Cyber criminology, Criminology and Cybercrime: Towards an Academic Discipline

Dr. Gregory Laidlaw

and

Charles E. Wilson, J.D.

University of Detroit Mercy

Center for Cyber Security and Intelligence Studies

Cyber Criminology: Towards an Academic Discipline and Cybersecurity Profession

Abstract

Cybercrime is a growing global phenomenon that has created a significant paradigm shift in critical areas of the personal life of citizens, and in both the public and private sectors. The negative impact of cybercrime is felt in many diverse areas, such as politics, economics, national security, public safety, and in many critical societal activities related to quality of life. Today, essential online functions are constantly under attack by a growing cadre of sophisticated cybercriminals, organized crime organizations, and nation-state actors. The purpose of this paper is to synthesize current research literature on cybercrime to highlight the scope of the problem; and to suggest a notional concept of criminological theories that can be applied to enhance cybercrime investigation and enforcement efforts. Additionally, the paper proposes the establishment of an academic minor "Cyber criminology" based on an interdisciplinary approach.

Keywords: cybercrime, criminological theories, cyber criminology, and interdisciplinary approach

Introduction

This paper focuses on identifying the nature of the individuals who are motivated to commit cybercrimes. We will examine who is involved in cybercriminal activity, why are they drawn to commit this particular form of crime, and how we can effectively reduce criminal behavior in cyberspace. We will present an overview of the issue, identify and define key terms and concepts, including selective criminological theories (Routine Activity Theory and Social Learning Theory) currently used to address criminal behaviors. We will also state the limitations of the criminological approach and describe emerging theories of cybercriminal behavior, namely, spatial transition theory (Jaishankar, 2007) and victim precipitation theory (Maras, 2017), and examine them in the context of combating cybercrimes. Finally, we will recommend the establishment of an academic minor "Cyber criminology" and describe an interdisciplinary educational program, in the form of an academic minor that can be used to enhance the students' education. Additionally, the minor program will complement the students' scholarship gained in their major area of study and/or expand their knowledge in an unrelated area of academic interest.

Historically, criminologists have focused on traditional forms of crime; however, over the past few decades, crime has moved to the Internet, opening the door to new types of crime and deviancy, as well as new methods of engaging in crime. This section briefly describes how Twenty-first century criminals increasingly employ selective criminal techniques facilitated by the Internet, maximized by the advancements in communication and computer technology, to further their criminal operations (Finklea and Theohary, 2015). The purpose of the paper is to advance the knowledge and promote scholarly dialogue and research on the convergence of cybercrime, criminology, criminal justice, and cybersecurity across the cyber landscape

Overview

There is clear and convincing evidence of an increasing frequency, mounting financial cost, evolving technical sophistication, and escalating harm emanating from serious cybercrime. A data breach at Equifax exposed the personal information of over 145 million Americans and Yahoo suffered a cyber intrusion that affected an estimated one (1) billion user accounts. Cybersecurity experts suggest that the information gained from these cyber-attacks will eventually be used by cyber criminals. According to O' Driscoll (2018), citing a Statista report, cybercrime accounted for $1.33 billion dollars in damages in 2016 in the United States alone. In the 2007 cyber-attack on TJX, the parent company of T.J. Maxx and Marshall retailers in America and Europe, hackers stole the personal identifiable information (PII) of over ninety-four million customers, according to Goodman (2015). Also, in 2007, the General Accountability Office (GAO) reported that all sectors in the U.S. face numerous challenges in their efforts to secure and protect cyberspace. The GAO report noted that the challenges exist in both the operational security and law enforcement arenas. Overall those individuals and entities responsible for security, protection, and enforcement operations in cyberspace have a difficult time detecting or responding to cybercrime. The GAO stated there is a deficiency in the

capability of law enforcement to effectively address the existing or emerging cybercrime challenges. The combination of the virtual and borderless environment of cyberspace makes it almost impossible for law enforcement to prevent, deter, or apprehend those who break laws in cyberspace.

