INPRESS at International Journal of Criminal Justice Sciences

Cybersecurity and Criminal Justice: Exploring the Intersections

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

Abstract
The study of cybersecurity is an interdisciplinary pursuit that includes STEM disciplines as well as the social sciences. While research on cybersecurity appears to be central in STEM disciplines, it is not yet clear how central cybersecurity and cybercrime is to criminal justice scholarship. In order to examine the connections between cybersecurity and criminal justice, in this study attention is given to the way that criminal justice scholars have embraced cybercrime research and coursework. Results show that while there are a number of cybercrime courses included in criminal justice majors, there are not a large number of cybercrime research studies incorporated in mainstream criminal justice journals.

Keywords: Cybersecurity, Cybercrime, Computer crime, Criminal justice, Academic programs, Interdisciplinary curriculum.

Introduction

The advent of the computer has changed the way individuals behave. From personal interactions to business interactions, much of what we do is now – in some form or fashion – connected to technology. A similar point can be made about crime; namely, a significant amount of crime is connected to technology. Our understanding about the connection between crime and technology, however, has not kept pace with the technological changes that have shaped criminal behavior.

Indeed, terms such as computer crime, Internet crime, cybercrime, and cybersecurity are now a part of the criminological lexicon. The development of these criminological concepts, and related laws, is a recent phenomenon. Florida was the first state to develop a computer crime law in 1978 (Hollinger & Lanza-Kaduce, 1988). Other states and the federal government followed suit. The development of these laws – unlike other laws such as drug laws, drunk driving laws, and domestic violence laws – were not traced to a group of advocates wanting legal changes. Instead, these laws were seen as a necessary extension of property laws in response to new opportunities for individuals to commit crimes (Hollinger & Lanza-Kaduce, 1988).

The evolution of cybercrime has not occurred in a vacuum. Other disciplines, particularly those in the STEM (Science, Technology, Engineering, and Mathematics) areas, have also responded to the technological changes with new courses, new avenues of research, and new careers. What is not clear, however, is the degree to which criminal justice scholars and criminologists have kept pace with these changes. As well, the connections between cybersecurity and criminal justice, while clear to criminologists, have not been empirically addressed. Better understanding of the connections between criminal justice and cybersecurity will help to strengthen our efforts to promote safer computing in all its forms.

[1] Vice Provost and Professor, Department of Sociology and Criminal Justice, 2020B Koch Hall, Old Dominion University, Norfolk, VA USA. E-mail: bpayne@odu.edu.
[2] PhD Student, Graduate Program in International Studies, 2019 Koch Hall, Old Dominion University, Norfolk, VA 23529. E-mail: lhadzhid@odu.edu.

Review of Literature

Cybersecurity has been described as the biggest threat facing financial institutions (McGee, 2016; Reuters, 2017), the federal government (Boyd, 2016), corporations (Moritz and Burg, 2015), and investors (Winn, 2017). It seems to be well accepted that cybersecurity is a growing threat that must be addressed. The response in higher education has been the development of cybersecurity academic programs, an increase in cybersecurity research, and the receipt of federal funds to support the expansion of cybersecurity programming and scholarship. Much of the focus, however, seems to be devoted to STEM areas even though criminal justice – as an academic discipline – has a great deal to offer in response to this growing technological threat. In particular, criminologists can help in (1) defining cybercrime, (2) explaining cyber offending and victimization; (3) identifying guardianship activities, (4) measuring victimization and offending, (5) developing future employees, (6) expanding the field of digital forensics, (7) determining interventions, (8) developing, researching, and understanding cyber law, (9) seeking NSA Designation, and (10) conducting interdisciplinary research. Each of these are discussed below.

Defining cybercrime. Perhaps one of the strengths of criminology is its ability to define crime in its various forms. A popular definition of crime refers to the behavior as "illegal acts committed in violation of the criminal law without defense or justification and sanctioned by the state as a felony or misdemeanor" (Tappan, 1960, p. 10). Cybercrime, then, would be illegal acts involving cyber technologies that are in violation of the criminal law, and so on. Another legal scholar writes that "cybercrime, like crime, consists of engaging in conduct that has been outlawed by a society because it threatens social order" (Brenner, 2012, p. 6). To be sure, legal definitions of crime (and cybercrime) are the foundation of a criminal justice approach to wrongful behavior.

Criminologists, however, encourage a broader orientation when defining crime. Within this broader perspective, criminologists might point to the following ways to define different types of cybercrime:

- *Defining cybercrime from a harm orientation* would focus more on whether the behavior hurts someone and less on whether the behavior is defined as criminally illegal.
- *Defining cybercrime from an ethical orientation* would focus more on whether the behavior is ethical and less on whether the behavior is criminal (e.g., is it ethical for companies to track individuals' whereabouts?).
- *Defining cybercrime from a social constructionist perspective* would focus on how cyber offenses came to be defined as illegal, how norms have changed over time, and the processes guiding those changes.
- *Defining cybercrime from a deviance perspective* would focus more on whether behaviors are defined as abnormal and less on legal prohibitions.
- *Defining cybercrime from a white-collar crime orientation* would focus on how certain types of cybercrimes are actually white-collar crimes (or crimes committed in the course of a legitimate occupation).
- *Defining cybercrime from workplace deviance orientation* would focus on how certain cyber behaviors in the workplace might be against workplace rules, but not illegal (e.g., using work email for personal reasons, opening spam, Internet shopping while at work, etc.).

This list is not exhaustive. The main point to be made is that criminologists would encourage a broader orientation to cybercrime than might be found in the STEM disciplines.

Explaining cyber offending and victimization. Criminologists devote a great deal of effort to explaining human behavior. The phrase "human factors" is a psychology concept that explores how individual factors contribute to behavior. This phrase can be extended to criminal justice and

criminology given the effort of criminologists to explain why individuals commit crime. In fact, of the criminologists involved in studying cybercrime, many of their studies have focused on explaining cybercrime and cyber victimization. The most popular criminological explanations of cybercrime include neutralization theory, self-control theory, learning theory, and routine activities theory.

