6-2020

Disciplinary and Interdisciplinary Trends in Cybercrime Research: An Examination

Brian K. Payne

Lora Hadzhidimova

Copyright © 2020 International Journal of Cyber Criminology – ISSN: 0974–2891
January – June 2020. Vol. 14(1): 81–105. DOI: 10.5281/zenodo.3741131
Publisher & Editor-in-Chief – K. Jaishankar / Open Access (Authors / Readers No Pay Journal).

Disciplinary and Interdisciplinary Trends in Cybercrime Research: An Examination

Brian K. Payne[1] & Lora Hadzhidimova[2]
Old Dominion University, United States of America

Abstract

Compared to other topics, cybercrime is a relatively new addition to the criminological literature. Interest in the topic has grown over the past decade, with a handful of scholars leading efforts to generate empirical understanding about the topic. Common conclusions reached in these studies are that more research is needed, cybercrime is interdisciplinary in nature, and cybercrime should be addressed as an international problem. In this study, we examine a sample of 593 prior cybercrime scholarly articles to identify the types of research strategies used in them, the patterns guiding those strategies, whether the research is interdisciplinary, and the degree to which scholars engage in international cybercrime studies. Attention is also given to co-authorship as well citation patterns. Implications for future research are provided.

Keywords: Cybercrime, Interdisciplinary Research, International Research, Research Collaborations.

Introduction

Reports about cybercrime have increased dramatically over the past decade. Criminologists have played an important role in shaping our understanding about the dynamics, risk factors, and consequences of these crimes. Regarding the dynamics of these crimes, researchers have explored the types of offenses and their patterns. Types of cybercrimes examined by criminologists include, but are not limited to, bullying (Su & Holt, 2010; Hinduja & Patchin, 2010; Marcum et al., 2012; Lembrechts, 2012; Kerstens & Veenstra, 2015;), sex crimes (Broadhurst & Jayawardene, 2007; Young, 2008; Martellozzo, Nehring & Taylor, 2010; Bergen et al., 2013; Açar, 2016), sexting (Jaishankar, 2009; Salter, Crofts & Lee, 2013; Marcum, Higgins & Ricketts, 2014; Martinez-Prather & Vandiver, 2014; Ngo, Jaishankar & Agustina, 2017; O'Conner et al., 2017; Sweeny &

[1] Professor, Department of Sociology & Criminal Justice and Vice Provost for Academic Affairs, Old Dominion University, Norfolk, VA 23529, USA. Email: bpayne@odu.edu (Corresponding Author)

[2] Adjunct Assistant Professor, Department of Political Science and the Center for Cybersecurity Education and Research, Old Dominion University, Norfolk, VA 23529, USA.
E-mail: lhadzhid@odu.edu

Slack, 2017), fraud (Holt & Graves, 2007; Rege, 2009; Dion, 2010; Conradt, 2011; Burgard & Schlembach, 2013; Kopp, 2015; Jegede, Ajayi & Allo, 2016), identity theft (Saunders & Zucker, 1999; Hinde, 2005; Rudner, 2008; Archer, 2011), and hacking (Bachmann, 2010; Holt, Strumsky & Smirnova, 2012; Nycyk, 2016; Madarie, 2017). While many patterns have been cited regarding these crimes, one consistent pattern identified in virtually all studies is the global nature of cybercrime. These offenses can originate anywhere in the world where cyber technology exists, and offenders are able to easily cross international borders without detection.

Criminologists have conducted a number of studies, many in the form of theory tests, to examine risk factors increasing the likelihood of cybercrime. Studies have considered the explanatory power of theories such as self-control theory (Higgins, 2007; Bossler & Holt, 2010; Choi, Lee & Lee, 2017), strain theory (Hay, Meldrum & Mann, 2010; Hinduja, 2012; Jang, Song & Kim, 2014), learning theory (D'Ovidio et al., 2009; Holt, Burruss & Bossler, 2010; Miller & Morris, 2016; Van Ouytsel, Ponnet, & Walrave), neutralization theory (Higgins, Wolfe & Marcum, 2008; Moore & McMullan, 2009; Smallridge & Roberts, 2013), and routine activities theory (Yar, 2005; Bossler & Holt, 2009; Reyns, Henson & Fisher, 2011; Navarro & Jasinski, 2012; Wick et al., 2017). More recently, recognizing the need for an interdisciplinary lens, some researchers have considered how theories such as biological theory (Owen, Noble & Speed, 2017) and action network theory (Luppicini, 2014; Van der Wagen & Pieters, 2015; Balzacq & Cavelty, 2016) relate to cybercrime. In addition, cyber criminologists like Jaishankar (2008) have introduced Space Transition Theory to better explain cyber offending. While support for different theories exists, no apparent general theory of cybercrime explains all of the offenses. Instead, some of them appear to be better suited for certain types of crimes.

Regarding the consequences of cybercrime, researchers have explored individual consequences for victims (Ngo & Paternoster, 2011; Wilsem, 2013; Näsi et al., 2015), legal consequences (Hinde, 2003; Moitra, 2005; Brenner, 2006; Calderoni, 2010), and the criminal justice system's response to cybercrime (Hinduja, 2004; Broadhurst, 2006; Wall, 2007; Hunton, 2011). These studies paint a broad picture of the wide range of consequences arising from cyber offending and cyber victimizations. They also drive home the point that cybercrime is both an international and interdisciplinary issue.

Connecting these themes together, in this project, attention is given to the way that criminologists study cybercrime. A specific focus is given to whether cybercrime is treated as a disciplinary or multidisciplinary problem. In addition, attention is given to the degree to which cybercrime is viewed through an interdisciplinary lens. Authorship patterns, citation patterns of cybercrime articles, research strategies, research topics, and types of samples are also considered. Exploring how cybercrime is studied by criminologists will help to determine directions needed to advance an interdisciplinary and global research agenda in the area of cybercrime.

Literature Review

Criminological research on cybercrime has increased over the past two decades. Initially conceived of as "computer crime," this body of research has evolved along with the types of crimes examined. Describing this increase in research, Jaishankar (2018) has found the concept of cyber criminology. Defined as "the study of causation of crimes that occur in the cyberspace and its impact in the physical space" (Jaishankar, 2007, p.1), cyber criminology has been identified as involving "the examination of criminal behavior and victimization in cyber space from a criminological or behavioral theoretical perspective" (Jaishankar, 2010, 2011b; Ngo & Jaishankar, 2017, p. 4). Further, cyber criminology, according to Jaishankar (2018), "encompasses multidisciplinary fields of inquiry – criminology, sociology, psychology, victimology, information technology and computer/Internet sciences" (p. 2).

Past its infancy, the study of cybercrime is, in some ways, in its teen years. Just as a teenager begins to assert his or her independence, cyber criminologists are beginning to demonstrate how they (and their research) are independent from criminology (and other fields for that matter). Three themes in the literature help to frame the current state of cybercrime research: (1) traditional criminological strategies are used to study cybercrime, but these strategies are used somewhat differently; (2) cybercrime is best understood and studied as an interdisciplinary topic; and (3) cybercrime is best conceptualized as an international problem. These areas are addressed below.

1. Strategies to Study Cybercrime

Traced to criminology, it should not be surprising that cybercrime research methodologies tend to apply the same methods used in criminological research studies. These strategies include surveys/interviews, experiments, analyses of existing data/information, and ethnographies. Just as technology has changed the way that criminals commit certain types of crimes, technology has also changed the way that criminologists study those crimes (Holt, 2015).

Surveys. Surveys are a common tool that researchers have used to study certain types of cybercrime and certain cybercrime topics. Cybercrime researchers have identified a number of problems with using surveys and interviews. These include identification, awareness, context, and developing trust. First, identifying cyber offenders or hackers willing to be surveyed or interviewed can be difficult (Jaishankar, 2018). Afterall, hacking can be illegal, depending on its type. Second, if the focus is on victimization, many cybercrime victims may not even know that they have been victimized (Holt & Bossler, 2014). Third, regarding context, surveys provide a snapshot into the respondents' world, but they reveal very little about how much time and the types of activities respondents engage in when online (Bossler, 2017). Fourth, developing trust is difficult in all forms of surveys and interviews. Given the suspicious nature of hackers and the relative newness of the cybercrime topic, it may be even more difficult in cybercrime studies.

Despite these limitations, interviews and surveys can be helpful if done with the appropriate sample. Recent interviews by Hutchings and Holt (2018) with six cybercrime researchers explored the strategies cybercrime researchers used when interviewing in their studies. Topics they considered included rationale for interviews, recruiting subjects, the need for some technical knowledge, researcher effects, whether the use of interviews varied across cybercrime types, ethical issues, and efforts to publish their results. They conclude that interviews provide contextual information about cybercrime that cannot be found in experiments or surveys of college students.

