DESIGNING THE CURRICULUM FOR A MINOR IN CYBER CRIMINOLOGY

Rajesh Prasad and Liana Pennington
Saint Anselm College, rprasad, lpennington@anselm.edu

Abstract - **We are living in an age of growing cyber crime and the costs associated with it. With more and more people and devices being connected through the Internet, there are plenty of opportunities for new kinds of criminal activity as the Internet provides cyber criminals with anonymity and global reach. According to the FBI, in 2018 the Internet Crime Compliant Center (IC3) [1] received 351,936 complaints with total losses exceeding $2.7 billion. The threat of cyber crime is real and pertinent when the Internet is intertwined with our everyday lives. We must prepare today's undergraduate students, tomorrow's future workforce, to fight this growing threat of cyber crime. If we do not prepare today, we will be vulnerable tomorrow. This paper details our experiences in developing and implementing an interdisciplinary minor in Cyber Criminology. The minor is designed for students who are interested in learning about cyber crime from the dual perspectives of computer science and criminal justice.**

Index Terms – Cyber Criminology, Cyber Security, Interdisciplinary Curriculum, Internet Crime.

INTRODUCTION AND MOTIVATION

The widespread use of technology and the Internet in today's society has made examining, investigating, and prosecuting cyber crime an essential priority. Wired and wireless Internet has become ubiquitous in today's digital age as the last decade has seen a surge in the use of Internet-based applications. Global citizens use their smart phones, computers and hand held devices to shop, socialize, communicate, entertain, store information and complete financial transactions. The Internet is intertwined with our daily lives. Five social networking sites (Facebook, YouTube, WhatsApp, WeChat, and Instagram) each have over a billion active users. [2] In addition, the integration of the Internet of Things (IoT) into our daily lives has led to an explosion of interconnected devices. As our lives become more interconnected through wearable and smart home devices, as a society we become even more vulnerable to exploitation by cyber criminals.

Cyber crime differs from traditional crime in a number of important ways. Cyber criminals do not have to be physically present at the scene of the crime. Instead, perpetrators can be located anywhere in the world with an Internet connection to commit a cyber crime. The global nature of cyber crime has important implications for investigation and prosecution, particularly as international cyber criminals increasingly target governments, infrastructure, financial institutions, and e-commerce websites to commit fraud, disruptive activities and terrorism. Even at an individual level, no person's personal and sensitive information is safe if kept on a digital device.

Upon this backdrop of the changing face of crime, we propose an interdisciplinary minor in Cyber Criminology to better prepare the future workforce to properly deal with these growing threats. Jaishankar defines Cyber Criminology as *"the study of causation of crimes that occur in the cyberspace and its impact in the physical space"*. [3] Our undergraduate minor in Cyber Criminology combines coursework in Computer Science and Criminal Justice to equip undergraduate students with the necessary tools to address these new crimes.

Cyber security is the new buzzword. Everyone is talking about the need to secure our computer systems, including the networks used by the federal government, financial institutions and corporations. To address this concern, many educational institutions have started to include studies in cyber security in their academic programs. However, a focus on cyber security alone is not sufficient to address the growing problem of cyber crime and system intrusion. Thomas Holt, an influential academic researcher in this area, wrote, *"[W]e 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."* [4]

This interdisciplinary nature of the Cyber Criminology minor takes a different focus than other programs focusing on cyber security. While cyber security programs typically focus on training students to design and build secure systems and networks, cyber criminology addresses what needs to be done after a network is breached or data is stolen. The field of cyber security includes at least four important aspects:

1. to protect and defend a computer system or a network of connected devices;
2. to detect if a computer system or network is breached;
3. to collect and analyze digital evidence of a cyber-crime in legally admissible ways; and
4. to present the digital evidence in a court of law according to new emerging laws and government policies.

While many cyber security curricula focus on aspects 1 and 2 above, there are very few curricula which prepare students

978-1-7281-7520-1/20/$31.00 ©2020 IEEE

concerning what to do after a crime has been committed. We focused on the 3rd and 4th aspects to develop an inter disciplinary minor in cyber criminology. In addition, our cyber criminology curriculum includes the study of the reasons underlying the commission of different cyber crimes in the hope of developing innovative ways of preventing and reducing incidents of cyber crime. The target audience for this minor are students who are interested in the interdisciplinary area of Computer Science and Criminal Justice.