Neutralization theory suggests that individuals know right from wrong, but they rationalize or neutralize their behavior in order to give themselves the justification to commit a crime. Five "original" neutralizations were developed by Sykes and Matza (1957), the criminologists who developed the theory. These neutralizations and their relevance to cybercrime can be summarized this way:

- Denial of injury - some cyber offenders might rationalize their behavior by convincing themselves that no one will be hurt from their offending.
- Denial of victim - some cyber offenders might rationalize their behavior by convincing themselves that the victim deserves the harm they experience (e.g., an employee might justify stealing from the employer through cybercrimes).
- Denial of responsibility - some cyber offenders might rationalize their behavior by stating that they are not responsible for their crimes.
- Appeal to higher loyalties - some cyber offenders might rationalize their behavior by stating they are committing the crime for the good of a larger group (e.g., nation-state crimes by terrorists).
- Condemnation of condemners - some cyber offenders might rationalize their behavior by stating that they are committing crimes that the government also commits (e.g., WikiLeaks is often justified by supporters who argue that the behavior provides governmental oversight).

Criminological research has supported the application of neutralization theory to cybercrimes and one research team has identified two neutralizations specific to certain types of cybercrime: (1) digital rights management software defiance refers to frustrations cyber offenders (cyber pirates in particular) have with digital rights software packages and (2) claims of future patronage refer to plans to purchase pirated software in the future (Smallridge & Roberts, 2013).

Suggesting that crime results from low self-control (which is believed to come from bad parenting), *self-control theory* has been tested on cybercrime by different researchers. One research team, for example, found a connection between level of self-control and cyber bullying (Marcum et al., 2012). Another research team found that self-control was connected to music piracy (Gunter et al., 2010). Expanding on these studies, a more recent study found that self-control theory can explain general forms of online deviance as well (Donner et al., 2014).

Learning theory (in its many different forms) has also been applied to cybercrime. Differential association, one of the more popular criminological learning theories, suggests that criminals learn how to commit crime through interactions with others, they learn the reasons to commit crime, and they learn motives for committing crime. One cybercrime study uses this theory to help understand how terrorists use the Internet to carry out their offenses (Freiburger & Crane, 2008). According to the authors, "Terrorist groups are no longer bonded by geographical boundaries; instead, through the Internet they are able to reach individuals in any location and recruit members from these locations. Once these relationships are established, the terrorist group becomes an important differential association for individuals, allowing them to be recruited as members" (p. 312). Others have used learning theory to study online sexual harassment (Choi et al., 2017), cyber deviance (Holt et al., 2010), and computer hacking (Morris & Blackburn, 2009). The studies find various levels of support for social learning theory, suggesting that the theory may help to understand some forms of cyber offending, but not all of them.

Routine activities theory has been used to explain cybercrime as well. Traced to Cohen and Felson (1979) who argued that crime occurs when three elements are present at the same time and in the same place (e.g., the absence of a capable guardian, the presence of motivated offenders, and a suitable target), cybercrime researchers have applied the theory to attacks on the critical infrastructure (Rege, 2014), malware infections (Bossler & Holt, 2009), cyber victimization (Marcum, 2009), cyber harassment (Wick et al., 2017), and other harmful cyber behaviors. More recently, criminologists have begun to explore how changes in the targets, guardians, and offenders can be used to model cybersecurity (Yang and Rege, 2017). The implications from such research will be groundbreaking and will have direct implications for strategies to improve cybersecurity guardianship.

Identifying guardianship strategies. Many criminal justice scholars focus their research solely on the development of strategies to protect against victimization. While computer engineers and computer scientists have the wherewithal to develop the computer technology needed to enhance a computer's security, the ability of that technology to actually work is best understood through a criminological lens. As an example, David Maimon and his colleagues (2013) used a honey pot to conduct an experiment. A honey pot is a network set up for the purpose of being attacked so that researchers can study the behavior of the attackers. In this study, the research team assigned the attackers to one of two teams – a team that received a warning in the form of a banner and a team that did not receive any warning at all. The researchers found that the warning did not keep offenders out, but it did get them out of the network quicker. They also found attack patterns were related to foreign students' countries of origins, which suggests that "the human element is a key component when dealing with computer security" (p. 337). In other words, technology by itself is not enough for guardianship; rather a criminological understanding of human behavior helps to fully implement guardianship strategies.

Measuring victimization and offending. Criminologists also provide insight into the extent of various forms of cyber offending and victimization. Using data from an international survey of more than 60,000 students, for instance, one study found that "the overall illegal downloads rate across all countries stood at 47.47%, while hacking perpetration was 5.38 percent" (Udris, 2016, p. 133). Another study of 378 teenagers found that a third of them had engaged in sexting behaviors (Martinez-Prather & Vandiver, 2014). As well, criminal justice scholars have debated the best sources of crime data – are they official reports of crime or self-reported experiences with crime? The answer is that "it depends." Criminologists recognize that official reports from government agencies miss the "dark figure" of crime (e.g., those crimes never reported) while also understanding that self-reported experiences with cybercrime and victimization are flawed as well. Still, depending on the nature of the cybercrime research, both official crime data and self-reported studies can be used to measure cyber offending and victimization.

Developing future employees. For higher education institutions that have criminal justice programs, the criminal justice major is frequently among the larger programs at the institution. It is often wrongly assumed that most of these majors are seeking careers in law enforcement. In reality, enrolled in a liberal arts major, criminal justice students aspire to all types of careers – from policing to the courts to corrections to corporate security to human services and so on. Some criminal justice graduates will work in the public sector and some will work in the private sector.

What does this have to do with cybersecurity? With appropriate training, criminal justice graduates could potentially be prepared for some of the "softer" careers in cybersecurity. At the end of 2017, nearly 750,000 individuals in the United States worked in cybersecurity careers. More striking, though, is the fact that there were more than 280,000 job openings in the United States at that same time (Cyberseek.org, 2017). While many of these jobs would requires graduates from a STEM

discipline, others require employees with strong communication, critical thinking, and policy development skills (or skills that are promoted in criminal justice). Indeed, nearly 81,000 of the job openings were in the "Oversee and Govern" category, a category characterized by the National Initiative on Cybersecurity Education as one that "Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work." In addition, roughly 45,000 of the job openings were in the "Collect and Operate" category, a category which has been compared to counter intelligence activities (Shoemaker et al., 2016). To be sure, having a criminal justice degree by itself will not prepare students for these jobs; however, criminal justice coursework combined with the appropriate STEM courses or cybersecurity/cybercrime courses would provide graduates the skills they need to thrive in those careers.