One researcher studied hacker motivations by surveying computer security experts and asking them about their hacking behaviors and motivations (Madarie, 2017). Another interviewed a troller to provide insight into the motives and experiences of those engaging in that behavior (Bishop, 2013). Other researchers have surveyed students in an effort to identify patterns surrounding various types of cybercrimes such as digital piracy (Hinduja, 2001; Higgins, Wilson & Fell, 2005; Gunter, 2008), cyberbullying (Kraft & Wang, 2009; Lembrechts, 2012; Branch et al., 2017), and hacking (Holt & Kilger, 2008; Marcum et al., 2014).

Experiments. The classic experiment includes the following components: a control group, an experimental group exposed to an independent variable, random assignment, and pre- and post- measures. It is rare that "classic experiments" are conducted in criminological endeavor and even rarer in cybercrime studies. More often, quasi-experiments (e.g., rigorous experiments lacking one of the "classic" components) are conducted. Consider a quasi-experimental study exploring adults' sexual interest in children. The authors described the following steps of their study:

> 1. The researcher chose a nickname from the list of typical names (20 per chat room) depending on country and gender of the impersonated person, and added the word "young". 2. Logged in to the chat room. 3. Wrote an open invitation in the general chat, seeking company (1 – 5 times) until the first contact responded, and invited the impersonated person to chat privately. 4. Asked what the contact was looking for in the chat room. 5. Asked where the contact lived, and claimed to be from the same city or nearby. 6. Asked the age of the contact, or made a remark on the age if the contacts age was provided in his nickname. 7. Revealed the portrayed age (i.e. 10, 12, 14, 16 or 18-years old). 8. Registered the contacts behavior after he had received knowledge of the portrayed age. 9. Gave an excuse for having to leave the chat room, e.g. "dinner time", or "mum came home". 10. Registered the contact's reply (Bergen et al., 2013, p.100).

Such an empirical design can provide useful data for scholars, but it can be time consuming. Regarding cyber criminologists and quasi-experiments, honeypots are perhaps more common research strategies. Honeypots are "computers that are created for the sole purpose of being hacked" (Bossler, 2017, p. 43). Researchers have explored questions such as when hacks occur most often (Kelly & Gan, 2011) and the degree to which warnings in cyber systems deter or otherwise impact hacker behavior (Maimon et al. 2014; Testa et al., 2017). Among this latter type of study, research shows that messages based on moral persuasion have been found to have "a greater impact on reducing both the incidence and the frequency of system trespasser behavior than the other warning message types" (Jones, Maimon & Ren, 2017, p. 162).

Experts have identified concerns about honeypots. For example, they note that honeypot studies provide little insight into the motives of offenders or offender dynamics in general (Holt, 2017b). As well, with the growth in automated attacks, researchers might by studying the "behavior" or scripts rather than the attacker (Bossler, 2017). It has also been noted that honeypots in university settings provide insight into offender behavior in university networks. The opportunity structures may vary across organizations (Bossler, 2017). What this means is that different patterns might be found in businesses, government agencies, or other settings. Bossler (2017) suggests that cyber criminologists have an "open discussion" about the limitations of honeypot data (p. 687)

Analyses of existing data. The analysis of existing data is a common tool used in criminology studies. Experts have noted that the Internet has "introduced new potential sources of data for study" (Tewksbury, 2015, p. 206). These new sources of data include web-forums, emails, chatroom conversations, and virtually everything that individuals communicate in the digital world (Holt, 2015). Authors have used existing data to study patterns surrounding organizational data breaches (Collins et al., 2011), malware distribution (Holt, 2012), and advanced fee fraud (Holt & Graves, 2007). The advantages of such studies are numerous: (1) researchers can explore trends over time, (2) researchers can access a large number of cases that otherwise would be inaccessible, and (3) researchers do not influence the response of the subjects being studies. For example, a study on organizational data breaches provided insights into historical trends (Collins et al., 2011). Also, because it would be difficult to interview malware distributors, Holt (2012) examined threads from ten Russian web forums designed to promote malware distribution. He found that trust, price, and customer service were those features that facilitated the sale of malware between sellers and buyers. In another study, Holt and Graves (2007) examined 412 advanced fee fraud emails. They found that scammers used varied writing styles and often asked for information that would allow them to commit identity theft. They were able to identify these patterns without contacting offenders (who undoubtedly would have reacted to the presence of a researcher).

Studies using existing data are potentially limited in that they may not provide a full perspective into certain types of crimes. Consider a study on organizational breaches that uses existing data. Such a study would only include those cases where organizations reported experiencing a breach. Some organizations have a legal duty to disclose, while others would do so voluntarily. Studies relying on public disclosures of breaches, then, would overrepresent those agencies (such as health care agencies) that have a legal duty to report breaches.

In addition, depending on the type of data used, researchers may not be sure that the data is accurate. When using a web forum, for example, researchers must consider the fact that comments they are analyzing might have been made by trolls or law enforcement officers (Holt, Smirnova, & Hutchings, 2016, p. 141). Ethical issues might also arise in studies using existing information, particularly when researchers access information that was not meant to be accessed. Holt and Dupont (2018) analyzed web-threads from a hacked forum to shed light on factors that predicted forum owners' decisions to accepted forum users into the community, which existed to sell stolen credit cards, viruses, malware, and other types of illegally obtained items. The authors note that using hacked data sources presents a "unique ethical challenge to researchers depending on the content of what is made available by the poster" (p. 7). In their study, none of the data included identifiable information and they treated their data similar to the way they would treat other types of online data.

Ethnographies. Ethnographies are qualitative studies where social scientists immerse themselves into the world of the research subject, either through in-depth interactions and interviews with the research subject or full immersion into their world. Cyber ethnography has been hailed as "a viable and important method for exploring cyber-interaction" (Downing, 2010, p. 290). One author team used an "auto-ethnographic" approach to describe "their personal experiences of online violence and hate, in response to speaking out against Islamophobia and gender inequality" (Barlow & Awan, 2016, p. 4). More common in cybercrime studies, though, are efforts in which researchers try to gain understanding about the cyber subculture.

Similar to traditional field studies, researchers will need to determine whether they will announce their presence to research subjects (Holt, 2017a). Such a decision is informed by methodological, legal, and safety domains. Regarding methodological domains, in some situations disclosing the researcher's identity may serve to limit the findings, particularly if the researcher's presence will alter the behavior of research subjects. In terms of legal domains, researchers will need to solicit approval from their institutional review boards prior to beginning their research. IRB members may pay close attention to studies in which researchers conceal their identity. Regarding practical domains, it may be necessary for researchers to conceal their identity simply to protect themselves (Holt, 2017a). Other times, it may be unwise to conceal one's identity among certain types of cyber research subjects. As Steinmetz (2015) points out, "hackers are often intelligent with access to resources. Deceit may unravel quickly" (p. 128).

2. Cybercrime as an Interdisciplinary Issue

Researchers are increasingly recognizing that cybercrime is an interdisciplinary topic drawing on a range of disciplines such as computer engineering, computer science, information technology, criminology, criminal justice, sociology, philosophy, law, psychology, and others.

Given the nature of cybercrime as a technological problem, a crime problem, a social issue, a business concern, and a hotbed for ethical issues, it makes sense that cybercrime should be addressed as an interdisciplinary topic. In addition, the dynamics of the offenses and the types of experts needed to address the offenses demonstrate the need to approach cybercrime through an interdisciplinary lens. An interdisciplinary approach will provide insight into human behavior, thereby allowing researchers to identify proactive strategies to curb cybercrime (Benjamin, Samtani & Chen, 2017).

Addressing the topic through an interdisciplinary lens is easier said than done. Bossler (2017) points out that "social scientists do not have the expertise to set up these technologies and need assistance of computer scientists" (p. 51). He adds, "Computer scientists focus little on the human element of cybercrime" (p. 52). Others have suggested that limited exposure to technology has hindered traditional criminologists' efforts to research cybercrime. The lack of a "common language" also creates barriers, but also opportunities, for interdisciplinary research (Holt, 2017, p. 3). This is expected to change in the future. As Jaishankar (2018) writes, "The digital native cyber criminologists will understand the technology better than the digital immigrant criminologists and they will have a multidisciplinary approach and will take the discipline of cyber criminology to greater heights" (p. 6). Along this line, Bossler (2017) concludes that one of four questions the cybercrime field should be asking is "how can criminologists and other social scientist collaborate more effectively with computer scientists and information technology specialists"?

