2018

Cyber Security and Criminal Justice Programs in the United States: Exploring the Intersections

Brian K. Payne
Old Dominion University, bpayne@odu.edu

Lora Hadzhidimova
Old Dominion University

Original Publication Citation

Payne, B. K., & Hadzhidimova, L. (2018). Cyber security and criminal justice programs in the United States: Exploring the intersections. International Journal of Criminal Justice Sciences, 13(2), 385-404. doi:10.5281/zenodo.2657646

International Journal of Criminal Justice Sciences
Vol 13 Issue 2 July – December 2018

Cyber Security and Criminal Justice Programs in the United States: Exploring the Intersections

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

Abstract

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

Keywords: Cyber security, Cyber crime, 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, cyber crime, and cyber security 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).

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

The evolution of cyber crime 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 cyber security and criminal justice, while clear to criminologists, have not been empirically addressed. Better understanding of the connections between criminal justice and cyber security will help to strengthen our efforts to promote safer computing in all its forms.

Review of Literature

Cyber security has been described as the biggest threat facing financial institutions (McGee, 2016; Reuters, 2017), the federal government (Boyd, 2016), corporations (Moritz & Burg, 2015), and investors (Winn, 2017). It seems to be well accepted that cyber security is a growing threat that must be addressed. The response in higher education has been the development of cyber security academic programs, an increase in cyber security research, and the receipt of federal funds to support the expansion of cyber security 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 cyber crime, (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 cyber crime– 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). Cyber crime, then, would be illegal acts involving cyber technologies that are in violation of the criminal law, and so on. Another legal scholar writes that "cyber crime, 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 cyber crime) 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 cyber crime:

- *Defining cyber crime 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 cyber crime 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 cyber crime 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 cyber crime from a deviance perspective* would focus more on whether behaviors are defined as abnormal and less on legal prohibitions.
- *Defining cyber crime from a white-collar crime orientation* would focus on how certain types of cyber crimes are actually white-collar crimes (or crimes committed in the course of a legitimate occupation).
- *Defining cyber crime 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 cyber crime 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 cyber crime, many of their studies have focused on explaining cyber crime and cyber victimization. The most popular criminological explanations of cyber crime 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 cyber crime 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 cyber crimes).
- 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 cyber crimes and one research team has identified two neutralizations specific to certain types of cyber crime: (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 cyber crime 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 cyber crime. 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 cyber crime 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 cyber crime 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), cyber crime 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 cyber security (Yang & Rege, 2017). The implications from such research will be groundbreaking and will have direct implications for strategies to improve cyber security 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 cyber crime and victimization are flawed as well. Still, depending on the nature of the cyber crime 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 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 cyber security? With appropriate training, criminal justice graduates could potentially be prepared for some of the "softer" careers in cyber security. At the end of 2017, nearly 750,000 individuals in the United States worked in cyber security 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 require 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 Cyber security Education as one that "Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cyber security 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 cyber security/cyber crime 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 cyber crimes. 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 cyber security offenders, one group of criminal justice scholars explored how cyber crime 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 cyber crime 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 cyber crime and cyber security.

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).
- *Cyber crimes against property* include theft, cyber bank theft, theft of trade secrets, theft of services, various forms of fraud, extortion, and blackmail.
- *Cyber crimes 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 cyber crimes. "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 cyber security 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 cyber security curriculum rigorously addresses topics of value to the federal government's cyber security 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 cyber security 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 cyber security 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 cyber security as an interdisciplinary topic. Combining criminal justice with STEM is most certainly an interdisciplinary avenue. In addition, each of the designations includes 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 cyber security program's resources and prominence. In terms of resources, the designation opens up the amount of cyber security scholarship dollars that can be awarded to the institution and the faculty from the program becomes eligible for additional cyber security grants. In turn, it is

believed that those institutions with the designation will be more sought after by cyber security 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 cyber crime. Seizing on this opportunity, criminologist Thomas Holt recently led the development of the International Interdisciplinary Research Consortium on Cyber crime. In the announcement of this effort, Holt (2016) wrote, *"…we have to develop a holistic research agenda to combat cyber crime and improve cyber security 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 cyber security."* Demonstrating this commitment to an interdisciplinary approach to cyber security, Holt – at Michigan State University's School of Criminal Justice – has led an annual interdisciplinary cyber crime conference over the past five years.