Expanding the field of digital forensics. Digital forensics is a relatively new type of criminal investigation that refers to investigations of cyber, computer, electronic, or other types of cybercrimes. The historical development of digital forensics involved a number of criminal justice professionals. Describing the early stages of digital forensics, one author wrote:

In the Baltimore area, forensic practitioners from the FBI, U.S. Secret Service, Maryland State Police and Baltimore County Police started an ad hoc organization called "Geeks with Guns." In the United Kingdom, practitioners from many law enforcement agencies formed the Forensic Computing Group (FCG) under the auspices of the Association of Chief Police Officers (ACPO). It was during this epoch that the High Tech Crime Investigation Association was formed. (Pollit, 2010, p. 8).

Some criminal justice scholars have characterized digital forensics as an occupation, but not yet a profession (Losavio et al., 2016). Steps to becoming a profession, it is argued, would include forming a national association, reserving training for the occupation to higher education, developing a code of ethics, and mobilizing politically (Losavio et al., 2016). Given the fact that criminal justice only recently (in the past fifty years) became a profession, and that digital forensics was partly born out of criminal justice professionals, criminal justice scholars have an important role in expanding the field of digital forensics.

Determining interventions. Criminal justice can also be useful in helping to identify appropriate interventions and responses to cyber offenders. Many criminological studies have explored how offenders are sanctioned for various offenses. These studies help to determine the patterns surrounding the sanctions, whether they are offered consistently, and – in some studies – whether the sentences are effective. In terms of sentencing cybersecurity offenders, one group of criminal justice scholars explored how cybercrime offenders in four states were punished (Marcum et al., 2011). Noting that "multiple pieces of legislation have been passed with the intention of toughening punishments for the various forms of cyber crime offenders," (p. 825) the authors found that female cyber offenders were given longer sentences than male offenders, which was unexpected given that female offenders typically receive shorter sentences. Regarding type of offense, they found that identity theft fraud, and destruction of property offenses received longer sentences than other cyber offenses. The authors conclude, "Whether this type of sentencing is a deterrent to current and future offenders is yet to be seen and worth future research; however, it is a start in the right direction" (p. 33). This is but one other type of research that criminal justice scholars can contribute to cybercrime research.

Developing, researching, and interpreting law. An understanding of the criminal law is key to a full understanding of criminal justice (Hemmens, 2016). Simply defined, law refers to written rules that proscribe certain sanctions when those rules are violated. Virtually all criminal justice students will be required to take a course related to the law. Just as an understanding of the criminal law is

necessary to understand criminal justice, an understanding of cyber law is needed in order to fully understand cybercrime and cybersecurity.

Because it is an area of study grounded in the law, criminal justice offers a framework for developing, researching, and interpreting cyber law. Legal expert Susan Brenner (2012) has identified several ways that cyber activities are regulated by the criminal law. These include:

- *Hacking laws* regulate against the unauthorized access of a computer (p. 22).
- *Federal malware law* was incorporated into the Computer Fraud and Abuse Act of 1991 to make it illegal to intentionally damage computers by transmitting viruses, worms or other forms of malicious malware (p. 42).
- *Cybercrimes against property* include theft, cyber bank theft, theft of trade secrets, theft of services, various forms of fraud, extortion, and blackmail.
- *Cybercrimes against persons* include cyber harassment, cyber stalking, and cyber threats.

Various jurisdictions have developed different laws to govern these behaviors. In addition to the criminal law, a full understanding of the procedural law (e.g., the body of law that dictates among other things how professionals are able to gather and use evidence) is needed for those who respond to cybercrimes. "Digital crime scenes" present a number of challenges for legal officials (Brenner, 2012). These challenges are perhaps best understood through a criminal justice or legal framework.

Seeking NSA Center of Academic Excellence Designation. Criminal justice also potentially plays a role in helping cybersecurity programs seek designation as a Center of Academic Excellence from the National Security Agency. Similar to an accreditation process, the CAE designation is a "stamp of approval" from the National Security Agency that signifies that a cybersecurity curriculum rigorously addresses topics of value to the federal government's cybersecurity workforce. NSA offers designations in the areas of cyber defense, information assurance, and cyber operations. These designations are offered for educational programs and for research programs. They are open to all regionally accredited higher education institutions in the U.S. Requirements for designation vary across two-year, four-year, and graduate programs.

To be designated as an NSA Center of Academic Excellence, the program must submit a detailed application that shows how the cybersecurity coursework meets criteria set by the NSA. These criteria vary across type of designations (e.g., cyber defense, information assurance, cyber operations, or research). The program must submit course syllabi and course materials showing how the criteria area is addressed in the cybersecurity program. It is here that criminal justice coursework may become relevant. For instance, for programs to receive a designation in cyber operations, there must be evidence that the program faculty addresses cybersecurity as an interdisciplinary topic. Combining criminal justice with STEM is most certainly an interdisciplinary avenue. In addition, each of the designations include different levels of law and policy as possible evaluative criteria. Here again, criminal justice can play a meaningful role.

Designation as a Center of Academic Excellence can boost a cybersecurity program's resources and prominence. In terms of resources, the designation opens up the amount of cybersecurity scholarship dollars that can be awarded to the institution and the faculty from the program become eligible for additional cybersecurity grants. In turn, it is believed that those institutions with the designation will be more sought after by cybersecurity students than those institutions without the designation.

Conducting interdisciplinary research. Because its historical underpinnings are multidisciplinary, criminal justice as an area of study offers many opportunities for interdisciplinary research efforts. The opportunity for interdisciplinary research is especially salient for cybercrime. Seizing on this opportunity, criminologist Thomas Holt recently led the development of the International

Interdisciplinary Research Consortium on Cybercrime. In the announcement of this effort, Holt (2016) wrote, *"...we have to develop an holistic research agenda to combat cybercrime and improve cybersecurity postures. This is only achieved by linking the social sciences with computer science and engineering disciplines to better understand all facets of this problem. Understanding both the human and the system is the only way to improve the state of the field of cybersecurity."* Demonstrating this commitment to an interdisciplinary approach to cybersecurity, Holt – at Michigan State University's School of Criminal Justice – has led an annual interdisciplinary cybercrime conference over the past five years.