An interdisciplinary focus ensures that students gain analytical and critical thinking skills as well as a solid foundation in computing. Students in the Cyber Criminology minor explore what it means to be a citizen in today's controversies involving privacy, security and technology. In these ways the Cyber Criminology minor encourages students to think critically concerning the myriad of ways new technology intersects with the rule of law. We hope that having this minor will equip students to become leaders in this emerging field of fighting crime.

The Threat of Cyber Crime And The Cyber Criminology Minor

Cyber crime is often defined as any crime utilizing a digital device or a network. *"Conceptualizing cyber-crime involves a number of key elements and questions that include where do the criminal acts exist in the real and digital worlds (and what technologies are involved in carrying out the crimes), why are malicious activities initiated, and who is involved in carrying out the malicious acts?"* [5] Cyber crime is one of the greatest threats facing the United States and its growth has enormous implications on national security, economic prosperity, and public safety. [6] Cyber threats are becoming more commonplace, more dangerous, and more sophisticated. The ubiquity of Internet-connected digital devices in the 21st century has led to an increase in computer-related crimes. Hacking, identity theft, malware, cyber harassment and online child exploitation pose an expanding threat. Cyber crimes can offer a large extrinsic reward, such as monetary profit, for these entities. No matter how much we secure a network, it will be breached. In addition, the online environment provides for higher level of anonymity, making apprehension and prosecution difficult for the criminal justice system. The future workforce not only must be ready to ensure the protection and defense of cyberspace, but also should be equipped with the theoretical knowledge and software/hardware tools to understand and investigate a cyber crime and take it to a court of law.

Cyber Criminology is the interdisciplinary study of cyber crime, including the responses to cyber crime in the criminal justice system, the legal and political controversies involving cyber crime, and the technical challenges to investigating and prosecuting cyber crime. Even if they themselves are not prosecuting the case, members of this future workforce must be able to understand the legal system to be able to work within the confines of the law and to assist the prosecutor. A curriculum in the interdisciplinary field of Cyber Criminology is necessary to prepare such a workforce. The study of cyber criminology will equip students with the knowledge and skills required to understand criminal behavior on the Internet and train them to combat financial and non-financial cyber crimes such as money laundering, digital piracy, ransomware, distributing illicit drugs, sex trafficking, cyber bullying, theft and cyber terrorism. We envision a minor in Cyber Criminology with five courses; each course is worth four credits:

1. An introductory course in Cyber Criminology
2. An introductory course in Computing
3. Computer Forensics
4. Cyber Law and Policy
5. Computer Networks and Security

Let us look briefly at each of the educational components in cyber criminology:

Introduction To Cyber Criminology

This is the introductory course in this minor to expand the students' knowledge from both a criminological and a computer science perspective governing cybercrime. This course is team-taught with one professor from Computer Science and one professor from Criminal Justice to provide complementary perspectives. A typical course offered at another institution primarily focuses on one perspective, while this team-taught course grants students the opportunity to explore how these two different disciplines can come together to explore an interdisciplinary issue.

This course traces the history, definitions and typologies of computer networks and many different type of cyber crime, examining the motivations of cyber crime offenders and the characteristics of cyber crime victims. The course discusses both financial and non-financial cyber crimes and the role of different law enforcement offices.

The students examine the most common types of cyber crime, including fraud, hacking, identity theft, scamming, malware, ransomware, botnets, Distributed Denial of Service (DDoS) attacks, spamming, phishing, social engineering, cyber stalking, cyber bullying and sex crimes. The coursework also prepares students to avoid falling victim to cyber crime. Through course readings and class discussions relating to recent cyber crime related events in the news, the course exposes students to how the criminal justice system investigates and prosecutes various cyber crimes. Special focus is paid to network-connected digital devices and how to recognize network-related crimes through hands-on activities. In this course, we try to bring in guest lecturers who provide real-world lessons on cybercrime. This course also fulfills a college general curriculum requirement in the Social Sciences.