Because of these types of cyber-attacks and other similar events, there is a growing need for an innovative approach to address the significant cyber threats facing the United States and international community. This paper proposes the adoption of an emerging academic and social science concept, “cyber criminology” which is derived from criminological theories used in the study of traditional criminal offending and applies them to cybercrime. Cyber criminology is a multidisciplinary field that encompasses practices from multiple fields such as criminology, victimology, sociology, information assurance, and computer information systems (Jaishankar, 2007). Cyber criminology focuses on why individuals commit cybercrimes and why they engage in certain criminal behavior in cyberspace. By understanding why, a person commits a crime, we can develop ways to better address cybercrime threats and recognize the criminal modus operandi most likely to be used in the perpetration of cybercrime activity. Specifically, this paper proposes that to be more successful in the fight against the escalating cybercrime threat, cyber criminology be established as an academic topic and offered as a minor for students enrolled in other disciplines as their major program of study. This academic adaptation will be the inaugural and foundational component for the eventual evolution and promotion of cyber criminology as an academic discipline and criminal justice and cybersecurity profession.

Key Terms

Cybercrime: The United Nations Office on Drugs and Crime (2005) defines cybercrime as conduct that entails criminal acts against the confidentiality, integrity and availability of computer data or systems represent the core of cybercrime. Other definitions include a wide range of activities, but these can generally be broken into two categories: (1) crimes that target computer networks or devices; and (2) crimes that use computer networks to advance other criminal activities.

Cyber criminology: "the study of causation of crimes that occur in the cyberspace and its impact in the physical space" (Jaishankar, 2007, p. 1).

Routine Activity Theory: Cohen and Felson (1979) originally held criminal activity is a crime of opportunity committed by a motivated offender against a suitable target under an unguarded condition.

Applying Criminological Theories

The paradigm shift in the nature, methods, and severity of cybercrime has created an urgent need for us to change our responses and capabilities in controlling cybercrime. The increased employment of computers and information networks has created an attractive attack surface for cybercriminals. Cybercrime continues to be an enormous national and international problem,

threatening both public and private sector entities, and individual citizens worldwide. According to Samenow (2014) human nature and the criminal mind does not change. However, the constant changes in society, such as globalization, technology, and the Internet, provide new venues and targets for the criminally inclined to employ fresh techniques and innovative methods. Therefore, it is important to understand the criminological aspects of the cybercrime phenomenon, so we can develop a better understanding of key characteristics about human behavior in cyberspace. The enhanced knowledge will aid in the crafting of theoretical and practical solutions. Moreover, it can lead to the development of effective prevention tactics and improved investigative techniques and response procedures.

An accepted and generalized premise of crime is that it follows opportunity. Therefore reduction of opportunity is a fundamental principle of crime prevention (Grabosky and Smith, 2009). Criminology is focused on developing an understanding of criminal behavior and the causation crime (Peak and Madensen, 2018). As a theoretical approach, criminology is derived from the discipline of sociology and entails the scientific study of the nature, extent, management, causes, control, consequences, and prevention of criminal behavior (Deflem, 2006). Although cybercrime research is relatively new to criminology, this area of research is gaining momentum (Valentine, Hay, Beaver and Blomberg, 2013). Each new advance in digital technology and every new software application will create an opportunity that criminals will seek to exploit (Grabosky, 2016). It is extremely important for law enforcement and cybersecurity practitioners to keep abreast of cybercrime developments and track the evolution of cybercriminals' behaviors, motivations and forms that these criminal activities take. There is an enormous need to develop more effective and efficient cybercrime countermeasures based on the foundational principles of theoretical, substantive and methodological research. Bucci (2009) stated that cybercrime is evolving and, unless it is controlled, it could mutate into a very dangerous national security issue with potentially catastrophic ramifications. The challenges of cybercrime require comprehensive approaches that go beyond the traditional bureaucratic, jurisdictional, terrestrial forms of cybersecurity, law enforcement, criminal investigation, and crime prevention. British sociologist Mary McIntosh (1975) suggested that improvements in crime investigation forces a reaction on the part of criminals who must become more organized to remain successful. Sinca (2015) noted that criminal- and cybersecurity entities are required to adopt innovative methods, techniques and countermeasures to effectively prevent, detect, respond to and investigate cybercrime incidents.