While Holt and his colleagues have done a remarkable job in promoting the interdisciplinary nature of cybercrime, it is not clear the degree to which criminal justice (as an area of study) has embraced cybersecurity or the degree to which cybersecurity programs have embraced criminal justice. To fill this void in the literature, in this study, we consider the following questions: (1) To what degree is cybersecurity embraced in criminal justice programs and by criminal justice scholars?; (2) To what degree is criminal justice embraced in cybersecurity programs?; and (3) Does the presence of criminal justice coursework impact NSA designation? Answering these questions will help to determine whether criminal justice ideals are helping to respond to cybersecurity trends.

Methods

To answer these questions, we focused on the degree to which national criminal justice and criminology organizations embraced cybersecurity, the degree to which criminologists wrote about the topics, and intersections between cybersecurity and criminal justice in a sample of higher education institutions. The sample of institutions was developed using two separate sampling frames. First, all institutions that had received some form of NSA designation as of Spring 2017 were included. Second, all institutions of members of the Academy of Criminal Justice Sciences were included. The combination of these two sampling frames resulted in a sample of 615 higher education institutions.

A coding schedule was developed to identify how each institution addressed cybersecurity and criminal justice. The coding schedule included information on whether the institution had a cybersecurity program, and if so, the degree level offered (bachelor's, master's, doctoral, associate degree or an undergraduate/graduate certificate), whether it had a criminal justice program, whether the institution offered criminal justice courses in its cybersecurity program (and the names of the classes), whether the institution offered cybersecurity courses in its criminal justice program (and the names of the classes), whether the cybersecurity program was public or private, whether the cybersecurity program was NSA designated, and the type of designation (if any) held by the institution's cybersecurity program. The second author visited each institution's website and reviewed their course catalogues to complete the coding schedule for each institution.

The coding design deserves some attention in regard to the question if an institution has a cybersecurity program or not. Some of the programs had names typical for STEM disciplines, such as "Information Science", but they still had a minor focus (not separate concentrations) on cybersecurity. These curricula were not considered parts of cybersecurity programs since the "cybersecurity" element was peripheral, not central for the instructional methodology of cybersecurity. An institution was listed as having cybersecurity program only if it had a name of the program that refers to the methods and goals of cybersecurity (such as "Digital Forensics" or "Cyber Criminology"). Institutions offering STEM-programs with a focus/concentration in cybersecurity or its variations were considered as having "cybersecurity" programs. Also worth mentioning is that some institutions had an NSA-designation for research but not a cybersecurity

program. Lastly, others did not offer such program but had established instead student clubs and centers for cybersecurity as an extracurricular effort.

Findings

Table 1 shows how often cybercrime topics are covered in national criminology/criminal justice associations, at their conferences, and in criminal justice journals. The topics do not appear with great regularity in any of these forums, with the exception of general searches of criminal justice abstracts. More specifically, 495 articles in criminal justice abstracts have the word "cybersecurity" in the article's title. Of those 495 articles, however, just 39 were published in academic journals. The vast majority of "cybersecurity" articles in criminal justice abstracts appear in magazines (n=406).

Table 1. Cybercrime, Cybersecurity, Computer Crime, and Internet Crime in Research Studies*

	Cybercrime	Cybersecurity	Computer Crime	Internet Crime
ACJS Website	28	7	31	20
ASC Website	56	9	72	6
CJ Abstracts (title)	95	494	61	17
NCJRS Abstracts Database (title)	56	5	291	73
Criminology (all fields)	8	1	4	0
Criminology (title)	0	0	1	0
JQ (text)	10	3	9	1
JQ (title)	1	0	0	0
Crime and Delinquency (text)	1	0	0	0
Crime and Delinquency (title)	0	0	0	0
JRCD (text)	4	0	2	2
JRCD (title)	0	0	1	0
JCJ (all fields)	9	2	8	2
JCJ (title)	0	0	1	0

*Either used CJ abstracts or the journal's publisher site depending on which strategy worked. The searches were conducted in December 2017 using various databases. For Justice Quarterly, Crime and Delinquency, and Journal of Research in Crime and Delinquency, we used criminal justice abstracts. For Criminology and Journal of Criminal Justice we used their publisher's website. Searches were done to focus on specific phrases rather than separate words.

To determine whether cybercrime articles appeared in mainstream top-tier criminology/criminal justice journals, searches were done of Criminology, Justice Quarterly, Crime and Delinquency, Journal of Research in Crime and Delinquency, and Journal of Criminal Justice. The results again show a lack of coverage given to the topic. In fact, the phrase "computer crime" appears in the titles of just three articles published in the five journals for the entire duration of the journals' existence. This does not mean that the journals do not publish cybercrime articles as the titles of those articles may simply not include the phrase, but it is an indication that these

topics are rarely covered. In addition, a look at the number of times these concepts appear in any field (or in any part of the article's text) leads to a similar conclusion.

To further understand the connections between criminal justice and cybersecurity, we reviewed the course catalogues of the 615 higher education institutions described above in the methods section. Table 2 provides a summary of these institutions. The vast majority of institutions housed a criminal justice program (86.5%) and a sizable proportion of them offered a cybersecurity program (57.9%). Roughly two-thirds of the institutions were public institutions and the other third were private institutions. In all, 209 of the cybersecurity programs had been designated as NSA Centers of Academic Excellence, with the cyber defense designation for four-year programs being the most popular.

Table 2. Sample Characteristics (n=615)

	n	%
Institution has cybersecurity program	356	57.9
Institution has criminal justice program	531	86.5
Criminal justice courses in cybersecurity program	61	17.1*
Cybersecurity courses in criminal justice program	86	16.2*
NSA Designation	209	34.0
CAEIAE4Y Designation	33	5.4
CAECDE4Y Designation	126	20.5
CAEIAE2Y Designation	11	1.8
CAECDE2Y Designation	32	5.2
CAEIAR Designation	5	.8
CAER Designation	65	10.6
Public Institution	422	68.6
Private Institution	193	31.4

*Percentages are calculated based on the total number of cybersecurity and criminal justice programs respectively.