The need to address cybercrime from an interdisciplinary perspective appears to be accepted among scholars. Criminologist Tom Holt recently created the International Interdisciplinary Research Consortium on Cybercrime, which is hailed as "the premier organization that links the fields of social and technical science together with practitioners and law enforcement to research and understand cybercrime and cybersecurity and promote a safer Internet" (The International Interdisciplinary Research Consortium on Cybercrime, no date). On one level, the consortium embraces and promotes the need to empirically address cybercrime through an interdisciplinary framework that brings together scholars from a wide range of academic disciplines. On another level, the consortium draws attention to the international nature of cybercrime.

3. Studying cybercrime as an international problem

Just as scholars agree that cybercrime is an interdisciplinary topic, they also agree that cybercrime is an international problem. As one author notes, "Cyberspace has defied the boundaries and has made geography (or place) irrelevant." (Jaishankar, 2010, p. 26). A study by Norton (Symantec) reveals that 65% of Internet users around the world have experienced cybercrime victimization, as the most victimized countries were China (83%), followed by Brazil and India with 76% and the U.S. with 73% (LaBrie, Collier & Palmer, 2010). In many ways, offenders are able to cross international borders while committing their offense.

The international nature of cybercrime creates myriad issues including legal obstacles, law enforcement barriers, jurisdictional concerns, and potential methodological problems. Scholars have called for international research to address these issues. In the words of one author team, "Given that cybercrime is a global phenomenon and the tools of cyber criminals are technology and anonymity, research examining the effectiveness of collaborative efforts …between cross-national law enforcement agencies are warranted." (Ngo & Jaishankar, 2017, p. 6). Whereas technology has allowed offenders to cross international borders, the same technology also allows scholars studying cybercrime to do the same. The question that arises is whether cyber criminologists have, in fact, crossed international borders in their research in the same way that offenders have. In other words, have criminologists engaged in cross-cultural studies of cybercrime?

The Current Study

Summing up the state of cybercrime research, three trends can be identified. First, criminologists use traditional forms of research, as Holt (2015) notes, "Criminologists…adapt existing data collection and analysis strategies to explore a range of offenses." Second, the interdisciplinary nature of cybercrime provides the opportunity for interdisciplinary research efforts. Third, the international nature of the behavior warrants the need for internationally focused studies on cybercrime. While these basic points about cybercrime research are nearly universally agreed upon, the degree to which different types of cybercrime studies are conducted, whether they are interdisciplinary in nature, and whether there is an international focus, is not clear. To provide insight into the state of cybercrime research, in this study, the following questions are addressed:

- What types of research methods are most frequently used in cybercrime studies?
- What types of samples are used in cybercrime studies?
- To what degree are the cybercrime studies interdisciplinary in nature?
- To what degree do the cybercrime studies involve international partnerships?
- Does the type of study, type of sample, or topic of study influence citations?

Addressing these questions will help to understand whether criminologists are addressing cybercrime in ways consistent with the behavior (e.g., as an interdisciplinary and international issue) or whether they are treating it simply as another form of crime to be studied in traditional ways.

Methods

The data for the present study includes 593 research articles gathered from three different groupings. First, articles published in the International Journal of Cyber criminology, the premier journal on the topic, from its creation through 2017 were included in the sample. Second, cybercrime articles authored by the International Journal of Cyber Criminology's (IJCC) editorial board members were included in the sample. Third, cybercrime articles published by members of the International Interdisciplinary Research Consortium on Cybercrime (IIRCC) were also included in the sample. Most of the information needed for analyzing the research articles was collected through Google Scholar, the journals in which the articles were published, and the professional information for the authors that appears on their institutions' websites. A coding schedule was developed to help in gathering relevant information about each article. This information is discussed below.

Analytic Plan and Measures

We gathered data about the scholarly articles' years of publication, the name of the leading author, the name of the journal, whether the article was a product of an individual work or of a research team, and if so, whether the team consisted of interdisciplinary authors, and whether this was a collaboration between members of the social and the hard sciences. Further, we collected information about gender dynamics for co-authored articles. We also categorized research teams into international ones and non-international ones. An international team, we identified, as a collaboration between scientists of whom at least one was part of a non-U.S. institution. Conversely, a non-international team represents a collaboration between members of a U.S. academic or non-academic institution(s), regardless of citizenship.

Next, we divided the articles' topics into various categories: malware, hacking, theory building and theory testing, cyberbullying, pornography and sex crimes, cyberwar, criminal justice professionals and criminal justice response to cybercrime, subcultures, piracy, law, fraud, victimization and computer safety. Then, the methods of the research articles were identified and labeled as surveys/interviews, experiments, analyses of existing records, legal research, literature reviews, focus groups or field research. In case the study was a survey/interview, we also collected information about the sample and grouped it into five types – sample of school students, of college students, of the public, of offenders, and of professionals. In addition to these data, we also looked for the numbers of citations of the selected scholarly articles and whether they were written by member(s) in the IJCC editorial board, member(s) of IIRCC, members of both entities, or by member(s) of neither of them.

The collected information was analyzed and results were presented through descriptive measures and correlations between the number of authors, the interdisciplinary and non-interdisciplinary collaborations, the collaborations solely from representatives of the social or the hard sciences, and the ones including both, the mixed-gender teams, and the ones that were international or non-international. We also conducted cross-tabulations that revealed other tendencies related to variations of the articles' characteristics - the presence or the absence of an interdisciplinary or international team, by the number of authors and the number of citations, by discipline, and by year. Where appropriate, t-tests were conducted to identify differences in mean citations and mean number of authors.

Findings

Table 1. Sample Characteristics

Variable	n	%
First author discipline		
Criminology	311	52.4
Computer Science	106	17.9
Law	57	9.6
Sociology	36	6.1
Psychology	26	4.4
Political Science	22	3.7
Business	13	2.2
Communications	13	2.2
Education	7	1.2
Engineering	2	0.3
Co-authored Manuscript	386	65.1
Topic		
CJ Response	112	18.9
Theory Building and Theory Tests	64	10.8
Computer Safety	63	10.6
Subculture	63	10.6
Cyber Bullying	55	9.3
Victimization	54	9.1
Piracy	33	5.6
Fraud	27	4.6
Pornography	26	4.4
Cyber War	23	3.9
Hacking	23	3.9
Malware	4	0.7
Year		
1990s	13	2.2
2000-2009	153	25.8
2010-March 2018	427	72
Mixed Gender Team	188	31.7
Interdisciplinary Authors	91	15.3
Social/Hard Sciences Team	25	4.2
International Team	69	11.6
Method		
Analysis of existing record/websites	222	37.4
Survey	184	31
Literature Review	96	16.2
Legal Research	52	8.8
Experiment	34	5.7
Focus Group	3	0.5
Field Research	2	0.3
Sample (surveys)		
College Students	72	12.1
Public	42	7.1
School students	37	19.9
Professionals	22	3.7
Offenders	13	2.2

Table 2. Interdisciplinary by Article Characteristics

Variable	Interdisciplinary Authors	Not Interdisciplinary
First author discipline		
Criminology	32 (35.2)	169 (57.3)
Sociology	15 (16.5)	5 (1.7)
Political Science	5 (5.5)	6 (2.0)
Law	5 (5.5)	13 (4.4)
Computer Science	15 (16.5)	79 (26.8)
Business	3 (3.3)	7 (2.4)
Engineering	1 (1.1)	1 (0.3)
Education	4 (4.4)	2 (0.7)
Psychology	8 (8.8)	11 (3.7)
Communications	3 (3.3)	2 (0.7)
Topic		
CJ Response	15 (16.5)	52 (17.8)
Computer Safety	10 (11)	50 (16.9)
Theory Tests	7 (7.7)	40 (13.6)
Subculture	8 (8.8)	27 (9.2)
Cyber Bullying	13 (14.3)	26 (8.8)
Victimization	6 (6.6)	27 (9.2)
Piracy	2 (2.2)	14 (4.7)
Fraud	11 (12.1)	9 (3.1)
Pornography	3 (3.3)	17 (5.8)
Cyber War	5 (5.5)	10 (3.4)
Hacking	4 (4.4)	11 (3.7)
Malware	1 (1.1)	2 (0.7)
Year		
1990s	1 (1.1)	3 (0.9)
2000-2009	10 (11.0)	48 (16.3)
2010-March 2018	80 (87.9)	244 (82.7)
Method		
Survey	24 (26.4)	116 (39.3)
Experiment	6 (6.6)	26 (8.8)
Analysis of existing record/websites	35 (38.5)	107 (36.3)
Legal Research	7 (7.7)	13 (4.4)
Literature Review	17 (18.7)	31 (10.5)
Focus Group	1 (1.1)	2 (0.7)
Field Research	1 (1.1)	0
Sample (surveys)		
School students	9 (36)	25 (21.4)
College Students	7 (28)	47 (40.2)
Public	9 (36)	24 (20.5)
Offenders	0	6 (5.1)
Professionals	0	15 (12.8)

