Journal of Cybersecurity Education, Research and Practice

Volume 2019 | Number 2 Article 5

January 2020

Teaching About the Dark Web in Criminal Justice or Related Programs at The Community College and University Levels.

Scott H. Belshaw
University of North Texas, scott.belshaw@unt.edu

Brooke Nodeland
University of North Texas, brooke.nodeland@unt.edu

Lorrin Underwood
University of North Texas, LorrinUnderwood@my.unt.edu

Alexandrea Colaiuta
University of North Texas, alexandreacolaiuta@my.unt.edu

Teaching About the Dark Web in Criminal Justice or Related Programs at The Community College and University Levels.

Abstract

Increasingly, criminal justice practitioners have been called on to help solve breaches in cyber security. However, while the demand for criminal justice participation in cyber investigations increases daily, most universities are lagging in their educational and training opportunities for students entering the criminal justice fields. This article discusses the need to incorporate courses discussing the Dark Web in criminal justice. A review of existing cyber-criminal justice programs in Texas and nationally suggests that most community colleges and 4-year universities have yet to develop courses/programs in understanding and investigating the Dark Web on the internet. The Dark Web serves as the new “Criminal Underground” for illegal activity and needs to be understood. This research outlines the need for criminal justice programs to teach courses in the Dark Web and offer course recommendations. Recommended syllabi material for Dark Web courses in criminal justice, and recommendations for development of these programs are included.

Keywords

cybersecurity, dark net, cybersecurity education, criminal justice, dark web

Cover Page Footnote

Special Thank you to Professor Peter Johnstone at the University of North Texas for his assistance on this article. His in-depth knowledge on Dark Web pedagogy really served as the foundation for this research.

INTRODUCTION

You can buy credit card numbers, all manner of drugs, guns, counterfeit money, stolen subscription credentials, hacked Netflix accounts and software that helps you break into other people's computers (Guccione, 2019). Buy login credentials to a $50,000 Bank of America account for $500. Get $3,000 in counterfeit $20 bills for $600 (Guccione, 2019). Buy seven prepaid debit cards, each with a $2,500 balance, for $500 (Guccione, 2019). A "lifetime" Netflix premium account goes for $6. You can hire hackers to attack computers for you. You can buy usernames and passwords (Guccione, 2019). Where does this illegal activity happen? - On the Dark Web.

Criminal justice programs have yet to fully incorporate the Dark Web courses in their academic preparation of future criminal justice practitioners. Students pursuing careers in criminal justice must be prepared to respond to modern threats including, but not limited to, a range of cyber related offenses (e.g. cyberbullying, cyberstalking, sexting, and cybersex crimes) as well as the traditional hacker, identity theft, terrorists, and nations wishing harm on the United States (Boleng, Schweitzer, and Gibson, 2007). Cyber threats have real world homeland security and individual security implications. The need for trained law enforcement officers with the skills to understand and investigate cybercrime increases daily. For example, large-scale attacks, such as those targeting Target, Equifax, and most recently Capital One, produce large amounts of data that can be distributed to criminals. Specifically, the Target breach occurred when cyber attackers accessed the company's server using credentials stolen from a third party vender allowing hackers to steal data from up to 40 million credit and debit card users during the 2013 holiday shopping season (Reuters, 2017). The Equifax breach likely affected close to 150 million people exposing social security numbers and other personal information, while the Capital One breach further exposed the personal information of roughly 100 million customers and applicants (Tomasic, 2019). These attacks provide criminals with personal information of American consumers making them vulnerable to identity theft or financial fraud (Sadiku, Tembley, & Musa, 2017). What happens to the data after it's been stolen? It is sold for profit on the Dark Web.

WHAT IS THE DARK WEB?

The Dark Web is comprised of hidden internet websites that are visible to the public, but their Internet Protocol or IP address details are intentionally hidden (Finklea, 2017). These websites can be visited by anyone on Internet, but it is not easy to find the server details on which the corresponding site is running, and it is difficult to track the one hosting the site. The Dark Web concept is achievable with the help of anonymity tools. One popular tool is The Onion Router (TOR). The

Dark Web is popular for both black market and user protection, so it has both positive and negative aspects (Finklea, 2017). Most of the products and services found on the Dark Web are used for sinister purposes. The Dark Web includes a wide range of networks, from small, friend-to-friend/peer-to-peer networks to large, popular networks such as Freenet, I2P and TOR, operated by public organizations and individuals (Finklea, 2017).