Regarding specific connections between criminal justice and cybersecurity, of the 531 criminal justice programs in the sample, just 16.2 percent of the programs (n=86) included cybersecurity coursework in the criminal justice curricula, with a handful of the criminal justice programs offering multiple cybersecurity courses. Table 3 shows the names of these courses. As shown in the table, cybercrime or its variations (cyber crime, cybercrimes, introduction to cybercrime) was the most popular cybersecurity course offered in criminal justice. In all, 31 courses were offered under this title or its variation. To be sure, though, a wide range of other cybersecurity courses are included in the criminal justice programs. In fact, 123 different cybersecurity courses are offered in criminal justice programs.

Table 3. Cybersecurity Courses Taught in Criminal Justice Programs

Advanced Digital Forensics	Cyber Threats & Counterintelligence
Advanced Issues in Cybercrime	Digital Crime and Criminal Justice
Agency Experience in Cyber Security	Digital Crime Investigation
Basic Data Recovery	Digital Evidence
Computer Crime (n=7)	Digital Evidence Practicum
Computer Crimes	Digital Forensics (n=2)
Computer Crime: Legal Issues	Digital Forensics I (n=3)
Computer Crime Research and Policy	Digital Forensics II (n=2)
Computer and Electronic Crime	Digital Forensic Analysis
Computer Forensics (n=4)	Digital Forensic Investigation
Computer Forensics II (n=2)	Digital Forensics Capstone
Computer Forensics III (n-2)	Digital Forensics in the Criminal Justice System
Computer Forensics and Cybercrime	Digital Forensics Hardware and Acquisition
Computer Network Investigations	Digital Forensics Investigations and Applications
Computer Security and Data Protection	Forensic Designations (CCE/ACE)
Contemporary Issues in Digital Forensics	First Responder Tools and Application
Crime in Cyberspace	Fundamentals of Cybercrime
Criminology of Cybercrime	Fundamentals of Computer Crime.
Cybercrime (n=12)	Hardening the Enterprise Network
Cybercrimes	Incident Response & Network Forensics
Cybercrime I: Legal Issues/Investigative Procedures	Information Assurance Risk and Compliance
	Information Security
Cybercrime II: Internet Vulnerabilities and Criminal Investigation	Information System Threats, Attacks and Defenses
Cybercrime and Digital Terrorism	Information Security and Assurance
Cybercrime Capstone	Administration
Cyber Crime and Computer Forensics	Information Warfare and Security
Cybercrime and Cybersecurity	Investigating Online Crimes
Cybercrime and Forensics	Insider Threat
Cybercrime and the Law	Interdisciplinary Topics in Cybersecurity
Cybercrime Investigation	Internet Vulnerability Criminal Act
Cybercrime Law and Investigations	Introduction to Computer Forensics (n=2)
Cybercrime, Technology, and Social Change	Introduction to Cybercrime (n=7)
Cyber and Surveillance Law and Governance	Introduction to Cyber Crime and Computer
Cyber Crime (n=10)	Security
Cyber Crimes (n=2)	Introduction to Cyber Security
Cyber-Crime and Cyber-Security	Intro to Cyber Security for Criminal Justice
Cyber Crime-Criminal and Civil Investigation	Investigation of Computer Crime
Cyber Crime, Ethics, and Law	Investigation of Cyber Crime
Cyber Crime and Security	Issues in Cybercrime
Cyber Crime, Security and the Law	Large Scale Cybercrime and Terrorism
Cyber Criminals and Computer Forensics	Malware Basics
Cyber Criminology	Mobile Device Forensics
Cybercriminology	Mobile Forensics
Cyber Ethics and Internet Culture	Network Forensics and Incident Response

Table 3 Continued	Network Forensics
	Networking Concepts
Cyber Forensics	Operation and File System Forensics
Cyber Investigations	Penetration Testing and Vulnerability Scanning
Cyber Law.	Principles of Digital Forensics
Cyber Law and Cybercrime	Readings in Cyber Crime
Cyber Law and Policy	Rules of Evidence/Legal Aspects of Cyber Security
Computer Operations in Criminal Justice	Security of Information and Technology
Cybersecurity	Security Systems
Cyber Security I	Seminar in Cybercrime
Cyber Security II	Seminar in Cybercrime Investigations
Cybersecurity and Loss Prevention/Exercise Data	Seminar in Cybercrime Law and Policy
Cybersecurity and Loss Prevention	Seminar in Cyber Security
Cybersecurity and Policy	Seminar in Cyber Warfare
Cybersecurity: Law & Ethics	Social Media & Cloud Security
Cyber Security/Law/Money Launder	Software Foundations for Cybersecurity
Cyber Security, Info Tech & Law Enforcement	Special Topics in Criminal Investigations in Cyber Security
Cyber Security Senior Seminar	Special Topics in Cyber Security
Cyber Technologies for Criminal Justice	Technology and Cyber Crime
Cyber Terrorism	White Collar and Cyber Crime

A similar pattern was found in the cybersecurity programs when reviewing the criminal justice courses offered in cybersecurity programs. Namely, a wide range of criminal justice courses are offered in the cybersecurity programs. Of the 356 cybersecurity programs in the sample, just 17.6% (n=61) of them included at least one criminal justice course in it. Table 4 shows the criminal justice coursework included in the cybersecurity programs. Introduction to Criminal Justice (n=17) and Criminal Law (n=10) were the most popular criminal justice courses offered in cybersecurity programs. In all, 152 different criminal justice courses are offered in cybersecurity programs.

Tests were conducted to determine whether presence of criminal justice courses in a cybersecurity program was related to the program being designated as an NSA Center of Academic Excellence (see Table 5). Significant differences were found, but in the opposite direction than was expected. In particular, cybersecurity programs that did not include criminal justice coursework in their program were more likely to receive the NSA designation than were those programs including criminal justice coursework. Of the 61 programs that offered criminal justice coursework in the cybersecurity curricula, 27 (44.3%) were NSA designated programs. In contrast, among the programs that did not have criminal justice courses in a cybersecurity program, 61.7% had received the NSA designation. In all, just 13% (27/209) of the NSA designated programs had criminal justice courses in their curricula.