Note: percentages refer to percent within interdisciplinary authors

Table 3. International Team by Article Characteristics

Variable	International Team	Not International Team
First author discipline		
Criminology	25 (36.2)	176 (55.7)
Sociology	1 (1.4)	18 (5.7)
Political Science	3 (4.3)	8 (2.5)
Law	2 (2.9)	16 (5.1)
Computer Science	30 (43.5)	64 (20.3)
Business	1 (1.4)	9 (2.8)
Engineering	0	2 (0.6)
Education	1 (1.4)	5 (1.6)
Psychology	5 (7.2)	14 (4.4)
Communications	1 (1.4)	4 (1.3)
Topic		
CJ Response	19 (27.5)	48 (15.2)
Theory Tests	2 (2.9)	45 (14.2)
Computer Safety	21 (30.4)	39 (12.3)
Subculture	7 (10.1)	28 (8.9)
Cyber Bullying	2 (2.9)	37 (11.7)
Victimization	4 (5.8)	29 (9.2)
Piracy	1 (1.4)	15 (4.7)
Fraud	2 (2.9)	18 (5.7)
Pornography	4 (5.8)	16 (5.1)
Cyber War	2 (2.9)	12 (3.8)
Hacking	3 (4.3)	12 (3.8)
Malware	3 (0.9)	0
Year		
1990s	0	4 (1.3)
2000-2009	5 (7.3)	75 (23.7)
2010-March 2018	64 (92.8)	237 (75.0)
Method		
Survey	14 (20.3)	126 (39.9)
Experiment	8 (11.6)	8 (11.6)
Analysis of existing record/websites	33 (47.8)	109 (34.5)
Legal Research	2 (2.9)	18 (5.7)
Literature Review	11 (15.9)	37 (11.7)
Focus Group	1 (1.4)	2 (0.6)
Field Research	0	1 (0.3)
Sample (surveys)		
School students	2 (13.3)	31 (24.6)
College Students	2 (13.3)	52 (41.3)
Public	6 (40.0)	27 (21.4)
Offenders	1 (6.7)	5 (4.0)
Professionals	4 (26.7)	11 (8.7)

Note: percentages refer to percent within international team authors

Table 1 shows an overview of the articles reviewed in this study. The first authors of just over half of the articles were criminologists and roughly 18% were computer scientists. The rest came from law, sociology, psychology, business, communications, education, and engineering. Roughly two-thirds of the articles were co-authored. Topics addressed most often included the criminal justice response, theory, computer safety, subculture, cyberbullying, and victimization. Nearly three-fourths of the articles were published since 2010. Just under one-third of the articles were authored by mixed gender teams (e.g., the articles included males and females). Roughly 15% of the articles were published by interdisciplinary teams, about 10% were international research teams, and just 4% were social science/hard science research teams. The most common research strategies were analyses of existing records/websites and surveys. Among the surveys, the most common samples used were college student samples. Surveys of professionals or offenders were much rarer. Also, only two of the articles had engineers as the lead author of the manuscript.

Table 2 shows a comparison between interdisciplinary and non-interdisciplinary articles. Criminologists and sociologists were more likely to serve as first authors of interdisciplinary articles. Cyberbullying articles and fraud articles were more likely to have interdisciplinary authors. Literature reviews were more likely to include interdisciplinary efforts than other empirical approaches. Also, in terms of raw numbers, there were more interdisciplinary efforts in the past decade, but the total percentage of interdisciplinary efforts over that time frame was not significantly different from the percentage between 2000 and 2009. So, while the likelihood of interdisciplinary pursuits in cybercrime research did not increase, the volume of interdisciplinary efforts did increase.

Table 4. Correlations between research collaboration types

Correlations						
		Number of Authors	Interdisciplinary Authors	Social/Hard Sciences Team	Mixed Gender Team	International Team
Number of Authors	Pearson Cor.	1	.087	.209*	.174**	.224**
	N	593	386	92	386	385
Interdisciplinary Authors	Pearson Cor.	.087	1	.064	.056	.061
	N	386	386	92	385	384
Social/Hard Sciences Team	Pearson Cor.	.209*	.064	1	-.211*	.044
	N	92	92	92	92	91
Mixed Gender Team	Pearson Cor.	.174**	.056	-.211*	1	.047
	N	386	385	92	386	385
International Team	Pearson Cor.	.224**	.061	.044	.047	1
	N	385	384	91	385	385

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

Table 3 shows a comparison between international co-authored manuscripts and non-international manuscripts. Computer scientists were more likely to engage in international research teams than others. In fact, 43% of the international articles had computer scientists as first authors and nearly one-third of the articles with computer science first author articles were international collaborations. As a comparison, just 12.5% (25 of 201) of the articles with criminologists as first authors involved international collaborations. In addition, international articles were more likely to focus on computer safety and be published in the past decade, and less likely to survey college students. These latter patterns are consistent with the types of research topics and strategies used by computer scientists and criminologists.

Table 5a. Discipline by Article Characteristics

	Criminology	Sociology	Political Science	Law	Computer Science
Topic					
Malware	1 (0.3)	0	0	0	3 (2.8)
Hacking	12 (3.9)	1 (2.8)	2 (9.1)	0	5 (4.7)
Theory Tests	57 (18.3)	0	2 (9.1)	0	1 (0.9)
Bullying	32 (10.3)	5 (13.9)	1 (4.5)	6 (10.5)	0
Pornography	15 (4.8)	2 (5.6)	0	0	3 (2.8)
Cyber War	5 (1.6)	1 (2.8)	7 (31.8)	4 (7)	6 (5.7)
CJ Response	66 (21.2)	4 (11.1)	5 (22.7)	5 (8.8)	21 (19.8)
Subculture	38 (12.2)	10 (27.8)	2 (9.1)	0	4 (3.8)
Piracy	23 (7.4)	2 (5.6)	0	0	2 (1.9)
Law	7 (2.3)	0	2 (9.1)	36 (63.2)	0
Fraud	11 (3.5)	9 (25)	1 (4.5)	1 (1.8)	2 (1.9)
Victimization	42 (13.5)	2 (5.6)	0	3 (5.3)	3 (2.8)
Comp. Safety	2 (0.6)	0	0	2 (3.5)	56 (52.8)
Method					
Survey	137 (44.1)	15 (41.7)	1 (4.5)	3 (5.3)	10 (9.4)
Experiment	5 (1.6)	1 (2.8)	0	0	24 (22.6)
Ex. Records	116 (37.3)	11 (30.6)	12 (54.5)	9 (15.8)	54 (50.9)
Legal Research	9 (2.9)	1 (2.8)	2 (9.1)	38 (66.7)	0
Lit Review	41 (13.2)	8 (22.2)	7 (31.8)	5 (8.8)	18 (17)
Focus group	2 (0.6)	0	0	1 (1.8)	0
Field research	1 (0.3)	0	0	1 (1.8)	0
Sample (for surveys)					
School students	28 (20.4)	6 (37.5)	0	0	0
College students	66 (48.2)	2 (12.5)	0	1 (33.3)	1 (10)
Public	18 (13.1)	5 (31.3)	0	1 (33.3)	5 (50)
Offenders	9 (6.6)	3 (18.8)	0	1 (33.3)	0
Professionals	16 (11.7)	0	1 (100)	0	4 (40)

Table 4 shows correlations between number of authors, interdisciplinary authors, social/hard sciences teams, mixed-gender teams, and international teams. Not surprisingly, the number of authors was positively related to the cybercrime article involving a social/hard sciences team, a mixed gender team, and an international team. Interestingly, number of authors was not related to the presence of an interdisciplinary team, though one would have expected that higher number authors would automatically increase the likelihood of an interdisciplinary pursuit. In addition, we found that social/hard science teams were less likely to include author teams including both male and female authors.