Based on the information noted above, it is imperative that those charged with addressing the cybercrime phenomenon develop and employ the technological expertise, operational capabilities, and skill sets required to prevent cybercrime, or investigate and prosecute cyber criminals. This paper proposes that cyber criminology serve as the theoretical, operational and methodological platform for implementing a comprehensive approach to countering the cybercrime threat. The approach is comprised of four selective criminological theories: (1) Routine Activity Theory, (2) Social Learning Theory, (3) Space Transition Theory and (4) Victim Participation Theory:

- Routine Activity Theory is explained by the intersection of three factors: (1) motivated offenders; (2) availability of suitable target or victims; and (3) the absence of capable

guardians. Researchers have used this theory to gain an understanding of the relationship and/or interaction between the criminal and the victim (Cox, Johnson and Richards, 2009). This theory has been used for almost three decades to effectively explain causation across several categories of crime and continues to serve as the theoretical base for several practical explanations of contemporary criminal behavior. Maras (2017) suggested that the value of the theory is that it contributed to the solution by not fixing offenders but rather fixing places and situations so that opportunities for crime are blocked. She concluded that this theory can be used to inform cybercrime prevention and reduction strategies and applied to make cybercrime less attractive to motivated cybercriminals.

- Social Learning Theory is often combined with the cognitive learning theory which theorizes that learning is influenced by psychological factors and behavioral learning based on responses to environmental stimuli. Bandura (197) integrated the two theories and also derived four key requirements for learning: (1) observation (environmental), (2) retention (cognitive), (3) reproduction (cognitive), and (4) motivation. His integrative approach to learning is known as the social learning theory. Maras stated that this theory has been used to explained certain types of cybercrime, such as digital piracy and hacking. The most influential agents of socialization are family and peers, and research has shown that cybercriminals learn or develop their skills from actors within their social sphere where illicit behavior is shared through social interactions. Moreover, cybercrime is exacerbated by the fact that the illicit activity is facilitated by a service-based criminal industry, in which specialists in the virtual underground economy develop products and services for use by other criminals. This crime-as-a-service business model drives innovation and sophistication and provides access to a wide range of tools that facilitate almost any type of cybercrime (Huang, Siegel, and Madnick, 2017). There is an absence of empirical research on offender behavior in cyber space, although learning and imitation play important roles in determining sources of criminal diffusion in cyberspace. (Broadhurst and Grabosky, 2005). The social learning theory can facilitate the development of a deeper understanding of the causes and motivations of cybercrime by discerning the who, why, and how of cybercrime.

- Space Transition Theory is an explanation of the different behavior patterns of the individuals who act in conforming manner in the terrestrial space but act in a nonconforming manner in virtual space. The theory argues that people behave differently when they move from one space to another. The creator of the theory K. Jaishankar (2007), suggested seven propositions as explanation of criminal behavior in cyberspace:

  1. Persons, with repressed criminal behavior (in the physical space) have a propensity to commit crime in cyberspace, which, otherwise they would not commit in physical space, due to their status and position.

  2. Identity Flexibility, Dissociative Anonymity and lack of deterrence factor in the cyberspace provides the offenders the choice to commit cyber crime

3. Criminal behavior of offenders in cyberspace is likely to be imported to Physical space which, in physical space may be exported to cyberspace as well.
4. Intermittent ventures of offenders in to the cyberspace and the dynamic spatial-temporal nature of cyberspace provide the chance to escape.

5. (a) Strangers are likely to unite together in cyberspace to commit crime in the physical space. (b) Associates of physical space are likely to unite to commit crime in cyberspace.

6. Persons from closed society are more likely to commit crimes in cyberspace than persons from open society.

7. The conflict of Norms and Values of Physical Space with the Norms and Values of cyberspace may lead to cybercrimes.

Victim Participation Theory holds that certain victims make themselves targets for crime by engaging in actions that are confrontational or risky (active); or by simply being present in a location that provides a motivated offender with the opportunity to commit an offense (passive); or by engaging provocative behavior in a criminogenic environment. Siegel (2006) suggests that some people cause or initiate a particularly volatile situation that result in the person being victimized. The victim may knowingly act in a provocative manner, uses fighting words or threats, or attacks first. The victim can display specific attributes, characteristics, or mannerism that unknowingly motivates or threatens the attacker. Victim precipitation may exist when an individual is part of a particular group that offends or threatens someone's political, social, and economic security, status or reputation.

The four criminological theories noted above are not the only explanatory descriptions for criminal behavior and/or victimology. However, taken together they form a theoretical integration approach which can be employed as a notional framework or descriptive model for broadly outlining and effectively articulating causation for the volume and distribution of cybercrime. Researchers have noted that "Regardless of the source of offender motivation,…. history suggests that the enforcement technology will always lag behind the criminal technology and criminals have always exploited opportunities that exceed law enforcement capabilities." (Albanese, 2011, p. 75). The use of cybercriminology can help close the gap between technology lag, theoretical knowledge, operational effectiveness, and organizational capabilities that plague both law enforcement and cybersecurity stakeholders who are responsible for addressing the cybercrime phenomenon.