Analyses were also conducted to explore whether differences existed between public and private institutions. Three differences were found. First, of the 422 public institutions, 255 (60%) offered a cybersecurity program. Of the 193 private institutions, 101 (52%) offered a cybersecurity program (Chi Square = 3.56, $p < .05$). Second, public institutions were more likely to be NSA designated. Of the 255 public institutions with cybersecurity programs, 62% (n=158) had an NSA designation. In comparison, of the 101 private institutions, roughly half (50.5%) were NSA-

Table 4. Criminal Justice Courses Taught in Cybersecurity Majors

Administration of Justice	Fraud Prevention and Detection Technologies
Advanced Digital Forensics	Hardening the Enterprise Network
Agency Experience in Cyber Security	Homeland Security
American Government and Politics	Homeland Security and Espionage (5)
Applied Criminology and Crime Prevention (5)	Homeland Security and Legal System
Asset Protection	Incident Response and Network Forensics
Basic Data Recovery	Info Systems Threat
Capstone: International Justice and Human Rights	Information Assurance Risk and Compliance
Compliance & Legal Issues	Information Warfare and Security
Computer Crime(s) (5)	Insider Threat
Computer Security and Data Protection	Internet Investigations
Computer Viruses	Internship and Capstone in Criminal Justice
Constitutional Law	Interview & Interrogation
Constitutional Law & Evidentiary Procedures	Introduction to Administration of Justice
Contemporary Criminal Justice Systems	Introduction to Computer Forensics (2)
Contemporary Criminal Law and Procedures	Introduction to Criminal Justice (17)
Corrections	Introduction to Cyber Crime (2)
Courts and Judicial Process	Introduction to Cyber Security
Crime and Criminology	Introduction to Forensic Science
Crime and Justice Systems	Introduction to Homeland Defense
Crime and Public Policy	Introduction to Homeland Security
Crime Scene Investigation	Introduction to Law and the Legal System
Crime Scene Investigation I	Introduction to Research Methods in Crim.
Crime Scene Investigation II	Introduction to the CJS (2)
Criminal Evidence and Court Procedure	Introduction to the Justice Studies
Criminal Evidence and Procedure(s) (5)	Investigating Online Crimes
Criminal Investigation(s) (3)	Investigation and Criminalistics
Criminal Justice	Investigation of Cyber Crime (5)
Criminal Justice Ethics	Investigations and Business Crimes (5)
Criminal Justice Science Seminar	Juvenile Delinquency and Justice
Criminal Justice Statistics	Law Enforcement (2)
Criminal Justice Systems and Policy	Law, Evidence and Ethics
Criminal Law (10)	Malware Basics
Criminal Law I	Mobile Device Forensics
Criminal Procedure (4)	Mobile Forensics
Criminalistics and Forensics	Network Forensics and Incident Response
Criminology (6)	Networking Concepts
Criminology and Social Control	Payment Systems and Fraud
Criminology Theory	Penetration Testing/Vulnerability Scanning
Cyber and Surveillance Law and Governance (5)	Practical Issues in Cryptography
Cyber Crime and Cyber Terrorism	Principles of Digital Forensics
Cyber Crime Investigations and Forensics I	Procedural Criminal Law
Cyber Crime Investigations and Forensics II	Ethics, Legal, Compliance Issues in Cybersec.
Cyber Crime Investigations and Forensics III	Ethics & Professionalism in Criminal Justice
Cyber Crime, Ethics, and Law	Ethics in Criminal Justice (2)

Table 4 Continued	Evidence
	Firewall & Security Ent Comp
Cyber Crime(s) (4)	First Responder Tools and Application
Cyber Criminal & Civil Investigations	Forensic Designations (CCE/ACE)
Cyber Criminology	Forensics and Crime Scene Investigation
Cyber Ethics and Internet Culture	Fraud
Cyber Forensics (2)	Professional Writing in Criminal Justice
Cyber Law and Cybercrime	Public and Private Security
Cyber Security	Readings in Cyber Crime
Cyber Security I	Risk Assessment and Fraud
Cyber Security Senior Seminar	Risk Assessment and Prevention (5)
Cyber Threats and Counterintelligence	Rules of Evidence/Legal Aspects of Cyber
Cybercrime and Cybersecurity	Security
Cybercrime and Forensics	Security of Information and Technology
Cybercrime and the Law	Seminar in Criminal Justice
Cybercrime Investigation	Social Media and Cloud Security
Cybercrime, Technology, and Social Change (5)	Special Topics in Criminal Investigations in
Cybercriminology	Cybersecurity
Cybersecurity and Loss Prevention	Special Topics in Criminal Justice
Cybersecurity and Loss Prevention/Exercise Data	Special Topics in Cyber Security
Cybersecurity: Law & Ethics	Substantive Criminal Law
Data Analysis for the Criminal Professional	Survey of Criminal Justice
Deviant Behavior/Social Disorganization	Survey of Criminology
Digital Crime Investigation	Terrorism
Digital Evidence	Terrorism and Society
Digital Forensics	The Constitution and Criminal Justice
Digital Forensics I (2)	The Criminal Court
Digital Forensics II (2)	The Law and High Technology Crime
Digital Forensics in the Criminal Justice System	Victimology
Digital Forensics Investigations and Applications	White Collar and Cyber Crime
Diversity and Ethical Dilemmas in Criminal Justice	White Collar Crime(s) (2)
Economic Crime Theory	White-Collar and Economic Crime
Enterprise Risk Management (5)	White-collar Criminology

Table 5. Criminal Justice Coursework and CAE Designation

	CJ in CAE	No CJ in CAE	Chi Square
NSA Designation	27 (44.3)	182 (61.7)	6.34**
CAEIAE4Y Designation	1 (1.6)	32 (10.8)	5.10*
CAECDE4Y Designation	19 (31.1)	107 (36.3)	.58
CAEIAE2Y Designation	2 (3.3)	9 (3.1)	.01
CAECDE2Y Designation	5 (8.2)	27 (9.2)	.06
CAEIAR Designation	1 (1.6)	4 (1.4)	.03

*$p \leq .05$, $p \leq .01$

designated programs (Chi Square = 3.92, $p < .05$). Third, private institutions were more likely to have criminal justice courses in their cybersecurity program. Nearly one-fourth of the private institutions (n=24) offered criminal justice coursework in their cybersecurity program. In comparison, less than 15% (37/218) of the public institutions offered criminal justice coursework in their cybersecurity major (Chi Square = 4.36, $p < .05$).