In the 1990s, the lack of security on the internet and its ability to be used for tracking and surveillance was becoming clear, and in 1995, David Goldschlag, Mike Reed, and Paul Syverson at the U.S. Naval Research Lab (NRL) wanted to know if there was a way to create internet connections that don't reveal who is talking to whom, even to someone monitoring the network (TOR Network, 2019). Their answer was to create and deploy the first research designs and prototypes of onion routing (TOR Network, 2019). From its inception in the 1990s, onion routing was conceived to rely on a decentralized network (TOR Network, 2019). The network needed to be operated by entities with diverse interests and trust assumptions, and the software needed to be free and open to maximize transparency and separation (TOR Network, 2019). Privacy and anonymity on the internet was the original reason this project was developed.

Some of the categories of Web-based hidden services include: Drugs, Fraud, Gambling, Hacking, Illegal hosting. Most Dark Websites are not directly accessible via a normal search made through a search engine; they effectively hide themselves. They are accessible only if the addresses of those sites are known to the user. Dark net markets operate over the Dark Web and include black market sales of illegal products, to stay hidden from governments and law enforcement agencies. The Dark Web is also used in other ways, like communication among whistle-blowers and protecting users from attacks or surveillance to ensure privacy in communication. But the Dark Web is mostly used in black markets as it promises total anonymity.

DARK WEB INVESTIGATIONS

Law enforcement officials are getting better at finding and prosecuting owners of sites that sell illicit goods and services (Guccione, 2019). In the summer of 2017, a team of cyber cops from three countries successfully shut down AlphaBay, the Dark Web's largest source of contraband, sending shudders throughout the network (Guccione, 2019). But many of these black market merchants simply went elsewhere. According to the Department of Justice, use of the Dark Web by criminals to anonymize communications makes it "impossible for law enforcement" to pursue criminal suspects (Ghappour, 2017).

In computer crime cases, locating the device or computer used by the suspect is the most critical step in discovering the perpetrator's identity and collecting evidence to build a successful prosecution (Ghappour, 2017). Without the suspect's laptop, investigators will lack evidence attributing virtual criminal conduct to an actual person (Ghappour, 2017). Conventional investigative methods rely on collection of data from third parties through compulsion and consent (Ghappour, 2017). When digital evidence is controlled by a person or entity subject to U.S. personal jurisdiction, compulsory process is used to obtain digital evidence (Ghappour, 2017).

When digital evidence is outside U.S. jurisdiction-such as when it is controlled by an entity with no physical presence or assets in the United States-formal and informal law enforcement cooperation mechanisms are used to obtain it (Ghappour, 2017). Twenty-first century criminals increasingly rely on the Internet and advanced technologies to further their criminal operations (Finklea, 2017). For instance, criminals can easily leverage the Internet to carry out traditional crimes such as distributing illicit drugs and sex trafficking (Finklea, 2017). In addition, they exploit the digital world to facilitate crimes that are often technology driven, including identity theft, payment card fraud, and intellectual property theft (Finklea, 2017). The FBI considers high-tech crimes to be among the most significant crimes confronting the United States (Finklea, 2017).

The Dark Web has been cited as facilitating a wide variety of crimes. Illicit goods such as drugs, weapons, exotic animals, and stolen goods and information are all sold for profit. There are gambling sites, thieves and assassins for hire, and troves of child pornography (Finklea, 2017). Data on the prevalence of these Dark Web sites, however, are lacking. TOR estimates that only about 1.5% of TOR users visit hidden services/Dark Web pages (Finklea, 2017). The actual percentage of these that serve a particular illicit market at any one time is unclear, and it is even less clear how much TOR traffic is going to any given site.

WHY DO CRIMINAL JUSTICE STUDENTS NEED TO LEARN ABOUT THE CYBERSECURITY AND THE DARK WEB?