The bar to enter and successfully perpetrate cybercrime is extremely low. Cyber criminals are forming private, trusted, and organized groups to conduct cybercrime. The adoption of specialized skill sets and professionalized business practices by these criminals is steadily increasing the complexity of cybercrime by providing actors of all technical abilities with the necessary tools and resources to conduct cybercrime. Not only are criminals advancing their abilities to attack a system remotely, but they are becoming adept at tricking victims into

compromising their own systems. Goodman (2105) stated that the cost of the cybersecurity protection efforts are increasing and amounts to approximately $100 Billion dollars in 2017.

Once a cyber network is compromised, cyber criminals will use their access to obtain personally identifiable information **(**PII**),** which includes online banking/brokerage account credentials and credit card numbers of individuals and businesses that can be used for financial gain. As cybercrime groups increasingly recruit experienced actors and pool resources and knowledge, they advance their ability to be successful in crimes against more profitable targets and will learn the skills necessary to evade the security industry and law enforcement. The potential economic benefits of cybercrimes are huge, and the probability of arrest and prosecution is extremely low. The main advantage of cybercrime over traditional crime is that "such crimes are less likely to be caught and prosecuted; only about 5% of cyber-criminals are caught" (Kshetri, 2009). Other cyber experts (Wall, 2001 & Yar, 2006) have categorized cybercrime in four subsets:

- Cyber-trespass (hacktivism, viruses, Denial of Service attacks).
- Cyber-deceptions (identity theft, fraud, piracy).
- Cyber-pornography (child pornography,
- Cyber-violence (cyberbullying, cyberstalking).

Cyber versus Traditional Crime

According to Richet (2013), the diffusion of cybercriminal activities is surpassing the capabilities of cybersecurity practitioners to control cybercrime. Currently, cybercriminals must no longer possess a high level of technical skill, practical expertise or accessibility

The National Computer Security Survey (2005) documented the nature, prevalence, and impact of cyber intrusions against businesses in the United States. It described three general types of cybercrime:

- Cyber-attacks are crimes in which the computer system is the target. Cyber-attacks consist of computer viruses (including worms and Trojan horses), denial of service attacks, and electronic vandalism or sabotage.
- Cyber theft comprises crimes in which a computer is used to steal money or other things of value. Cyber theft includes embezzlement, fraud, theft of intellectual property, and theft of personal or financial data.
- Other computer security incidents encompass spyware, adware, hacking, phishing, spoofing, pinging, port scanning, and theft of other information, regardless of whether the breach was successful.

Cyber versus Traditional Criminals

There are some studies that suggest that cybercrime offenders have the same demographics as traditional offenders. Cybercriminals, for example, are more likely to be men (ResearchAgenda).

Yet Odinot et al. (2016) conclude that the characteristics of offenders that are important in the offline world, such as age, physical health, and social behavior, are less important. This seems to be the dilemma as experienced by researchers and sociologists studying cybercrime and its motivation. Traditional theories used to explain traditional crime and criminal motivation such as moral development theory, social learning theory, strain theory, and the general theory of crime appear to only partially explain cybercrime and cyber. In addition to Odinat's observation that age, physical health, and social behavior are less important, two additional aspects stand out in relation to cybercrime, the personal anonymity and the separation of criminal and the crime scene. Jaishanka states that "the analogy of crimes of physical space and cyberspace can never be complete and successful…and therefore cybercrime is an entirely new form of crime" (pp. 290-291). In an attempt to reconcile the differences between physical and vertical crime as well as the difference between traditional and cyber criminals Jaishanka proposes a new theory called Space Transition Theory that focuses on the differences in crime and the differences in criminals based on where the crime is committed and the type of crime

There are limitations to the usage and potential benefits offered by cyber criminology. For example, the absence of robust evidence about the extent, role, and nature of criminal actors in cyber space impedes the development of sound countermeasures. Given the diversity of the types and sources of cybercrime, it is important to avoid stereotypical images of cyber criminals. Offenders come from many nations, and motivations are diverse, although financial goals appear to dominate (Broadhurst, et, al, 2014). Additionally, Yar (2005) noted that cyber criminology has limited utility in an environment that defies many of our theoretical assumptions about how the socio-interactional setting of routine activities is configured.