Table 5b. Discipline by Article Characteristics

	Business	Engineering	Education	Psychology	Communications
Topic					
Malware	0	0	0	0	0
Hacking	1 (7.7)	0	0	1 (3.8)	1 (7.7)
Theory Tests	1 (7.7)	0	0	3 (11.5)	0
Bullying	2 (15.4)	0	3 (42.9)	5 (19.2)	1 (7.7)
Pornography	0	0	0	6 (23.1)	0
Cyber War	0	0	0	0	0
CJ Response	3 (23.1)	0	2 (28.6)	1 (3.8)	5 (38.5)
Subculture	3 (23.1)	0	1 (14.3)	1 (3.8)	4 (30.8)
Piracy	0	0	0	6 (23.1)	0
Law	0	0	0	0	1 (7.7)
Fraud	2 (15.4)	0	0	1 (3.8)	0
Victimization	1 (7.7)	0	1 (14.3)	1 (3.8)	1 (7.7)
Comp. Safety	0	2 (100)	0	1 (3.8)	0
Method					
Survey	3 (23.1)	0	0	15 (57.7)	0
Experiment	0	0	0	3 (11.5)	1 (7.7)
Ex. Records	7 (53.8)	1 (50)	2 (28.6)	3 (11.5)	7 (53.8)
Legal Research	0	0	1 (14.3)	0	1 (7.7)
Lit Review	3 (23.1)	1 (50)	4 (57.1)	5 (19.2)	4 (30.8)
Focus group	0	0	0	0	0
Field research	0	0	0	0	0
Sample (for surveys)					
School students	0	0	0	3 (18.8)	0
College students	1 (33.3)	0	0	1 (6.3)	0
Public	1 (33.3)	0	0	12 (75)	0
Offenders	0	0	0	0	0
Professionals	1 (33.3)	0	0	0	0

Tables 5a and 5b shows the relationships between disciplinary backgrounds and topic, research strategy, and type of sample. Topics were clearly connected to disciplinary backgrounds: criminologists were more likely to study the criminal justice response,

- sociologists were more likely to study subcultures,
- political scientists were more likely to study cyber war,
- law scholars wrote legal articles, and computer scientists focused on computer safety.

Table 6. Mean Differences for Number of Authors and Citations

Variable	Mean # Authors (s.d.)	Mean Cites (s.d.)
First author discipline	F=15.01★★★	F=.623
Criminology	2.09 (1.04)	47.15 (138.21)
Sociology	1.94 (1.94)	16.94 (23.66)
Political Science	1.50 (0.51)	26.73 (29.71)
Law	1.40 (0.68)	57.60 (252.72)
Computer Science	3.10 (1.41)	47.49 (120.87)
Business	2.31 (0.95)	8.38 (14.39)
Engineering	2.50 (0.71)	9.50 (12.02)
Education	2.00 (0.58)	23.86 (44.55)
Psychology	3.27 (2.18)	10.31 (11.47)
Communications	1.62 (0.87)	16.31 (41.15)
Topic	F=9.36★★★	F-2.12★
CJ Response	2.01 (0.99)	18.62 (29.97)
Theory Tests	2.25 (1.14)	55.53 (67.31)
Computer Safety	3.37 (1.41)	56.25 (149.47)
Subculture	1.97 (1.06)	23.24 (32.82)
Cyber Bullying	2.16 (1.05)	109.42 (299.08)
Victimization	2.06 (1.09)	24.96 (80.34)
Piracy	1.79 (0.99)	40.73 (48.08)
Fraud	2.37 (1.21)	11.37 (18.03)
Pornography	2.96 (2.01)	16.15 (26.64)
Cyber War	1.83 (0.78)	26.52 (32.58)
Hacking	2.57 (1.53)	35.52 (52.14)
Malware	3.25 (1.71)	17.75 (28.86)
Interdisciplinary Authors	t=-1.72★ (df=384)	t=3.60★★★ (df=326.38)
Yes	3.04	17.84 (25.74)
No	2.82	58.72 (185.60)
International Team	t=-3.61★★ (df=83.21)	t=3.17★★ (df-380.70)
Yes	3.39 (1.39)	20.06 (35.67)
No	2.76 (.972)	55.55 (183.31)
Method	F=13.31★★★	F=1.33
Survey	2.41 (1.29)	60.18 (174.82)
Experiment	3.53 (1.31)	21.74 (31.95)
Analysis of existing record/websites	2.23 (1.24)	28.86 (83.72)
Legal Research	1.52 (0.75)	64.83 (264.68)
Literature Review	1.77 (0.93)	34.56 (57.50)
Focus Group	2.33 (0.58)	14.67 (23.67)
Field Research	1.50 (0.71)	1.50 (0.71)
Sample (surveys)	F=2.81★	F=2.03★
School students	2.84 (1.04)	128.19 (284.37)
College Students	2.21 (1.10)	49.24 (49.41)
Public	2.71 (1.83)	49.81 (234.42)
Offenders	1.77 (0.93)	31.31 (25.34)
Professionals	2.41 (1.18)	14.68 (22.60)

★p<.05, ★★★p<.001 (one-tailed)

Table 7a. Annual Trends (2008-2012)

Year					
	2008	2009	2010	2011	2012
Discipline+					
Criminology	20 (66.7)	19 (65.5)	19 (48.7)	19 (67.9)	27 (64.3)
Sociology	2 (6.7)	1 (3.4)	1 (2.6)	2 (7.1)	3 (7.1)
Political Science	0	0	1 (2.6)	0	1 (2.4)
Law	1 (3.3)	2 (6.9)	7 (17.9)	1 (3.6)	4 (9.5)
Computer Science	5 (16.7)	4 (13.8)	6 (15.4)	5 (17.9)	4 (9.5)
Business	0	2 (6.9)	3 (7.7)	1 (3.6)	2 (4.8)
Engineering	0	0	0	0	0
Education	0	0	2 (5.1)	0	1 (2.4)
Psychology	2 (6.7)	1 (3.4)	0	0	0
Communications	0	0	0	0	0
Method					
Survey	16 (53.3)	12 (41.4)	12 (30.8)	9 (32.1)	17 (40.5)
Experiment	2 (6.7)	3 (10.3)	1 (2.6)	1 (3.6)	0
Existing Records/web	4 (13.3)	9 (31.0)	19 (48.7)	11 (39.3)	15 (35.7)
Legal Research	1 (3.3)	3 (10.3)	4 (10.3)	2 (7.1)	4 (9.5)
Literature Review	6 (20.0)	2 (6.9)	2 (5.1)	4 (14.3)	6 (14.3)
Sample++					
School Students	1 (6.3)	0	3 (25)	1 (11.1)	3 (17.6)
College Students	11 (68.8)	11 (91.7)	5 (41.7)	5 (55.6)	7 (41.2)
Public	3 (18.8)	1 (8.3)	0	0	2 (11.8)
Offenders	1 (6.3)	0	3 (25)	0	1 (5.9)
Professionals	0	0	1 (8.3)	3 (33.3)	4 (23.5)
Additional Variables					
Interdisciplinary Team	2 (11.8)	4 (18.2)	3 (13.0)	2 (11.1)	5 (18.5)
International Team	1 (5.9)	2 (9.1)	0	0	2 (7.7)
Topic					
Malware	0	0	0	0	0
Hacking	0	2 (6.9)	0	1 (3.6)	2 (4.8)
Theory Tests	8 (26.7)	4 (13.8)	5 (12.8)	4 (14.3)	8 (19.0)
Cyber Bullying	3 (10.0)	1 (3.4)	4 (10.3)	3 (10.7)	4 (9.5)
Pornography	2 (6.7)	2 (6.9)	3 (7.7)	1 (3.6)	0
Cyber War	0	1 (3.4)	2 (5.1)	1 (3.6)	1 (2.4)
CJ Response	4 (13.3)	3 (10.3)	3 (7.7)	4 (14.3)	9 (21.4)
Subculture	5 (16.7)	2 (6.9)	6 (15.4)	4 (14.3)	4 (9.5)
Piracy	3 (10.0)	4 (13.8)	2 (5.1)	3 (10.7)	3 (7.1)
Law	0	3 (10.3)	4 (10.3)	1 (3.6)	3 (7.1)
Fraud	0	2 (6.9)	1 (2.6)	1 (3.6)	2 (4.8)
Victimization	2 (6.7)	2 (6.9)	4 (10.3)	3 (10.7)	3 (7.1)
Computer Safety	3 (10.0)	3 (10.3)	5 (12.8)	2 (7.1)	3 (7.1)

+Refers to discipline of first authors

++Sample is only included for surveys.