The Department of Homeland Security (DHS) is actively seeking the advancement of cybersecurity career development. The DHS argues, "America needs well-trained professionals working in cybersecurity roles. These professionals are critical in both private industry and the government for the security of individuals and the nation. The DHS is committed to strengthening the nation's cybersecurity workforce through standardizing roles and helping to ensure we have well-trained cybersecurity workers today as well as a strong pipeline of

future cybersecurity leaders of tomorrow" (Cybersecurity Education & Career Development, (n.d.)). DHS houses the National Initiative for Cybersecurity Careers and Studies and offers opportunities for development of cybersecurity education programs at all levels highlighting the need for graduating students in cybersecurity as well as understanding how the Dark Web works. The initiative describes the range of activities and behaviors necessary to prevent and respond to cyber threats stating, "strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure" (Explore Terms, (n.d)). These activities often constitute criminal behavior and should be investigated as such. Often these exploitive actions originate in the Dark Web.

Current offerings at colleges and universities vary greatly between institutions. While some of the education and training needs of cyber personnel are similar to those of law enforcement officers addressed in current university criminal justice curricula, there are distinct curricular aspects as well. The purpose of this paper is to examine the offering of Dark Web courses in criminal justice. To do so, we explore why departmental offerings in the Dark Web courses across the state and cybersecurity programs across the country are needed to prepare future criminal justice personnel for careers in investigating on the Dark Web. The paper will further provide example syllabi recommendations for Dark Web courses in criminal justice. Since 9/11, the demand for cybersecurity education has received increasing attention as the private industry and the U.S. military have recognized that the days of the "innocent" hacker are long over (Boleng et al., 2007; Belshaw, 2012; Brown et al., 2012; McGuire, 2006; Mirkovic & Benzel, 2006;). The literature surrounding cybersecurity, Dark Web and criminal justice education is sparse. Few criminal justice programs in the United States offer courses, concentrations, or full programs in cybersecurity or offer classes on the Dark Web. Among those courses that do exist, they are often structured in a traditional lecture format. Similar to the initial lack of attention paid to general security type courses by criminal justice programs, cybersecurity has received little to no focus. For example, criminal justice course offerings in security were limited until the 1960s as the primary ideology at the time was that providing security was a business concern and not a criminal justice concern (Swart, 2000). Furthermore, cyber type classes have traditionally been harder to fill with students because of the notion that those fields will not offer monetary reward and are undervalued by students (Gabbidon, 2002; Swart, 2000). The cost of implementing may be a contributing factor for the lack of cybersecurity and Dark Web courses in criminal justice. Setting up a new program, making it

meaningful to students, and providing a level of education that will prepare students for job responsibilities, is often difficult to achieve on the limited budgets of academic programs (Dhillon & Hentea, 2005). However, the notion that these programs have to be overly expensive to start was countered by Dhillon & Hentea (2005) who outlined how a meaningful internet cyber program, incorporating lectures and labs with equipment, can be achieved on a low budget while providing a meaningful education to students. Another concern may be the security of the university's network in accessing the Dark Web and using it as an instructional tool. This may be addressed by allocating only certain university computers to access the Dark Web.

Several prior studies have highlighted the importance of taking a multidisciplinary approach to cyber education (Boleng et al., 2007; Katz, 2010; LeClair, 2013; Logan, 2002; McGettrick, 2013; Shumba, 2004). However, students interested in pursuing careers in this field continue to be pushed towards programs in other disciplines, such as business or computer science, as criminal justice programs have yet to follow suit in developing cybersecurity educational opportunities (Katz, 2010; Logan, 2002). Criminal justice students face a unique set of challenges in completing these programs (and/or courses) as they often lack the technical experience needed to be successful in Information Technology (IT) related programs (Nodeland, Belshaw & Saber, 2018). This often puts the criminal justice student at a disadvantage, as they often do not have the IT background to be successful in highly technical positions (Cheung et al., 2011; Katz, 2010). The issue with leaving cyber out of criminal justice is that many of the investigations into cybercrime will fall upon local law enforcement professionals who will be unprepared (Logan, 2002; McGuire, 2006), or to private investigators who, often times, are former law enforcement (Belshaw, 2012). These investigators often lack the knowledge to logon to the Dark Web or have an understanding of Dark Web website navigation because the websites are not generally published.