These findings should be interpreted with some caution. Using course catalogues to identify cybersecurity and criminal justice coursework indicates that the program has certain types of coursework included. It does not, however, give any indication of how often courses are instructed. In addition, our focus has been based on the U.S. higher educational system. As an international problem, it is plausible that other countries have tied together criminal justice and cybersecurity differently. Despite these limitations, these findings lead to some interesting conclusions that provide fodder for future discussion.

Discussion

Generally, our findings suggest that criminal justice is beginning to make inroads into the study of cybersecurity and cybercrime, though the pace and depth of the integration of cybersecurity/cybercrime into criminal justice is seemingly slow. Less than one-fifth of criminal justice programs include cybercrime coursework in their curricula and about the same proportion of cybersecurity programs include criminal justice coursework in their curricula. Those criminal justice programs that have developed cybercrime coursework are in a position to help address the growing demand for cybersecurity professionals. Those that have not are encouraged to consider opportunities for increasing understanding about cybercrime within their criminal justice programs. To assist in efforts to expand cybercrime coursework, it may be helpful to explore possible reasons why cybercrime and cybersecurity coursework is rare in criminal justice programs. This will be followed by practical recommendations aimed at expanding the role of criminal justice in cybersecurity.

Six possible reasons explain why criminal justice programs have not more fully embraced cybersecurity offerings. First, the topic of cybersecurity may not be appealing to program administrators. The very label of "cybersecurity" and "cybercrime" implies a scientific focus which many social scientists may choose to avoid.

Second, the roots of many criminal justice programs – criminology programs in particular – are sociological. Consequently, these programs focus primarily on understanding crime and criminal justice from a sociological perspective. Cybersecurity – at its core – may require more of an applied focus than traditional sociologists are willing to embrace.

Third, because cybersecurity is a new area of study, criminal justice professionals may not fully understand the dynamics of this emerging field. It may be wrongly assumed that cybersecurity is simply about computers and engineering, when in fact, the human element is central to cybersecurity.

Fourth, and somewhat related, it should not be surprising that criminal justice scholars are not fully aware of cybersecurity given that cybercrime is so rarely included as coursework in criminal justice doctoral programs. Our review found very few cybercrime courses taught at the graduate level. While focusing on different topics, others have noted that the presence of certain coursework in doctoral programs will inform the types of research scholars conduct after graduating from those programs (Wright et al, 2008).

Fifth, the seemingly slow introduction of cybersecurity to criminal justice may reflect an overall resistance to interdisciplinary efforts (Payne, 2016). While criminal justice is interdisciplinary by

its very nature, it has been suggested that members of the discipline resist interdisciplinary pursuits. Disciplinary power, lack of resources, administrative misunderstanding about interdisciplinary work, and academic socialization are possible reasons for the resistance to interdisciplinary pursuits (Payne, 2016).

Finally, scholars have noted an overall resistance among criminal justice scholars to study white-collar crime (Lynch et al., 2004; McGurrin et al., 2013). The similarities between white-collar crime and cybercrime may drive some of this resistance by criminal justice scholars. The result of ignoring white-collar crime in criminal justice scholarship has been described as "cyclical" in that when professors do not research the topic, there is less information for professors to teach about and there is less new knowledge which would encourage new scholarship (McGurrin et al., 2013). The same can be said for the lack of criminal justice scholarship on cybercrime.

Despite this dim assessment of the state of criminal justice programing and scholarship in the area of cybersecurity, avenues for better connecting criminal justice and cybersecurity exist. First, and foremost, cybercrime scholars should expand on the foundational successes they have already enjoyed. The International Interdisciplinary Research Consortium on Cybercrime noted above is one example of a great start to promoting interdisciplinary cybercrime efforts. In addition, fruitful endeavors such as the branding of an area of study as "cyber criminology" should be embraced. Coined by Jaishankar (2007), cyber criminology refers to *"the study of causation of crimes that occur in the cyberspace and its impact in the physical space*." A group of scholars has taken the lead in advancing these interdisciplinary pursuits. It is this group of scholars who have the knowledge and expertise needed to further expand cybercrime research. Increased attention to social sciences in cybersecurity curricula is also demonstrated by a certain number of traditional STEM-programs that offer concentrations in cybersecurity, cybercrime, and digital forensics that include criminal justice courses.

Second, senior criminal justice faculty and program administrators should continue to be educated about the value of interdisciplinary pursuits. Departmental and disciplinary boundaries frequently keep criminal justice faculty from pursuing interdisciplinary efforts (Payne, 2016). Ironically, most interdisciplinary pursuits more accurately lead to solutions to complex problems that cannot be solved by a single discipline. Whether discussing cybersecurity – or some other interdisciplinary problem – it is important that criminal justice faculty become increasingly aware about the need for interdisciplinary efforts.

Third, criminal justice faculty are also encouraged to educate their peers across campus and administrators about the value of criminal justice. As a relatively new area of study, it is likely that criminal justice is not yet well understood by those working in STEM fields. This would potentially explain the low number of cybersecurity programs including criminal justice coursework. As was shown in the review of literature above, criminal justice has a great deal to offer to the study of cybersecurity. The task at hand is to demonstrate that value.

Fourth, cybercrime experts from criminal justice should also strive to increase awareness about criminal justice among federal officials and those responsible for developing NSA Center of Academic Excellence designations. As a growing area of study, "cyber criminology" has opportunities for integration into the NSA-CAE designation process. Becoming a part of this process would expand resources for cybercrime faculty, given them the academic credibility they deserve, and increase the value of criminal justice students' degrees.

Fifth, in a similar way, cyber criminologists are advised to expand awareness about NSA designation among criminal justice professors so they are better able to prepare courses that meet

the knowledge units required for designation as a Center of Academic Excellence. It is not enough for cyber criminologists to claim that our courses meet certain criteria without first developing coursework that target specific knowledge units. Currently, 27 of the 209 NSA designated programs include criminal justice coursework in the programs. While a low amount, this demonstrates that criminal justice coursework can have value in the NSA designation process.

Sixth, it is important to recognize that words matter in any interdisciplinary effort. For criminal justice and criminology scholars, the phrase "cybercrime" means a great deal. For STEM professionals, the preferred terminology appears to be cybersecurity. Efforts should be undertaken to identify similarities and differences between "cybercrime" and "cybersecurity" and, where feasible, it would be useful to develop a common lexicon in these interdisciplinary pursuits.