Table 7b. Annual Trends (2013-2017)

Year					
	2013	2014	2015	2016	2017
Discipline					
Criminology	24 (48.0)	31 (47.0)	18 (43.9)	36 (42.4)	41 (59.4)
Sociology	4 (8.0)	4 (6.1)	3 (7.3)	7 (8.2)	3 (4.3)
Political Science	4 (8.0)	3 (4.5)	3 (7.3)	0	3 (4.3)
Law	3 (6.0)	4 (6.1)	4 (9.8)	7 (8.2)	3 (4.3)
Computer Science	5 (10.0)	13 (19.7)	8 (19.5)	26 (30.6)	10 (14.5)
Business	3 (6.0)	0	1 (2.4)	1 (1.2)	0
Engineering	0	0	0	0	1 (1.4)
Education	0	1 (1.5)	0	0	1 (1.4)
Psychology	5 (10.0)	6 (9.1)	4 (9.8)	3 (3.5)	5 (7.2)
Communications	2 (4.0)	4 (6.1)	0	5 (5.9)	2 (2.9)
Method					
Survey	18 (36.0)	26 (39.4)	14 (34.1)	20 (23.5)	19 (27.5)
Experiment	2 (4.0)	5 (7.6)	6 (14.6)	6 (7.1)	5 (7.2)
Existing Records/web	20 (40.0)	22 (33.3)	13 (31.7)	40 (47.1)	34 (49.3)
Legal Research	3 (6.0)	2 (3.0)	3 (7.3)	5 (5.9)	2 (2.9)
Literature Review	6 (12.0)	11 (16.7)	5 (12.2)	13 (15.3)	9 (13.0)
Sample (for surveys)					
School Students	3 (16.7)	8 (30.8)	6 (37.5)	7 (35.0)	3 (15.8)
College Students	5 (27.8)	6 (23.1)	2 (12.5)	2 (10.0)	5 (26.3)
Public	5 (27.8)	9 (34.6)	4 (25.0)	8 (40.0)	7 (36.8)
Offenders	2 (11.1)	2 (7.7)	1 (6.3)	0	1 (5.3)
Professionals	3 (16.7)	1 (3.8)	3 (18.8)	3 (15.0)	3 (15.8)
Additional Variables					
Interdisciplinary Team	11 (33.3)	10 (22.7)	8 (28.6)	18 (25.7)	17 (31.5)
International Team	6 (17.6)	7 (15.9)	7 (15.9)	21 (30.0)	19 (35.2)
Topic					
Malware	1 (2.0)	0	1 (2.4)	1 (1.2)	1 (1.4)
Hacking	2 (4.0)	1 (1.5)	0	4 (4.7)	5 (7.2)
Theory Tests	5 (10.0)	5 (7.6)	1 (2.4)	10 (11.8)	5 (7.2)
Cyber Bullying	5 (10.0)	10 (15.2)	5 (12.2)	7 (8.2)	8 (11.6)
Pornography	3 (6.0)	7 (10.6)	3 (7.3)	3 (3.5)	1 (1.4)
Cyber War	3 (6.0)	1 (1.5)	2 (4.9)	2 (2.4)	2 (2.9)
CJ Response	10 (20.0)	9 (13.6)	11 (26.8)	15 (17.6)	17 (24.6)
Subculture	6 (12.0)	9 (13.6)	3 (7.3)	9 (10.6)	11 (15.9)
Piracy	3 (6.0)	3 (4.5)	0	1 (1.2)	2 (2.9)
Law	2 (4.0)	2 (3.0)	3 (7.3)	4 (4.7)	2 (2.9)
Fraud	2 (4.0)	3 (4.5)	5 (12.2)	6 (7.1)	2 (2.9)
Victimization	5 (10.0)	7 (10.6)	3 (7.3)	8 (9.4)	7 (10.1)
Computer Safety	5 (6.0)	9 (13.6)	4 (9.8)	15 (17.6)	6 (8.7)

+Refers to discipline of first authors
++Sample is only included for surveys.

In terms of research strategies, legal scholars were more prone to write legal research articles and computer scientists more often used existing records. In addition, among all the disciplines, student samples appeared to be a preferred method for criminologists, sociologists, and psychologists. Among psychologists, student samples seemed to be preferred sample over the other types of samples.

Table 6 shows the mean differences between first author discipline, topic, interdisciplinary authors, international teams, methods, sample types, and mean number of authors and mean number of citations. Regarding disciplinary backgrounds of first authors, law-authored articles had fewer authors and computer science-authored articles had more authors. Cybercrime articles receiving the most citations were those focusing on bullying, computer safety, and theory, and those that involved surveys, legal research, and surveys of college students. Those that involved interdisciplinary teams and international collaborations were cited less often than those that were non-interdisciplinary and non-international.

Tables 7a and 7b show trends in cybercrime research based on all the variables we included. A few trends are noteworthy. First, in 2016, there was an increase in the number of first-authored articles by computer scientists. Besides that, though, the disciplinary representations appear to be comparable between 2017 and 2008. There have been changes in methodologies over time, however, a decrease in cybercrime surveys occurred (particularly those using college student samples) and an increase in the use of existing data/websites occurred. Theory tests decreased and studies on the criminal justice response increased. In the same timeframe, there was an increase in interdisciplinary articles and international collaborations. In fact, in 2008, just two of the articles involved interdisciplinary teams; in 2008, this increased to seventeen. Also, in 2008, just one of the articles involved an international collaboration; in 2017, 19 of the articles were international collaborations.

Discussion and Conclusion

The results of this study show that interdisciplinary cybercrime studies are rare, but they are increasing. The same can be said of international collaborations between U.S. authors and authors from other countries. The findings also show that the methodologies and addressed topics aligned with the disciplinary backgrounds of the authors in cybercrime studies. In addition, computer scientists were more likely to engage in international collaborations and the number of authors increased the likelihood of international teams, mixed gender teams, and soft/hard sciences teams, but not interdisciplinary teams. The findings also show a trend suggesting more international collaborations, an increase in interdisciplinary efforts, and a reduction of student samples in favor of public surveys. These findings have implications for future cybercrime research.

First, the upsurge in research by computer scientists and criminologists has been noted elsewhere (Holt, 2017). Much of this research relies on existing data, perhaps in part due to the research expertise of computer scientists and the availability of online data. Also, due to the fact that it is hard to identify offenders (Jaishankar, 2018), it is harder to include them in cybercrime studies. Cyber criminologists are encouraged to bridge both disciplinary and methodological divides in their future efforts. Doing so will provide rich insight in cyber offending.

Second, it is important that strategies are developed to reward interdisciplinary research. Because interdisciplinary cybercrime studies receive fewer citations, one must question the utility of using raw number of citations to judge the value of interdisciplinary endeavors. It is plausible that some scholars might resist working outside of their discipline for fear that their research will not be valued by their disciplinary colleagues. The lower number of citations for interdisciplinary articles suggests that these concerns have at least some merit. At the same time, given the interdisciplinary nature of cybercrime, it is imperative that cyber criminologists resist the temptations to stay solely within their disciplinary domains.

Third, the need for international collaborations is clear. Here, cyber criminologists are encouraged to look to computer scientists, who have apparently figured out strategies to conduct international research. After all, if cyber criminals can cross international borders through cyberspace with ease, cyber criminologists could do the same!

Fourth, graduate students should be better prepared in four areas: cybercrime, international research/globalization, interdisciplinary research, and strategies to conduct cybercrime research. This last area is particularly worthwhile. Strategies to study cybercrime, while similar to traditional criminological research strategies, are qualitatively different. Issues such as sample selection, the global nature of the behavior, the possibility that online data used in a study might disappear, the risk of computer viruses, and a range of ethical issues arise (Holt, 2015).

Specific recommendations for future cybercrime studies can also be suggested. Obviously, as the virtual world changes, research opportunities for cyber criminologists will change as well. While theory tests appear to be diminishing, let's hope that such studies do not go the way of the dinosaur. The value in understanding the factors causing cyber offending cannot be understated. In addition, researchers should delve further into the question of why international and interdisciplinary cybercrime studies are cited less often. In addition, research should explore what it is about certain types of cybercrime studies that make those studies more likely to be cited. It is also essential that cyber criminologists continue to focus on public attitudes, the criminal justice response, and more-tech driven crimes.

Finally, it is important that the increase in interdisciplinary and international collaborations be highlighted. This increase points to the success of the *International Journal of Cyber Criminology*, members of its editorial board, and members of the International Interdisciplinary Research Consortium on Cybercrime to promote and publish articles that are responsive to the dynamics of cyber offending. The task at hand is for these scholars to continue to do the same and to encourage graduate students to join in their efforts.

Acknowledgement

This research is supported in part by the National Science Foundation under grant DGE-1723635.

References

Acar, K. V. (2016). Sexual extortion of children in cyberspace. *International Journal of Cyber Criminology, 10*(2), 110-126.

Archer, N. (2011). Consumer identity theft prevention and identity fraud detection behaviours. *Journal of Financial Crime*, *19*(1), 20-36.