In the end, criminal justice programs need to do their part in preparing the future workforce to deal with investigations on the Dark Web. A qualified workforce, to deal with cybersecurity, is already in short supply and for the foreseeable future demand for well-qualified cyber experts will only increase (Boleng et al., 2007; Cheung et al., 2011; LeClair, Abraham, & Shih, 2013). To ensure a well-rounded workforce that is in great demand, it is imperative that Dark Web education programs expand while providing a well-balanced and meaningful education. For this to be accomplished, criminal justice programs need to expand and embrace the teaching of cybersecurity classes including ones on the Dark Web (Hentea & Dhillon, 2006; Swart, 2002; Nodeland, Belshaw & Saber, 2018). General criminal justice programs have increased in popularity and embracing

cybersecurity education will enhance these program offerings and ensure the expansion of the discipline (Williams, McShane, & Karson, 2007).

METHODS

To determine the state of cybersecurity education in criminal justice, we first compiled a list of 2- and 4-year colleges in Texas. Once the list was created, we utilized publicly available information from the official university/college website for each school to identify schools offering a program in cybersecurity as well as the department housing the program, whether that program was at the undergraduate level, graduate level, or a certificate program; what type of school (2-year, 4-year, public, private); and courses offered in the cyber program. We also included if they are currently offering any classes in the Dark Web. Only colleges or universities that were open and in operation at the time of the data collection were examined. The results are presented in Table 1 below.

Among colleges and universities in Texas offering a cybersecurity program, there were no criminal justice programs housing a cybersecurity related program. Cybersecurity programs were housed in 7 business departments, 14 computer science departments, and 1 engineering department. There were 17 cybersecurity programs at the undergraduate level, 3 at the graduate level, and 20 certificate programs. Taken together, this suggests that business and engineering departments are taking a more active approach to educating students on cybersecurity and the Dark Web than criminal justice programs.

Some schools have shown the need for criminal justice courses in cybersecurity by requiring these courses outside of technical majors, such as computer science. Specifically, one school recommends students minor in criminal justice while others require courses such as criminal investigations. These recommendations suggest that departments outside of criminal justice are beginning to see the need for providing this type of training to their students. Further, this suggests the importance of training criminal justice professionals in investigating cybersecurity.

Next, in order to further explore the state of cyber education in criminal justice, we conducted an online search for cybersecurity programs in criminal justice anywhere in the country either online or in a traditional campus-based program. In addition, we reviewed universities certified by the National IA (Information Assurance) Training and Education Programs for cybersecurity programs in criminal justice. The authors identified 8 colleges or universities offering cybersecurity programs in criminal justice in the form of either a certification, undergraduate or graduate degree. These universities are among the first to incorporate cybersecurity into their criminal justice programs. Boston

Table 1. Cybersecurity/Dark Web Programs in Texas

School	*Type*	*Public, private or for profit*	*Department/ Program*	*Programs (U,G,Cert)*[1]	***Courses in Dark Web***	*Distribution method*[2]
Amarillo College	2	Public	Computer Cybersecurity Certificate	Cert.	N	Campus based
			Computer Networking/ Cyber-Security	A.A.S.	N	
Central Texas College	2	Public	Business and Business Technology; Information Security	Cert.	N	Both
Collin College	2	Public	Information Systems	A.A.S; Cert.	N	Campus based
DeVry University Texas	4	For profit	Cybersecurity Programming Degree Specialization, Computer information Systems Degree with specialization in Cybersecurity - College of Engineering	B.S.	N	Both

Houston Community College	2	Public	Computer Systems Networking: Cybersecurity, Network Systems and Cybersecurity Level I and II Information Technology: Cybersecurity	A.S.S.; Cert.	N	Campus based
Kilgore College	2	Public	Whitten Applied Tech. Center (WHITN); Computer science program Computer Networking: Cybersecurity	A.S.S.; Cert.	N	Both
Lamar State College Orange	2	Public	Business & Technology: Cisco Networking/Cybersecurity Technician	Cert.	N	Both
Laredo Community College	2	Public	Computer Information Systems: Network and Cybersecurity Technology	A.S.S.	N	Campus based
LeTourneau University	4	Private	Computer Science: Cybersecurity	B.S.	N	Campus based
North Central Texas College	2	Public	Computer Information Systems: Cybersecurity	A.A.S; Cert.	N	Campus based