Other limitations offered by researchers focus of the argument that cybercrime is not an entirely new form of contemporary and/or innovative genre of crime. For example, Brenner (2010) suggested that most of the cybercrime we see today simply represents the migration of traditional crime to cyberspace where cybercriminals use available technology to commit old crimes in new ways. Other commentators have agreed with Brenner, suggesting that cybercrime is not a new type of crime but simply that "cyberspace" is just a new environment used to help commit crimes that are not new at all (Wilson, 2008). However, while acknowledging its limitations, researchers propose that cyberspace frees individuals from many of the constraints that apply to activities in the physical world, and current forms of crime fighting may not transition well to online. Others have questioned whether cybercrime is a category of crime in need of new theory or whether it is better understood by existing theories.

Space Transition theory endeavors to explain the nature of the behavior of the persons who bring out their conforming and non-conforming behavior in the physical space and cyberspace and specifically argues that people behave differently when they move from one space to another

The postulates of the theory state: (1) persons with repressed criminal behavior (in physical space) have a propensity to commit crimes in cyberspace that they otherwise would not commit due to their status and position; (2) identity flexibility, dissociative anonymity, and lack of deterrence factors in cyberspace provide the offenders with the means to commit cybercrime; (3) criminal behavior of offenders in cyberspace is likely to be imported to physical space, and

criminal behavior in physical space may be exported to cyberspace as well; (4) intermittent venture of offenders in to the cyberspace and the dynamic spatiotemporal nature of cyberspace provide a chance to escape; (5) (a) strangers are likely to unite together in cyberspace to commit crime in the physical space and (b) Associates of physical space are likely to commit crime in cyberspace; (6) persons from closed society are more likely to commit crimes in cyberspace than persons from open society; and (7) the conflict of norms and values of physical space with the norms and values of cyberspace may lead to cybercrimes.

Victims

The last side of the triangle is the victim or victims. While initially it seems unjust to blame the victim in any way for the crime, it is important to understand what if any behaviors contributed to the crime.

Detecting, preventing and responding to cybercrime incidents is problematic because of the difficulty in determining with some degree of certainty the identity, intent, or the motivations of an actor. The reality is that cybercrime can be very complex, extremely broad in scope, and may involve many multifaceted factors which are extremely difficult to discern (Krasvin, 2004). In 2010, Koops concluded that the Internet is transforming crime and it deserves special attention in criminology as well as criminal law and policy. The key to ability to distinguish criminal actors based on recognition of the various factors related to causes, motivations and modus operandi can facilitate the prevention, detection, investigation and quicker resolution of cybercrimes that have already occurred

While existing studies of the criminals and the crimes that commit do not adapt well to the online world, the existing theories for victimization appear to be well suited in explaining cyber victims. The significance difference in the nature of the crime (removal of time and place constraints), just means that the potential victims are exposed to a larger range of potential criminals. By focusing efforts in training and education, we may be able to reduce victimization through training and education. Most people inherently understand how to avoid attracting criminal attention in the physical world, yet do not exhibit such restraint in the online world. They may not recognize the parallels between flashing large amounts of cash in public and posting pictures of their expensive cars, boats, and houses on Facebook right below the post about their upcoming vacation in Hawaii.

Proposed Cyber criminology Minor

In order to analyze cybercrime in a more holistic manner, we need practitioners trained in a more holistic approach. Current academic fields segment the study of crime and criminal from the study of methods when it comes to cybercrime. By combining criminal justice studies with the technical aspects of digital forensics and penetration testing, students will see a complete picture of who commits cybercrimes and what motivates them, as well as how the crime is perpetrated and how they can be apprehended.

The proposed minor (detailed in Appendices A, B and C) attempts to combine criminal justice and cybersecurity to allow each major more exposure to the related programs and to provide a specialization for majors other than Cybersecurity and Criminal Justice.

While reviewing other Cyber criminology programs, one of the issues we found was that Cyber criminology programs were based in either the Criminal Justice or Computer Science departments, and this focus was reflected in the minor requirements. While each of the programs used the term interdisciplinary, the requirements reflected the host department with a requirement for a single class in the other department. While our proposed minor will be officially listed as a Criminal Justice minor, the requirements are evenly split between Criminal Justice and Cybersecurity departments.