While Holt and his colleagues have done a remarkable job in promoting the interdisciplinary nature of cyber crime, it is not clear the degree to which criminal justice (as an area of study) has embraced cyber security or the degree to which cyber security 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 cyber security embraced in criminal justice programs and by criminal justice scholars?; (2) To what degree is criminal justice embraced in cyber security 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 cyber security trends.

Methods

To answer these questions, we focused on the degree to which national criminal justice and criminology organizations in the United States embraced cyber security, the degree to which criminologists wrote about the topics, and intersections between cyber security 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 cyber security and criminal justice. The coding schedule included information on whether the institution had a cyber security 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 cyber security program (and the names of the classes), whether the institution offered cyber security courses in its criminal justice program (and the names of the classes), whether the cyber security program was public or private, whether the cyber security program was NSA designated, and the type of designation (if any) held by the institution's cyber security 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 cyber security 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 cyber security. These curricula were not considered parts of cyber security programs since the "cyber security" element was peripheral, not central for the instructional methodology of cyber security. An institution was listed as having cyber security program only if it had a name of the program that refers to the methods and goals of cyber security (such as "Digital Forensics" or "Cyber Criminology"). Institutions offering STEM-programs with a focus/concentration in cyber security or its variations were considered as having "cyber security" programs. Also worth mentioning is that some institutions had an NSA-designation for research but not a cyber security program. Lastly, others did not offer such program but had established instead student clubs and centers for cyber security as an extracurricular effort.

Findings

Table 1. Cyber crime, Cyber security, Computer Crime, and Internet Crime in Research Studies⋆

	Cyber crime	Cyber security	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.

Table 1 show how often cyber crime 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 "cyber security" in the article's title. Of those 495 articles, however, just 39 were published in academic journals. The vast majority of "cyber security" articles in criminal justice abstracts appear in magazines (n=406).

To determine whether cyber crime 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 cyber crime 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.

Table 2. Sample Characteristics (n=615)

	n	%
Institution has cyber security program	356	57.9
Institution has criminal justice program	531	86.5
Criminal justice courses in cyber security program	61	17.1★
Cyber security 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 cyber security and criminal justice programs respectively.

To further understand the connections between criminal justice and cyber security, 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 cyber security program (57.9%). Roughly two-thirds of the institutions were public institutions and the other third were private institutions. In all, 209 of the cyber security programs had been designated as NSA Centers of Academic Excellence, with the cyber defense designation for four-year programs being the most popular.

Regarding specific connections between criminal justice and cyber security, of the 531 criminal justice programs in the sample, just 16.2 percent of the programs (n=86) included cyber security coursework in the criminal justice curricula, with a handful of the criminal justice programs offering multiple cyber security courses. Table 3 shows the names of these courses. As shown in the table, cyber crime or its variations (cyber crime, cyber crimes, introduction to cyber crime) was the most popular cyber security 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 cyber security courses are included in the criminal justice programs. In fact, 123 different cyber security courses are offered in criminal justice programs.