Finally, criminal justice scholars should promote the expansion of cybercrime and cybersecurity programming. From developing general education cybercrime classes to developing cybercrime majors and minors to developing certificates and degree programs, many opportunities exist for better connecting criminal justice and cybersecurity. The technological revolution changed the way crime is committed. It should also change the topics we study and teach about in criminal justice.

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

References

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

Boyd, A. (2016, February 4). DNI Clapper: Cyber bigger threat than terrorism. *Federal Times*. Retrieved from: https://www.federaltimes.com/management/2016/02/04/dni-clapper-cyber-bigger-threat-than-terrorism/.

Brenner, S. W. (2012). *Cybercrime and the law: Challenges, issues, and outcomes*. Boston: UPNE.

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

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

Cybersecurity Career Pathway (2017). Retrieved December 30, 2017, from http://cyberseek.org/pathway.html.

Donner, C. M., Marcum, C. D., Jennings, W. G., Higgins, G. E., & Banfield, J. (2014). Low self-control and cybercrime. *Computers in Human Behavior*, *34*, 165-172.

Freiburger, T., & Crane, J. S. (2008). A systematic examination of terrorist use of the Internet. *International Journal of Cybercriminology, 2*(1), 309-319.

Gunter, W. D., Higgins, G. E., & Gealt, R. E. (2010). Pirating youth: Examining the correlates of digital music piracy among adolescents. *International Journal of Cyber Criminology*, *4*(1/2), 657-671.

Hemmens, C. (2016). Teaching law and courts in criminal justice: Outside looking in. *Journal of Criminal Justice Education*, *27*(4), 497-508.

Hollinger, R. C., & Lanza-Kaduce, L. (1988). Process of criminalization: The case of computer crime laws. *Criminology, 26*(1), 101-126.

Holt, T. (2016, April 20). Introducing the International Interdisciplinary Research Consortium on Cybercrime (IIRCC). Retrieved December 29, 2017, from https://www.linkedin.com/pulse/introducing-international-interdisciplinary-research-consortium-holt.

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.

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

Losavio, M., Seigfried-Spellar, K. C., & Sloan III, J. J. (2016). Why digital forensics is not a profession and how it can become one. *Criminal Justice Studies*, *29*(2), 143-162.

Lynch, M. J., McGurrin, D., & Fenwick, M. (2004). Disappearing act: The representation of corporate crime research in criminological literature. *Journal of Criminal Justice*, *32*(5), 389-398.

Maimon, D., Kamerdze, A., Cukier, M., & Sobesto, B. (2013). Daily trends and origin of computer-focused crimes against a large university computer network. *British Journal of Criminology*, *53*(2), 319-343.

Marcum, C. D. (2009). *Adolescent online victimization: A test of routine activities theory*. El Paso: LFB Scholarly Pub.

Marcum, C. D., Higgins, G. E., & Tewksbury, R. (2011). Doing time for cyber crime: an examination of the correlates of sentence length in the united States. *International Journal of Cyber Criminology*, *5*(2), 825-835.

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.

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.

McGee, M. K. (2016, May 18). SEC chair: Cybersecurity is no. 1 risk. Retrieved December 30, 2017, from https://www.bankinfosecurity.com/sec-chair-cybersecurity-no-1-risk-a-9114.

McGurrin, D., Jarrell, M., Jahn, A., & Cochrane, B. (2013). White-collar crime representation in the criminological literature revisited, 2001-2010. *Western Criminology Review*, *14*(2), 3-20.

Moritz, B. & Burg, D. (2015, February 17). How corporate America can fight cybersecurity threats. *Fortune*. Retrieved from: http://tinyurl.com/jhfsxh5.

Morris, R. G., & Blackburn, A. G. (2009). Cracking the code: An empirical exploration of social learning theory and computer crime. *Journal of Crime and Justice*, *32*(1), 1-34.

Payne, B. K. (2016). Expanding the boundaries of criminal justice: emphasizing the "s" in the criminal justice science s through interdisciplinary efforts. *Justice Quarterly*, *33*(1), 1-20.

Pollitt, M. (2010). Pollitt, M. (2010, January). A history of digital forensics. In *IFIP International Conference on Digital Forensics* (pp. 3-15). Berlin, Heidelberg: Springer.

Rege, A. (2014). A criminological perspective on power grid cyber attacks. *Journal of Homeland Security and Emergency Management*, *11*(4), 463-487.

Reuters (2017, April 20). Fitch: Cyber risk is a growing threat to financial institutions. Retrieved December 30, 2017, from https://www.reuters.com/article/fitch-cyber-risk-is-a-growing-threat-to/fitch-cyber-risk-is-a-growing-threat-to-financial-institutions-idUSFit994598.

Shoemaker, D., Kohnke, A., & Sigler, K. (2016). *A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2.0).* Boca Raton: CRC Press.

Smallridge, J., & Roberts, J. (2013). Crime specific neutralizations: an empirical examination of four types of digital piracy. *International Journal of Cyber Criminology, 7*(2), 125-140.

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

Tappan, P. W. (1960). *Crime, justice and correction* (Vol. 10). New York: McGraw-Hill.

Udris, R. (2016). Cyber deviance among adolescents and the role of family, school, and neighborhood: A Cross-National Study. *International Journal of Cyber Criminology*, *10*(2), 127-146.

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: a test of routine activities Theory. *International Journal of Cyber Criminology*, *11*(1), 24-38.

Winn, C. (2017, September 24). Cybersecurity is now the biggest risk facing independent RIAs. Retrieved December 30, 2017, from http://www.cetusnews.com/business/Cybersecurity-Is-Now-the-Biggest-Risk-Facing-Independent-RIAs.HkeTEFQHsW.html.

Wright, J. P., Beaver, K. M., DeLisi, M., Vaughn, M. G., Boisvert, D., & Vaske, J. (2008). Lombroso's legacy: The miseducation of criminologists. *Journal of Criminal Justice Education*, *19*(3), 325-338.

Yang, S., & Rege, A. (2017). EAGER: Collaborative: A criminology-based simulation of dynamic adversarial behavior in cyberattacks. Retrieved December 30, 2017, from https://www.nsf.gov/awardsearch/showAward?AWD_ID=1742789&HistoricalAwards=false