Proposed Implementation

The proposed minor consists of 6 classes (18 Credits):
The 5 required courses:

CJS 1300 Introduction to Criminal Justice
CJS 1320 Introduction to Cyber criminology
CIS 4450 Digital Forensics
CIS 4710 Ethical Hacking/Penetration Testing
CJS 4200 Evidence and Criminal Procedure

With any one class from the following list:

CJS 3950 Criminal Investigation
CJS 4870 Victimology
CJS 4890 White Collar Crime
CJS 4950 Criminalistics (Forensic Science)
CIS 3350 Human Factors in IT Security
CIS 4550 Advanced Digital Forensics
CIS 4590 Network Security

Overview and Conclusions

Cybercrime and cyber criminals share some of the same characteristic with traditional crime and criminals, but the online environment presents new and unique opportunities for traditional criminals, as well as creating a new category of online criminals. The environment also creates new methods and operational opportunities. Cybersecurity practitioners are used to the technological aspects of the crime, the “when” and “what” aspects, but pay little attention to who commits the crimes and why. Without an understanding of the criminals and their motivations, cybersecurity will always be defensive, reactive, and one step behind.

References

Holt, T. J. (2010). Examining the Role of Technology in the Formation of Deviant Subcultures. *Social Science Computer Review*, *28*(4), 466-481. DOI: 10.1177/0894439309351344.

Jaishankar, K. (2007) International Journal of Cyber Criminology Vol 1 Issue 2 July 2007. Retrieved from http://www.cybercrimejournal.com/Editoriaijccjuly.pdf.

Kshetri, N. (2009). Positive externality, increasing returns, and the rise in cybercrimes. Communications of the ACM, 52(12). doi:10.1145/1610252.1610288 PMID:21218176.

Maras, M-H. (2017). Cyber criminology. Oxford University Press. New York, NY.

O'Driscoll, A. (2018) 107 Cybersecurity and cybercrime statistics, surveys, trends and studies. Retrieved from https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/US.

Ponemon (2017) Cost of cyber security study. https://www.accenture.com/t2017/PDF-62/Accenture-2017CostCybercrime-US-FINAL.

Richet, J-l. (2013). From young hackers to crackers. International Journal of Technology and Human Interaction, 9(3), 53-62, July-September 2013. Retrieved from

Samnow, S. (2014) Inside the criminal mind: Revised and updated. Broadway Books, Crown Publishing, Random House LLC, New York, NY.

Walls, D.S, ed. (2001) *Crime and the Internet.* New York: Routledge.

Yar, M. (2006). *Cybercrime and society.* Sage Publishing, London.

Appendix A: Minor Proposal

A. Summary

The proposed Cyber Criminology Minor in the department of Criminal Justice (CJ) leverages our universities s designation as a NSA Center of Excellence in Information Assurance Education (CAE/IAE) and leverages out strength in both Cybersecurity and Criminal Justice as well as it investments in the Center for Cyber Security and Intelligence Studies (CCSIS)

B. Description of the Minor

B1: Narrative description of the program

The Minor in Cyber criminology is available to all students who must maintain a cumulative GPA of 2.0 in all minor courses; all courses must be taken for a grade (no courses for the minor may be taken on a pass/fail basis). A maximum of 6 credits may be counted toward both the major and the minor. At least 12 credits in the minor must be taken at the university, unless they are taken as part of a consortium agreement. Students must declare a major before declaring a minor and must declare the minor by the first semester of the junior year.

B2: List all courses in the curriculum

The curriculum will involve the completion of 18 credits (six courses) 12 of which will be taken in addition to the student's major requirements and those of the University core curriculum.

Course
CJS 1300 Introduction to Criminal Justice
CJS 1320 Introduction to Cyber criminology
CIS 4450 Digital Forensics
CIS 4710 Ethical Hacking
CJS 4200 Evidence and Criminal Procedure
+ **1 Elective** (3cr) CJS 3950 Criminal Investigation CJS 4870 Victimology CJS 4890 White Collar Crime CJS 4950 Criminalistics (Forensic Science) CIS 3350 Human Factors in IT Security

CIS 4550 Advanced Digital Forensics
CIS 4590 Network Security

B3: Indicate the delivery format of all new courses

Other than the new course Introduction to Cyber criminology, these courses are part of the existing Computer and Information Systems(CIS) or Criminal Justice Studies(CJS) undergraduate program. Consequently, the offering of the Minor will utilize existing capacity in the program rather than require an increase in existing resources. Initially, the course material will be offered in the traditional sense with day and evening classes though efforts will be made to develop the online delivery component upon the programs implementation.

Courses are scheduled in a regular rotation that will ensure completion of the Minor requirements in conjunction with the student's major undergraduate degree study; e.g., the course of study will be within the conventional 126 credit limits.