Computing I

Computers or computer-like devices (smart phones, tablets, etc.) are essential to cyber crime. In any cyber crime, the computer or computer-like devices are either the target of a crime, the instrument of a crime or incidental to the crime. It is important that students in this minor understand basic computing principles and fundamental concepts of how computers work. The Computing I course at our college is an introductory course that teaches the essential ideas of Computing and gives the students a broad overview to the field of Computer Science. The course also provides a general background on hardware, software and the Internet. The course has no prerequisite and no previous experience is required. This course teaches students how to think logically and solve problems efficiently. It also develops computational thinking skills in students, which is vital for success across all disciplines.

In Computing I, students are introduced to the general concepts and techniques of computer programming. Students learn their first programming language, Python. Python is used as the first programming language because it is easy to learn compared to stricter programming languages like Java or C++. Python is one of the most powerful and widely used programming languages in the world. One of the reasons for its popularity is its rich set of libraries and frameworks, which allows one to easily write utility scripts. The programming language fits into the minor as scripts are widely used by law enforcement and corporate enterprises to extract useful data from raw data. This course also fulfills a college general curriculum requirement in Quantitative Reasoning.

COMPUTER FORENSICS

Students also learn how to investigate cyber crimes and to preserve important digital evidence through a Computer Forensics course. "*Computer forensics is defined as the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law*." [7] In computer forensics, students learn the basic knowledge and skills to acquire, secure, recover, validate and analyze digital information for use in criminal and civil investigations. The digital information needs to be delivered in a time sensitive, critical, concise, neutral and thoughtful manner. The digital forensic course structure and content introduce students to the tools and techniques of computer and smart phone forensics investigations. The course allows students to experience searching for scientific-driven and data-driven evidence within the confines of the law. Students are able to do forensic data analysis with real data and hands-on exercises with software similar to programs used by law enforcement officers (ex. Blacklight). The final class project allows students to analyze large amount of digital evidence and identify the most significant data.

The interdisciplinary perspective gained by the Cyber Criminology minor helps the cyber forensics investigator understand the motivation of cyber criminals to better follow their online digital footprints. Students in this course develop critical thinking and problem solving techniques, which are essential for success in any career. The students also learn the concept of preserving the chain of evidence and writing a report on their findings from the digital forensic investigation. This course also fulfills a college requirement in Writing.

CYBER LAW AND POLICY

The course sequence in the minor also includes a course in cyber law and policy which examines how the criminal justice system investigates and prosecutes various cyber crimes at the national and international levels. This course focuses on how laws relating to cyber crime are conceptualized, enforced and prosecuted. Technology, and the social and cultural changes it has brought about, challenges the traditional approaches to criminal law and procedure in many ways. Laws evolve slowly and struggle to keep up with these rapid changes. Sometimes it makes sense to extend existing legal concepts to new cyber-related problems, but often old legal concepts do not map well to a new cyber environment.

This course examines cyber crime from a law and policy perspective, including its impact on Fourth and Fifth Amendment jurisprudence and the changing conceptions of privacy and identity. The field of cyber law and policy is still in its infancy in many ways. New legislation and policies are often introduced only after an cyber crime incident has taken place, with the law constantly racing to catch up to the frantic pace of emerging technology. Since the online environment provides for a higher level of anonymity, apprehension and prosecution are particularly difficult with cyber crimes. In addition, cyber crime is a worldwide phenomenon, providing a rich environment for criminal activity ranging from identity theft to malware infections. Often it is unclear which laws apply to cases involving parties in different jurisdictions or whether a cross-border law enforcement partnership is necessary or feasible. This course also fulfills a college general curriculum requirement in Citizenship.

COMPUTER NETWORKS AND SECURITY

Cyber crime is criminal activity carried out by means of computers or the Internet. The Internet is a global network of networks. Hence, the study of cyber criminology must include a study of computer networks, both wired and wireless. The course focuses on the structure, topology and a basic theoretical understanding of computer networking. The students become familiar with hardware, software and services that comprise an enterprise network. Students gain a general understanding of the TCP/IP stack in Internet and network communication protocols. The students also learn common application layer protocols and network services used in Internet and web communication. The syllabus also includes the basic principles and hands-on exercises on how security is implemented on a computer or in a network setting.

These topics give students a solid foundation in networks to help them understand and investigate cyber crimes. A deep understanding of computer networks and how the network protocol works will help a cyber crime investigator to retrace steps in the process of detecting crime and gathering evidence. For example, in most cyber crimes the first step is finding the Internet Protocol (IP) address and Medium Access Control (MAC) address. The IP address leads to the geolocation and Internet Service Provider (ISP) and the MAC address leads to the actual device used by the cyber criminal.

