, C. (2013). Child pornography and the restitution revolution. *Journal of Criminal Law and Criminology, 103*, 343–406.

Lusthaus, J. (2012, May). Trust in the world of cybercrime. *Global Crime, 13*(2), 71–94.

Marcum, C., Higgins, G., Freiburger, T., & Ricketts, M. (2012a). Battle of the sexes: An examination of male and female cyber bullying. *International Journal of Cyber Criminology, 6*, 904–911.

Marcum, C. D., Higgins, G. E., & Tewksbury, R. (2012b). Incarceration or community placement: Examining the sentences of cybercriminals. *Criminal Justice Studies, 25*(1), 33–40.

Marcum, C., Higgins, G., Wolfe, S., & Ricketts, M. (2011). Examining the intersection of self-control, peer association, and neutralization in explaining digital piracy. *Western Criminology Review, 12*, 60–74.

Morris, R., & Higgins, G. (2010). Criminological theory in the digital age. *Journal of Criminal Justice, 38*, 470–480.
Payne, B. K. (2016). *White-collar crime: The essentials* (2nd ed.). Thousand Oaks, CA: Sage.
Podgor, E. (2004). Cybercrime: National, transnational, or nternational? *Wayne Law Review, 50*, 97–108.
Ponemon Institute. (2015). *2015 cost of cyber crime study: Global*. Traverse City, MI: Poneman Institute LLC.
Reijmer, M., & Spruitt, T. (2014). *Cybersecurity in the news A grounded theory approach to better understand its emerging prominence, technical report*. Utrecht, The Netherlands: Utrecht University.
Reyns, B., Fisher, B., Bossler, A., & Holt, T. (2018). Opportunity and self-control: Do they predict multiple forms of online victimization? *American Journal of Criminal Justice*. https://doi.org/10.1007/s12103-018-9447-5.
Seigfried-Spellar, K. (2013). Individual differences of internet child pornography users. *International Journal of Cyber Criminology, 7*(2), 141–154.
Smith, G. S. (2015). Management models for international cybercrime. *Journal of Financial Crime, 22*(1), 104–125.
U.S. Department of Justice (USDOJ). (2010). *Arlington security guard, who hacked into hospital's computer system, pleads guilty to federal charges* [Press release]. Retrieved July 30, 2011, from http://www.justice.gov/usao/txn/PressRel10/mcgraw_ple_pr.html
Wall, D. (2013). Policing identity crimes. *Policing and Society, 23*, 437–460.
Wall, D. (1999). Cybercrimes: New wine, no bottles? In P. Davies, P. Francis, & V. Jupp (Eds.), *Invisible crimes*. London: Palgrave Macmillan. https://doi.org/10.1007/978-1-349-27641-7_5.
Wick, S. E., Nagoshi, C., Basham, R., Jordan, C., Kim, Y. K., Nguyen, A. P., & Lehmanne, P. (2017). Patterns of cyber harassment and perpetration among college students in the United States. *International Journal of Cyber Criminology, 11*, 24–38.
Williams, B., Bengert, A., & Ward-Caldwell, B. (2016). Hacked: A qualitative analysis of media coverage of the Sony Breach. iConference Proceedings. Available online at https://www.ideals.illinois.edu/handle/2142/89417.
Williams, M. (2016). Guardians upon high. *British Journal of Criminology, 56*, 21–48.
Yar, M. (2006). *Cybercrime and society*. Thousand Oaks, CA: Sage.
Yu, S. (2011). Digital piracy and stealing. *International Journal of Criminal Justice Sciences, 6*, 239–250.

Brian Payne is vice provost of academic affairs and a professor of sociology and criminal justice at Old Dominion University. He received his PhD in criminology from Indiana University of Pennsylvania in 1993. He is the author or co-author of eight books and more than 160 scholarly journal articles. His scholarship has been supported by the National Science Foundation and the National Institute for Standards and Technology. He is a past president of the Southern Criminal Justice Association and the Academy of Criminal Justice Sciences.

Brittany Hawkins was born in Boston, Massachusetts and raised in San Francisco bay area where she attended James Logan High School. She graduated from Claflin University in May 2018 with a Bachelor's degree in Criminal Justice. She is currently working on her obtaining her Masters in Criminal Justice.

ChunSheng Xin is a Professor in the Center for Cybersecurity Education and Research and the Department of Electrical and Computer Engineering, Old Dominion University. He received his Ph.D. in Computer Science and Engineering from the State University of New York at Buffalo in 2002. His interests include cybersecurity, privacy, secure computing, wireless communications, and networking. His research is supported by 15 NSF and other federal grants, and results in more than 100 papers in leading journals and conferences, including three Best Paper Awards from IEEE Percom, Globecom, and ICCCN, as well as books, book chapters, and patent. He has served as Co-Editor-in-Chief/Associate Editors of multiple international journals, and symposium/track chairs of multiple international conferences including IEEE Globecom and ICCCN. He is a senior member of IEEE.