Appendix B provides a listing of the courses in the curriculum, including the catalog number, title, description and units of credit.

Appendix C provides a listing of other university's Cyber criminology program requirements

B4: Describe how the program demonstrates academic integrity

Consistent with the universities mission, the Criminal Justice and Cybersecurity programs emphasize service to others and skills that will ensure responsible citizenship in a changing world. Cyber criminology minors will support Presidential Directive 54, the Comprehensive National Cybersecurity Initiative (CNCI). The CNCI directs higher education to prepare citizens to ensure that the boarders of cyberspace are secure. That contribution both addresses the current and future needs of the citizens of the US as well as serving the global community.

The proposed program respects academic integrity and intellectual merit put forth at the university through the adherence to all applicable student policies, procedures and honor codes.

B5: Indicate unusual or unique characteristics of the proposed minor

Because the field is relatively new, a minor in Cyber criminology would be unique in the area. There are only 3 other existing programs in the country, The University of Alabama, Saint Anslem College in New Hampshire and Georgia Southern University-Armstrong

In reviewing their approach to this subject area, there appears to be a lack of the interdisciplinary approach as presented in this proposal. Several focus on Cyber criminology as a sub discipline of criminology and ignore the motives and methods that come from computer science. Our diversity of contributors and the flexibility of the program provides for a unique feature as compared to the

approach taken by the University of Alabama approach, which is much less technical. The University of Alabama's only technical requirement is a basic course in digital forensics, while our approach provides a more balanced technical education with Introductory and Advanced Digital forensics as well as Ethical Hacking (Penetration Testing)

B7: Describe how the proposed minor affects related departments or fields of concentration

Since the Cybersecurity program is looking to merge the body of knowledge of Cybersecurity with the in-depth Major study of other programs, the Cybersecurity Minor could potentially attract students into those other programs. That is particularly true given that the job outlook in the coming decade is very favorable for Cybersecurity and the ongoing need for security specialists with domain knowledge in other specialized areas of study.

incorporates CIS 4650Information and Society.

D. Objectives, Outcomes and Assessment

D1: Indicate the program objectives and learning outcomes

The learning objectives, outcomes and assessment were developed in conjunction with the recommendations of the NIST-NICE Framework. NICE has published this complete definition of the field with the aim of providing a point of reference for the definition of the academic curriculum of a Cybersecurity study a college, or university. This Framework is the national standard for Cybersecurity education.

NICE is composed of seven general areas of concentration. There are 31 specialty areas distributed within these specialty areas, supported by 2,000 well-defined KSAs. The level of definition and acceptance of the NICE framework provides an easy point of reference for confirming that the detail of the proposed courses will satisfy the guidelines of the University Curriculum as put forth by the Faculty Assembly.

. The General Objectives of the Minor are to:

Provide a comprehensive and fully integrated understanding of the body of knowledge in Cybersecurity as captured in the Securely Provision, Operate and Maintain, Protect and Defend, Investigate and Oversee and Govern Areas. The other two areas are part of Intelligence Analysis and will not be covered in this Minor

Through focused discussion and hands-on assignments ensure integration of knowledge obtained from Minor with student's Major area of study

Develop an understanding of the ethical issues associated with the collection and use of information, as well as instill the ability to respond appropriately when confronted by new ethical challenges

Develop a practical skill set that can be referenced to one of the job task categories in NICE.

Develop conceptual and human relations capabilities sufficient to ensure our graduate's leadership status within the community.

Appendix B: Course Descriptions

Required Courses

CJS 1300 Introduction to Criminal Justice
A study of the agencies and processes involved in the Criminal Justice System - legislature, the police, the prosecutor, the public defender, the courts and corrections; an analysis of the roles and problems of law enforcement in a democratic society, with an emphasis upon inter-component relations and checks and balances; selected problems of administration in the Criminal Justice System, with an emphasis on Social Justice as a guide to policy formation.

CJS 1320 Introduction to Cyber criminology
Examines both traditional and contemporary forms of cybercrime from the social and behavioral sciences. Topics include: social learning theory, space transition theory, routine activity theory, moral disengagement, techniques of neutralization as a framework for explaining cybercrime and cyber criminals

CJS 4200 Evidence and Criminal Procedure
Rules of evidence of importance at the operational level in law enforcement and with criminal procedure in important areas such as arrest, force, and seizure. Supreme Court decisions affecting law enforcement.