Even though only the fundamentals of network security like firewall, Network Address Translation (NAT), encryption, wireless security, the need for anti-virus software, intrusion detection and prevention are covered in this course, understanding this area aids students in strengthening their networks against cyber crime.

SUCCESS OF THE MINOR AND PLANS FOR A NEW MAJOR IN CYBER CRIMINOLOGY

We have had success designing and implementing this new minor in Cyber Criminology at a small Catholic liberal arts school in the Northeast. Very few colleges nationwide have Cyber Criminology or similar minors and majors. Jaishankar finds only three schools nationwide which offer minors in Cyber Criminology or Cyber Crime. [8] At least two of these programs, the minors at The University of Alabama and Georgia Southern University, are situated in the Criminal Justice department rather than a result of a full interdisciplinary effort between Computer Science and Criminal Justice. Additionally, at least one other school, John Jay College of Criminal Justice, offers a minor in Cyber Criminology.

Since its introduction in Spring 2018, we have enrolled 36 students in the minor. The minor has attracted new students each year since its inception. The gateway course, Introduction to Cyber Criminology, has reached full enrolment with a waiting list for the past three semesters it has been offered. One benefit of the Cyber Criminology minor has been that students in the Criminal Justice program, a very popular major at the College, are now enrolling in Computer Science courses that they would not likely have enrolled in otherwise.

An important component of the minor's success is the integration of a number of different teaching practices with a focus on active learning. The team-taught gateway course, Introduction to Cyber Criminology, includes many small group exercises and real-life examples from the news as well as hands-on computer activities. Computing I includes a weekly lab where students learn computer programming. The Computer Forensics course includes simulated forensic analysis so that students can build real skills relating to what work on a real case would look like. In Cyber Law and Policy, students engage in a month long moot court simulation where students take on the role of either a prosecutor or defense attorney and argue in front of a panel of lawyers from the community acting as judges. Each of these teaching methods, in both computer science and criminal justice courses, have the objective of keeping students energized and to reach students with different learning styles. The hands-on training also leads to students' development of important new skills for the workplace.

Due to the success of the minor, we are in the process of finalizing a new major in Cyber Criminology in response to student interest. We surveyed some of our currently enrolled and recently graduated minors (N=18) concerning their potential interest in this new major. Students were asked if they would have taken/been interested in the Cyber Criminology major if it were offered when the student joined the college as a freshman. 88.89% of responding students (16) said Yes. 100.00% (18) of the responding students said that they would be interested in enrolling in a double major in Cyber Criminology if it were possible.

We hope to start enrolling students in this new Cyber Criminology major in Fall 2020. The major will include the five courses in the minor as well as four additional Criminal Justice courses (Introduction to Criminal Justice, Research Methods, Law Enforcement in the Digital Age, and Cyber Criminology Senior Seminar) and two additional Computer Science courses (Information Security and a Computer Science elective). The new major will allow students to develop additional depth of skills and knowledge in preventing, investigating and prosecuting cyber crime.

THE IMPORTANCE OF INCREASING CYBER CRIME AWARENESS TO PREPARE THE FUTURE WORKFORCE

An undergraduate program in Cyber Criminology helps to prepare students to combat this growing threat of cyber crime. There is an urgent need for academic and workforce development in the area of cyber crime. Workplaces face a crucial lack of college graduates who are able to design and build secure systems. In addition, there is a lack of adequate numbers of professionals to investigate and prosecute cyber crime when it is occurs. More attention is needed to understand how and why cyber crime occurs and how it differs from traditional crime in order to effectively develop new paths of prevention and intervention. This is an area of study that has seen tremendous growth recently and the demand for new experts with a background in both the criminal justice and computer science fields is only expected to increase. [8]

The integration of social science and computer science is the most distinctive feature of the interdisciplinary minor in Cyber Criminology. By incorporating social science based criminal justice coursework, students gain an appreciation of the complex social processes and structures involved in crime prevention, detection and prosecution. As a social science, criminal justice courses rely on evidence-based practices and the empirical testing of social theories. Students with a deep understanding of why crime occurs through the study of different criminological theories are better equipped to develop new technological means to prevent cyber crimes from happening. Similarly, students with an understanding of crime typologies or different types of crime will be more likely to effectively investigate cyber crime through various computer forensic means. Cyber crime is at its essence a social problem that will continue to have serious societal effects, even though it is committed through means of a computer. With the study of cyber crimes still being in its infancy, it is important that social scientific analysis continues to examine cyber crime and that social science informs various technological practices.