Bachmann, M. (2010). The risk propensity and rationality of computer hackers. *International Journal of Cyber Criminology*, *4*(1/2), 643-656.

Balzacq, T., & Cavelty, M. D. (2016). A theory of actor-network for cyber-security. *European Journal of International Security*, *1*(2), 176-198.

Barlow, C., & Awan, I. (2016). "You need to be sorted out with a knife": The attempted online silencing of women and people of Muslim faith within academia. *Social Media+ Society*, *2*(4), 1-11.

Benjamin, V., Samtani, S., & Chen, H. (2016). Conducting large-scale analyses of underground hacker communities. In Holt, T. J. (Ed.), *Cybercrime Through an Interdisciplinary Lens* (pp. 56-75). London: Routledge.

Bergen, E., Antfolk, J., Jern, P., Alanko, K., & Santtila, P. (2013). Adults' sexual interest in children and adolescents online. *International Journal of Cyber Criminology*, *7*(2), 94-111.

Bishop, J. (2013). The effect of de-individuation of the Internet Troller on Criminal Procedure implementation: An interview with a Hater. *International Journal of Cyber Criminology*, *7*(1), 28-48.

Bossler, A. M. (2017). Need for debate on the implications of honeypot data for restrictive deterrence policies in cyberspace. *Criminology & Public Policy*, *16*(3), 681-688.

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, *3*(1), 400–420.

Bossler, A. M., & Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice*, *38*(3), 227-236.

Branch, K., Hilinski-Rosick, C. M., Johnson, E., & Solano, G. (2017). Revenge porn victimization of college students in the United States: An exploratory analysis. *International Journal of Cyber Criminology*, *11*(1), 128-142.

Brenner, S. W. (2006). Cybercrime jurisdiction. *Crime, law and social change*, *46*(4-5), 189-206.

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*, *29*(3), 408-433.

Burgard, A., & Schlembach, C. (2013). Frames of fraud: A qualitative analysis of the structure and process of victimization on the Internet. *International Journal of Cyber Criminology*, *7*(2), 112–124.

Calderoni, F. (2010). The European legal framework on cybercrime: striving for an effective implementation. *Crime, law and social change*, *54*(5), 339-357.

Choi, K. S., Lee, S. S., & Lee, J. R. (2017). Mobile phone technology and online sexual harassment among juveniles in South Korea. *International Journal of Cyber Criminology*, *11*(1), 110-127.

Collins, J. D., Sainato, V. A., & Khey, D. N. (2011). Organizational data breaches 2005-2010. *International Journal of Cyber Criminology*, *5*(1), 794-810.

Conradt, C. (2012). Online auction fraud and criminological theories. *International Journal of Cyber Criminology*, *6*(1), 912-923.

D'Ovidio, R., Mitman, T., El-Burki, I. J., & Shumar, W. (2009). Adult-child sex advocacy websites as social learning environments: A content analysis. *International Journal of Cyber Criminology*, *3*(3), 421-440.

Dion, M. (2010). Advance fee fraud letters as Machiavellian/Narcissistic narratives. *International Journal of Cyber Criminology*, *4*(1/2), 630-642.

Downing, S. (2010). Online gaming and the social construction of virtual victimization. *Eludamos. Journal for Computer Game Culture*, *4*(2), 287-301.

Gunter, W. D. (2008). Piracy on the high speeds. *International Journal of Criminal Justice Sciences*, *3*(1), 54-68.

Hay, C., Meldrum, R., & Mann, K. (2010). Traditional bullying, cyber bullying, and deviance: A general strain theory approach. *Journal of Contemporary Criminal Justice*, *26*(2), 130–147. DOI: 10.1177/1043986209359557

Higgins, G. E. (2007). Digital piracy, self-control theory, and rational choice: An examination of the role of value. *International Journal of Cyber Criminology*, *1*(1), 33-55.

Higgins, G. E., Wilson, A. L., & Fell, B. D. (2005). An application of deterrence theory to software piracy. *Journal of Criminal Justice and Popular Culture*, *12*(3), 166-184.

Higgins, G. E., Wolfe, S. E., & Marcum, C. D. (2008). Music piracy and neutralization: A preliminary trajectory analysis from short-term longitudinal data. *International Journal of Cyber Criminology*, *2*(2), 324–336.

Hinde, S. (2003). The law, cybercrime, risk assessment and cyber protection. *Computers & Security*, *22*(2), 90-95.

Hinde, S. (2005). Identity theft and fraud. *Computer Fraud & Security, 2005*(6), 18-20.

Hinduja, S. (2001). Correlates of Internet software piracy. *Journal of Contemporary Criminal Justice*, *17*(4), 369–382. DOI: 10.1177/1043986201017004006

Hinduja, S. (2004). Perceptions of local and state law enforcement concerning the role of computer crime investigative teams. *Policing: An International Journal of Police Strategies & Management*, *27*(3), 341-357.

Hinduja, S. (2012). General strain, self-control, and music piracy. *International Journal of Cyber Criminology*, *6*(1), 951-967.

Hinduja, S., & Patchin, J. W. (2010). Bullying, cyberbullying, and suicide. *Archives of suicide research*, *14*(3), 206-221.

Holt, T. J. (2012). Exploring the intersections of technology, crime, and terror. *Terrorism and Political Violence*, *24*(2), 337-354.

Holt, T. J. (2015). Qualitative criminology in online spaces. In Copes, H., & Miller, J. M. (Eds.), *The Routledge Handbook of Qualitative Criminology,* (pp. 189-204). London: Routledge.

Holt, T. J. (2017a). Situating the problem of cybercrime in a multidisciplinary context. In T. J. Holt (Ed.), *Cybercrime Through an Interdisciplinary Lens* (pp. 1-16). London: Routledge.

Holt, T. J. (2017b). On the value of honeypots to produce policy recommendations. *Criminology & Public Policy*, *16*(3), 739-747.

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, *35*(1), 20-40.

Holt, T. J., & Bossler, A. M. (2015). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. London: Routledge.

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2010). Social learning and cyber-deviance: Examining the importance of a full social learning model in the virtual world. *Journal of Crime and Justice*, *33*(2), 31-61.

Holt, T. J., & Dupont, B. (2019). Exploring the factors associated with rejection from a closed cybercrime community. *International Journal of Offender Therapy and Comparative Criminology*, *63*(8), 1127-1147.

Holt, T. J., & Graves, D. C. (2007). A qualitative analysis of advance fee fraud e-mail schemes. *International Journal of Cyber Criminology*, *1*(1), 137-154.

Holt, T. J., & M. Kilger, Techcrafters and makecrafters: A comparison of two populations of hackers. *2008 WOMBAT Workshop on Information Security Threats Data Collection and Sharing*, Amsterdam, 2008, pp. 67-78. DOI: 10.1109/WISTDCS.2008.9

Holt, T. J., Smirnova, O., & Hutchings, A. (2016). Examining signals of trust in criminal markets online. *Journal of Cybersecurity*, *2*(2), 137-145.

Holt, T. J., Strumsky, D., Smirnova, O., & Kilger, M. (2012). Examining the social networks of malware writers and hackers. *International Journal of Cyber Criminology*, *6*(1), 891–903.

Hunton, P. (2011). The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation. *Computer Law & Security Review*, *27*(1), 61-67.

Hutchings, A., & Holt, T. (2018). Interviewing cybercrime offenders. *Journal of Qualitative Criminal Justice and Criminology, 7*(1), 75-95.

Jaishankar, K. (2007). Cyber criminology: Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology*, *1*(1), 1-6.

Jaishankar, K. (2008). Space transition theory of cyber crimes. In F. Schmallager & M. Pittaro, (Eds.), *Crimes of the Internet,* (pp. 283-301). Upper Saddle River, NJ: Prentice Hall.

Jaishankar, K. (2009). Sexting: A new form of Victimless Crime?. *International Journal of Cyber Criminology*, *3*(1), 21-25.

Jaishankar, K. (2010). The future of cyber criminology: Challenges and opportunities. *International Journal of Cyber Criminology, 4*(1&2), 26–31.

Jaishankar, K. (2011). Introduction/ Conclusion. In K. Jaishankar (Ed.), *Cyber criminology: Exploring Internet Crimes and Criminal Behavior,* (pp. xxvii–xxxv and pp. 411-414). Boca Raton, FL: CRC Press.

Jaishankar, K. (2018). Cyber criminology as an academic discipline. *International Journal of Cyber Criminology, 12*(1), 1-8.

Jang, H., Song, J., & Kim, R. (2014). Does the offline bully-victimization influence cyberbullying behavior among youths? Application of general strain theory. *Computers in Human Behavior*, *31*, 85-93.