Table 3. Cyber security Courses Taught in Criminal Justice Programs

Advanced Digital Forensics	Cyber Threats &Counterintelligence
Advanced Issues in Cyber crime	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 Cyber crime	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 Cyber crime
Criminology of Cyber crime	Fundamentals of Computer Crime.
Cyber crime (n=12)	Hardening the Enterprise Network
Cyber crimes	Incident Response & Network Forensics
Cyber crime I: Legal Issues/Investigative Procedures	Information Assurance Risk and Compliance
	Information Security
Cyber crime II: Internet Vulnerabilities and Criminal Investigation	Information System Threats, Attacks and Defenses
	Information Security and Assurance
Cyber crime and Digital Terrorism	Administration
Cyber crime Capstone	Information Warfare and Security
Cyber Crime and Computer Forensics	Investigating Online Crimes
Cyber crime and Cyber security	Insider Threat
Cyber crime and Forensics	Interdisciplinary Topics in Cyber security
Cyber crime and the Law	Internet Vulnerability Criminal Act

Cyber crime Investigation	Introduction to Computer Forensics (n=2)
Cyber crime Law and Investigations	Introduction to Cyber crime (n=7)
Cyber crime, Technology, and Social Change	Introduction to Cyber Crime and Computer Security
Cyber and Surveillance Law and Governance	Introduction to Cyber Security
Cyber Crime (n=10)	Intro to Cyber Security for Criminal Justice
Cyber Crimes (n=2)	Investigation of Computer Crime
Cyber-Crime and Cyber-Security	Investigation of Cyber Crime
Cyber Crime-Criminal and Civil Investigation	Issues in Cyber crime
Cyber Crime, Ethics, and Law	Large Scale Cyber crime and Terrorism
Cyber Crime and Security	Malware Basics
Cyber Crime, Security and the Law	Mobile Device Forensics
Cyber Criminals and Computer Forensics	Mobile Forensics
Cyber Criminology	Network Forensics and Incident Response
Cybercriminology	Network Forensics
Cyber Ethics and Internet Culture	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 Cyber crime	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
Cyber security	Security Systems
Cyber Security I	Seminar in Cyber crime
Cyber Security II	Seminar in Cyber crime Investigations
Cyber security and Loss Prevention/Exercise Data	Seminar in Cyber crime Law and Policy
Cyber security and Loss Prevention	Seminar in Cyber Security
Cyber security and Policy	Seminar in Cyber Warfare
Cyber security: Law & Ethics	Social Media & Cloud Security
Cyber Security/Law/Money Launder	Software Foundations for Cyber security
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 cyber security programs when reviewing the criminal justice courses offered in cyber security programs. Namely, a wide range of criminal justice courses are offered in the cyber security programs. Of the 356 cyber security 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 cyber security programs. Introduction to Criminal Justice (n=17) and Criminal Law (n=10) were the most popular criminal justice courses offered in cyber security programs. In all, 152 different criminal justice courses are offered in cyber security programs.

Table 4. Criminal Justice Courses taught in Cyber Security 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)

Cyber Crime(s) (4)	Evidence
Cyber Criminal & Civil Investigations	Firewall & Security Ent Comp
Cyber Criminology	First Responder Tools and Application
Cyber Ethics and Internet Culture	Forensic Designations (CCE/ACE)
Cyber Forensics (2)	Forensics and Crime Scene Investigation
Cyber Law and Cyber crime	Fraud
Cyber Security	Professional Writing in Criminal Justice
Cyber Security I	Public and Private Security
Cyber Security Senior Seminar	Readings in Cyber Crime
Cyber Threats and Counterintelligence	Risk Assessment and Fraud
Cyber crime and Cyber security	Risk Assessment and Prevention (5)
Cyber crime and Forensics	Rules of Evidence/Legal Aspects of Cyber Security
Cyber crime and the Law	Security of Information and Technology
Cyber crime Investigation	Seminar in Criminal Justice
Cyber crime, Technology, and Social Change (5)	Social Media and Cloud Security
Cybercriminology	Special Topics in Criminal Investigations in Cyber security
Cyber security and Loss Prevention	Special Topics in Criminal Justice
Cyber security and Loss Prevention/Exercise Data	Special Topics in Cyber Security
Cyber security: 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

Tests were conducted to determine whether presence of criminal justice courses in a cyber security 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, cyber security 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 cyber security curricula, 27 (44.3%) were NSA designated programs. In contrast, among the programs that did not have criminal justice courses in a cyber security 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.