In addition, the interdisciplinary study of cyber crime addresses conceptual gaps that exist in many computer security curricula. A common perception is that if individuals and organizations protect their network they would be safe from outside threats such as viruses, worms, hacking and ransomware. In fact, depending on the size and nature of the business, companies spend thousands to millions of dollars to protect their network against external threats. Yet, no matter how strong the network defenses, there is always a chance of a network breach and a cyber crime occurrence. Cyber crime can take place from within the network firewall too. The Verizon 2019 Data Breach Investigations report says that 34% of all breaches in 2018 were caused by insiders. [9] These insider threats, often rogue employees gaining unauthorized access to privileged information, are particularly hard to detect. One effective strategy to prevent internal threats is to educate an ethical workforce. However, because of resource constraints or lack of time, cyber ethics and issues concerning cyber crime are rarely taught at colleges and universities. Yet workforce professionals will face a number of complex ethical decisions when working with sensitive data or sharing privileged information or granting access control. We advocate that cyber ethics should be integrated across multiple courses and taught using real world examples and class discussion because the future workforce will be handling sensitive data and information in their professional life and should be able to make moral decisions. A curriculum in Cyber Criminology that integrates the study of criminal justice along with computer science prepares students to address these complicated ethical issues.

Furthermore, the study of cyber criminology encourages students to think deeply about issues concerning what it means to be a citizen in the digital age. The investigation and prosecution of cyber crimes involves important debates concerning the right balance between the state's interest in public safety against the individual's interest in liberty and freedom from governmental intrusion. The interdisciplinary approach to studying cyber crime has students thinking critically about the intersection of new technology and the rule of law. Encouraging students to gain an understanding of cyber crime from both a computer science and a criminal justice perspective helps students understand the changing conceptions of privacy and identity relating to our close connections to technology and encourages students to become engaged and thoughtful citizens in a rapidly changing world.

CONCLUSION

Cyber crime is a growing threat. New curricula which combine a computer science and criminal justice perspective are needed to adequately address this threat. We introduce the Cyber Criminology minor so that we can build a workforce ready to address this rapidly expanding problem of cyber crime.

The interdisciplinary Cyber Criminology minor gives students an overview of federal and state laws and criminal activity identification and prosecution relating to cyber crime. The students in this minor will learn trends in cyber crime and the theoretical and practical skills that will prepare them to play an important role in the criminal investigation of computer crimes. Students learn methods for identifying, collecting and analyzing digital devices and data related to cyber crime investigations. The minor focuses on challenges faced by intelligence, homeland security, law enforcement and private organizations, including cyber crime countermeasures, cyber terrorism, cyber stalking and cyber bullying. The Cyber Criminology minor attracts students from other majors, particularly Criminal Justice, who likely would not otherwise take courses in the Computer Science Department.

REFERENCES

[1] https://pdf.ic3.gov/2018_IC3Report.pdf.

[2] https://ourworldindata.org/rise-of-social-media.

[3] Jaishankar K., "Cyber criminology: Evolving a novel discipline with a new journalt", International Journal of Cyber Criminology, Vol 1, Issue 1, pp. 1-6, 2007.

[4] https://www.linkedin.com/pulse/introducing-international-interdisciplinary -research-consortium-holt

[5] https://www.justice.gov/usao-vt/cybercrime.

[6] https://www.fbi.gov/investigate/cyber.

[7] https://www.us- cert.gov/sites/default/ files/publications/ forensics.pdf.

[8] Jaishankar K., "Cyber Criminology as an Academic Discipline: History, Contribution and Impact", International Journal of Cyber Criminology, Vol 12, Issue 1, pp. 1-8, 2018.

[9] https://www.ekransystem.com/en/blog/insider-threat-statistics-facts-and-figures.

.

AUTHOR INFORMATION

Rajesh Prasad, Associate Professor, Department of Computer Science, Saint Anselm College.

Liana Pennington, JD, PhD, Assistant Professor, Department of Criminal Justice, Saint Anselm College

.