Jayawardene, K. & Broadhurst, R. (2007). Online Child Sex Solicitation: Exploring the feasibility of a research 'sting'. *International Journal of Cyber Criminology*, *1*(2), 228-248.

Jegede, A. E., Ajayi, M. P., & Allo, T. (2016). Risk and investment decision making in the technological age: A dialysis of cyber fraud complication in Nigeria. *International Journal of Cyber Criminology*, *10*(1), 62-78.

Jones, H., Maimon, D., & Ren, W. (2016). Sanction threat and friendly persuasion effects on system trespassers' behaviors during a system trespassing event. In T. J. Holt (Ed.), *Cybercrime Through an Interdisciplinary Lens,* (pp. 164-180). London: Routledge.

Kelly, G., & Gan, D. (2011). Analysis of attacks using a honeypot. In *International Cybercrime, Security and Digital Forensics Conference*.

Kerstens, J., & Veenstra, S. (2015). Cyber bullying in the Netherlands: A criminological perspective. *International Journal of Cyber Criminology*, *9*(2), 144-161.

Kopp, C., Layton, R., Sillitoe, J., & Gondal, I. (2015). The role of love stories in romance scams: A Qualitative Analysis of Fraudulent Profiles. *International Journal of Cyber Criminology*, *9*(2), 205-217.

Kraft, E. M., & Wang, J. (2009). Effectiveness of cyber bullying prevention strategies. *International Journal of Cyber Criminology*, *3*(2), 513-535.

LaBrie, J., Collier, A., & Palmer, A. (2010). The Norton cybercrime report. Retrieved from: https://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_USA-Human%20Impact-A4_Aug4-2.pdf.

Lembrechts, L. (2012). Digital image bullying among school students in Belgium. *International Journal of Cyber Criminology*, *6*(2), 968-983.

Luppicini, R. (2014). Illuminating the dark side of the internet with actor-network theory. *Global Media Journal, 7*(1), 35-49.

Madarie, R. (2017). Hackers' motivations. *International Journal of Cyber Criminology*, *11*(1), 78-97.

Maimon, D., Alper, M., Sobesto, B., & Cukier, M. (2014). Restrictive deterrent effects of a warning banner in an attacked computer system. *Criminology*, *52*(1), 33-59.

Marcum, C. D., Higgins, G. E., Freiburger, T. L., & Ricketts, M. L. (2012). Battle of the sexes: An examination of male and female cyber bullying. *International Journal of Cyber Criminology*, *6*(1), 904-911.

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2014). Sexting behaviors among adolescents in rural North Carolina. *International Journal of Cyber Criminology*, *8*(2), 68-78.

Marcum, C. D., Higgins, G. E., Ricketts, M. L., & Wolfe, S. E. (2014). Hacking in high school: Cybercrime perpetration by juveniles. *Deviant Behavior*, *35*(7), 581-591.

Martellozzo, E., Nehring, D., & Taylor, H. (2010). Online child sexual abuse by female offenders: An exploratory study. *International Journal of Cyber Criminology*, *4*(1&2), 592-609.

Martinez-Prather, K., & Vandiver, D. M. (2014). Sexting among teenagers in the United States: A retrospective analysis of identifying motivating factors, potential targets, and the role of a capable guardian. *International Journal of Cyber Criminology*, *8*(1), 21-35.

Miller, B., & Morris, R. G. (2016). Virtual peer effects in social learning theory. *Crime & Delinquency*, *62*(12), 1543–1569. DOI: 10.1177/0011128714526499

Moitra, S. (2005). Developing Policies for Cybercrime. *European Journal of Crime, Criminal Law and Criminal Justice*, *13*(3), 435-464.

Moore, R., & McMullan, E. C. (2009). Neutralizations and rationalizations of digital piracy: A qualitative analysis of university students. *International Journal of Cyber Criminology*, *3*(1), 441-451.

Näsi, M., Oksanen, A., Keipi, T., & Räsänen, P. (2015). Cybercrime victimization among young people: a multi-nation study. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, *16*(2), 203-210.

Navarro, J. N., & Jasinski, J. L. (2012). Going cyber: Using routine activities theory to predict cyberbullying experiences. *Sociological Spectrum*, *32*(1), 81-94.

Ngo, F., & Jaishankar, K. (2017). Special article: Commemorating a decade in existence of the *International Journal of Cyber Criminology*. *International Journal of Cyber Criminology, 11*(1), 1–9. DOI: 10.5281/zenodo.495762

Ngo, F. T., & Paternoster, R. (2011). Cybercrime Victimization. *International Journal of Cyber Criminology*, *5*(1), 773-793.

Ngo, F., Jaishankar, K., & Agustina, J. R. (2017). Sexting. *International Journal of Cyber Criminology*, *11*(2), 161-168.

Nycyk, M. (2016). The new computer hacker's quest and contest with the experienced hackers. *International Journal of Cyber Criminology*, *10*(2), 92–109.

O'Connor, K., Drouin, M., Yergens, N., & Newsham, G. (2017). Sexting legislation in the United States and abroad. *International Journal of Cyber Criminology*, *11*(2), 218–245.

Owen, T., Noble, W., & Speed, F. C. (2017). Biology and cybercrime. In Owen, T., Noble, W., & Speed, F. C*., New Perspectives on Cybercrime,* (pp. 27-44). Palgrave Macmillan, Cham.

Rege, A. (2009). What's love got to do with it? Exploring online dating scams and identity fraud. *International Journal of Cyber Criminology*, *3*(2), 494-512.

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimization. *Criminal justice and Behavior*, *38*(11), 1149-1169.

Rudner, M. (2008). Misuse of passports: identity fraud, the propensity to travel, and international terrorism. *Studies in conflict & terrorism*, *31*(2), 95-110.

Salter, M., Crofts, T., & Lee, M. (2013). Beyond criminalisation and responsibilisation: Sexting, gender and young people. *Current Issues in Criminal Justice*, *24*(3), 301-316.

Saunders, K. M., & Zucker, B. (1999). Counteracting identity fraud in the information age: The Identity Theft and Assumption Deterrence Act. *International Review of Law, Computers & Technology*, *13*(2), 183-192.

Smallridge, J. L., & Roberts, J. R. (2013). Crime specific neutralizations. *International Journal of Cyber Criminology*, *7*(2), 125–140.

Steinmetz, K. F. (2015). Becoming a hacker. *Journal of Qualitative Criminal Justice and Criminology*, *3*(1), 31-60.

Su, C., & Holt, T. J. (2010). Cyber bullying in Chinese web forums. *International Journal of Cyber Criminology*, *4*(1/2), 672-684.

Sweeny, J., & Slack, J. (2017). Sexting as 'sexual behavior' under rape shield laws. *International Journal of Cyber Criminology*, *11*(2), 246-260.

Testa, A., Maimon, D., Sobesto, B., & Cukier, M. (2017). Illegal roaming and file manipulation on target computers: Assessing the effect of sanction threats on system trespassers' online behaviors. *Criminology & Public Policy*, *16*(3), 689-726.

Tewksbury, R. (2015). Studying deviance. In Goode, E. (Ed.), *The Handbook of Deviance*, (pp. 210-224). Chichester, West Sussex: John Wiley & Sons.

The International Interdisciplinary Research Consortium on Cybercrime. (n.d.). Retrieved from https://cj.msu.edu/iircc/iircc.html.

Van der Wagen, W., & Pieters, W. (2015). From cybercrime to cyborg crime: Botnets as hybrid criminal actor-networks. *British Journal of Criminology*, *55*(3), 578-595.

Van Ouytsel, J., Ponnet, K., & Walrave, M. (2017). Cyber dating abuse: Investigating digital monitoring behaviors among Adolescents from a Social Learning Perspective. *Journal of Interpersonal Violence*. DOI: 10.1177/0886260517719538

Wall, D. S. (2007). Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police Practice and Research*, *8*(2), 183-205.

Wick, S. E., Nagoshi, C., Basham, R., Jordan, C., Kim, Y. K., Nguyen, A. P., & Lehmann, P. (2017). Patterns of cyber harassment and perpetration among college students in the United States. *International Journal of Cyber Criminology*, *11*(1), 24–38.

Wilsem, J. V. (2013). Hacking and harassment—Do they have something in common? Comparing risk factors for online victimization. *Journal of Contemporary Criminal Justice*, *29*(4), 437-453.

Yar, M. (2005). The novelty of 'cybercrime' An assessment in light of routine activity theory. *European Journal of Criminology*, *2*(4), 407-427.

Young, K. (2008). Understanding sexually deviant online behavior from an addiction perspective. *International Journal of Cyber Criminology*, *2*(1), 298–307.