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≤.05, p≤.01

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 cyber security program. Of the 193 private institutions, 101 (52%) offered a cyber security program (Chi Square = 3.56, $p < .05$). Second, public institutions were more likely to be NSA designated. Of the 255 public institutions with cyber security programs, 62% (n=158) had an NSA designation. In comparison, of the 101 private institutions, roughly half (50.5%) were NSA-designated programs (Chi Square = 3.92, $p < .05$). Third, private institutions were more likely to have criminal justice courses in their cyber security program. Nearly one-fourth of the private institutions (n=24) offered criminal justice coursework in their cyber security program. In comparison, less than 15% (37/218) of the public institutions offered criminal justice coursework in their cyber security major (Chi Square = 4.36, $p < .05$).

These findings should be interpreted with some caution. Using course catalogues to identify cyber security 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 cyber security differently. Despite these limitations, these findings lead to some interesting conclusions that provide fodder for future discussion.

Discussion and Conclusion

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

by practical recommendations aimed at expanding the role of criminal justice in cyber security.

Six possible reasons explain why criminal justice programs have not more fully embraced cyber security offerings. First, the topic of cyber security may not be appealing to program administrators. The very label of "cyber security" and "cyber crime" 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. Cyber security – at its core – may require more of an applied focus than traditional sociologists are willing to embrace.

Third, because cyber security 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 cyber security is simply about computers and engineering, when in fact, the human element is central to cyber security.

Fourth, and somewhat related, it should not be surprising that criminal justice scholars are not fully aware of cyber security given that cyber crime is so rarely included as coursework in criminal justice doctoral programs. Our review found very few cyber crime 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 cyber security 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 cyber crime 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 cyber crime.

Despite this dim assessment of the state of criminal justice programing and scholarship in the area of cyber security, avenues for better connecting criminal justice and cyber security exist. First, and foremost, cyber crime scholars should expand on the foundational successes they have already enjoyed. The International Interdisciplinary Research Consortium on Cyber crime noted above is one example of a great start to promoting interdisciplinary cyber crime efforts. In addition, fruitful endeavors such as the branding of an area of study as "cyber criminology" should be embraced. Coined and founded by Jaishankar (2007), cyber criminology is the academic discipline that refers to "*the study of causation of crimes that occur in the cyberspace and its impact in the physical space*." To further the discipline, Jaishankar (2007) founded the first journal of this field, the International Journal of Cyber Criminology (www.cybercrimejournal.com). Also, a group of scholars have

taken the lead in advancing these interdisciplinary pursuits. It is this group of scholars who have the knowledge and expertise needed to further expand cyber crime research. Increased attention to social sciences in cyber security curricula is also demonstrated by a certain number of traditional STEM-programs that offer concentrations in cyber security, cyber crime, 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 cyber security – 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 is 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 cyber security 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 cyber security. The task at hand is to demonstrate that value.

Fourth, cyber crime 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 cyber crime 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 "cyber crime" means a great deal. For STEM professionals, the preferred terminology appears to be cyber security. Efforts should be undertaken to identify similarities and differences between "cyber crime" and "cyber security" 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 cyber crime and cyber security programming. From developing general education cyber crime classes to developing cyber crime majors and minors to developing certificates and degree programs, many opportunities exist for better connecting criminal justice and cyber security. 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). *Cyber crime 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.

Cyber security Career Pathway (2017). Retrieved, 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 cyber crime. *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 Cyber Criminology, 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 Cyber crime (IIRCC). Retrieved 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: Cyber security is no. 1 risk. Retrieved from https://www.bankinfosecurity.com/sec-chair-cyber security-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 cyber security 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, 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 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 Cyber security Education (NICE) Cyber security 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). Cyber security is now the biggest risk facing independent RIAs. Retrieved from http://www.cetusnews.com/business/Cyber security-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 cyber attacks. Retrieved from https://www.nsf.gov/awardsearch/showAward?AWD_ID=1742789&HistoricalAwards=false.