CIS 4450 Introduction to Digital Forensics
This course introduces fundamental concepts in forensics and security control. It provides essential knowledge and skills for digital forensic auditors. This includes examination of the range of commonly accepted digital forensic audit methods and tools. It also introduces the principles that underlie assurance of the integrity, confidentiality and availability of information assets.

CIS 4710 Ethical Hacking
This course introduces genres of cyber-attack tools and techniques, examining the most widely used and most damaging from each category at a high level. Ways to design and implement the most effective defenses to ensure the confidentiality, availability, and integrity of software systems and data will be explored both in lecture and in basic laboratory exercises. Emphasis will be placed on ethical and professional conduct

Electives

CJS 3950 Criminal Investigation
Fundamentals of criminal investigation, including techniques of surveillance, crime scene search and recording, collection and preservation of physical evidence, scientific aids, modus operandi, sources of information such as interviewing and interrogation, follow-up and case preparation.

CJS 4870 Victimology
The process of becoming a victim of crime. Psychological stages through which victims pass. Crisis intervention with crime victims as well as means of prevention. Specific crime patterns and implications for victims. Consideration of victim response to such events as natural disasters and loss of loved ones.

CJS 4890 White Collar Crime
The problem of criminal deviance by the wealthy and powerful, including pro and anti-organizational deviance. Conflict, structural, and person-centered theories of elite deviance are compared. The appropriateness of various social control efforts is also looked at. Case studies of various industries and organizations.

CJS 4950 Criminalistics (Forensic Science)
A general course in forensic operations and techniques. Firearms identification, ballistics, and glass examinations. Physical impressions, document and ink studies, and the science of fingerprints applied to crime investigations. Forensic photography and specimen identification.

CIS 3350 Human Factors in IT Security
Human factors in design and operation of secure systems. Balance between theory, standards and practices related to human-computer interaction. Emphasizes design issues and processes as they apply to ensuring disciplined practice

CIS 4550 Advanced Digital Forensics
This course provides advanced understanding of system forensics. It takes the perspective that organizational control originates form the ability to track and assign accountability for electronic transactions. This course will provide a thorough understanding of forensic procedures associated with all known methods of violation and attack.

CIS 4590 Network Security
This is the ultimate security course on protecting company assets through network security. Topics include Firewall, Perimeter Security, Intrusion Detection Systems (IDS), Edge Devices, and Assessment. Students will learn how to develop a set of firewall rules that will keep hackers out, how to look at all possible ways in which unauthorized users might gain access to network assets, and how an IDS can provide an analysis showing who has access to the system. Students will develop a security plan and monitor ongoing activities to determine effectiveness of a security model.

Appendix C: Other Cyber Criminology Programs

The University of Alabama -Cyber Criminology Minor

The Cyber criminology minor is housed in the Department of Criminology and Criminal Justice, and requires 18 credits,12 required and 6 electives.

Required Courses (12 hours)

CC 201 Introduction to Cyber Criminology

CC 301 Cyber Law and Policy

CC 401 Law Enforcement in the Digital Age

CS 202 Introduction to the Internet

Elective Courses (6 hours)

CC 402 Digital Forensic Investigation

CC 395 Joint Electronic Crimes Task Force (JECTF) Internship

AC 334 Introduction to Fraud Risk Management

CJ 300 Survey of Criminal Theories

CS 340 Legal and Ethical Issues in Computing

PY 368 Introduction to Personality

CC 290/490 Special Topics in Cyber Criminology

Saint Anslem College, New Hampshire

Offers a 5-course minor in Cyber criminology housed in the Computer Science Department

CJ 214 - Introduction to Cyber Criminology

CJ 215 - Cyber Law and Policy

CS 111 - Computing I

CS 228 - Computer Forensics

CS 230 - Computer Networks

Georgia State University – Armstrong

The Department of Criminal Justice, Social and Political Science participates in offering an interdisciplinary minor in Cyber Security.

Required Courses (15 hours)

CRJU 1100 - Introduction to Criminal Justice

CRJU 1210 - Introduction to Cyber Crime

ITEC 1310 - Programming for Information Technology

CRJU 5010U - Digital Forensics I

CRJU 5020U - Digital Forensics II

Elective Courses (3 Hours)

CRJU 3160 - White-Collar and Organized Crime

CRJU 3190 - Criminal Law

CRJU 3300 - Criminology

CRJU 3500 - Criminal Evidence and Procedure

CRJU 5300U - Juvenile Delinquency