Sam Houston State University	4	Public	Computer Science: Cybersecurity	G Cert.	N	Both
San Antonio College	2	Public	Information Assurance and Cybersecurity	A.S.S.; Cert.	N	Both
South Plains College	2	Public	Computer Information Systems: Cybersecurity	Cert.	N	Both
Southern Methodist University	4	Private	Computer Science and Engineering Cyber Intelligence Cybersecurity	B.S., M.S., Ph.D., Cert.	N	Both
St Philip's College	2	Public	Business Information Systems; Information Assurance and Cybersecurity	A.A.S, Cert.	N	Both
St. Mary's University	4	Private	Department of Computer Science; School of Science, Engineering and Technology	G Cert. M.S.	N	Campus based
Sul Ross State University	4	Public	Computer Science: Cybersecurity	B.S.	N	Campus based
Texas A & M University Corpus Christi	4	Public	Department of Computing Sciences; Cybersecurity and Infrastructure	B.S.	N	Campus based

Texas A & M University Texarkana	4	Public	Cybersecurity	Cert.	N	Online
Texas State Technical College	2	Public	Cybersecurity	A.S.S., Cert.	N	Campus based
Texas Tech University	4	Public	Department of Computer Science: Center for the Science & Engineering of Cybersecurity	Cert.	N	Campus based
The University of Texas at El Paso	4	Public	Computer Science	G Cert.	N	Campus based
The University of Texas at San Antonio	4	Public	College of Business: Department of Information Systems and Cybersecurity	B.B.A.	N	Campus based
University of Dallas	4	Private	Satish & Yasmin Gupta College of Business: Cybersecurity	M.S.; Cert	N	Both
University of North Texas	4	Public	Computer Science and Engineering Information Science	M.S.; Ph.D.; U and G Cert.	Y	Campus based

University of Phoenix	4	For-profit	College of Information Systems & Technology	U and G Cert.	N	Online
University of the Incarnate Word	4	Private	School of Media & Design: Bachelor of Science in Cybersecurity; Computer of Information Systems	B.S.	N	Campus based
Wayland Baptist University	4	Private	Business Administration, Cybersecurity	B.A.S.	N	Both

[1]*U = (Undergraduate certificate as well as Associates and Bachelors programs), G = (Graduate certificate as well as Masters and P.h.D.'s), Cert. = Certificate*

[2]*Recommends a minor in criminal justice but no specific courses*

[3]*Distribution method = Campus based programs are offered completely on campus and in person; Online programs are offered solely online, and Both means that the program and/or courses are offered both on campus and online*

University Metropolitan College is among the few schools in the nation to offer a cybersecurity program in criminal justice. Their Master of Criminal Justice, Cybercrime Investigation and Cybersecurity degree provides students courses in legal practices and cyber criminology, practical digital investigative knowledge, as well as policies related to cybersecurity risk assessment. Utica College has the most diverse offering of cybersecurity certificate and degree options in criminal justice, or justice studies providing students with both continuing education and degree programs. Other cybersecurity courses in criminal justice vary by university and are included Table 2 below.

U.S. News & World Report (2017) reports that many online cybersecurity bachelor's degree programs require students complete courses covering ethics, cybercrime law and information security but none on Dark Web research. In addition to technical courses, which prepare students to protect governments and business from cyberattacks, they suggest courses in computer forensics, criminal investigations, and criminal evidence to provide students with skills to track down perpetrators of cybercrimes. Similar to other developing fields, they also suggest completion of an offline internship to gain field work experience and enhance their skills before graduation. Only one of the programs surveyed was currently offering classes in the Dark Web or Dark Net at the time of the data collection. This was a school in Texas. The Department of Criminal Justice program offers a graduate class on Illicit Drugs and the Dark Web as an elective.

DISCUSSION: RECOMMENDATIONS FOR INCORPORATING DARK WEB COURSES INTO CRIMINAL JUSTICE PROGRAMS

Criminal justice programs are best situated to provide students with the foundational knowledge to respond to and investigate threats. Criminal justice students represent the law enforcement and criminal justice practitioners of tomorrow and, therefore, should be prepared to handle all aspects of criminal investigation, including searching in the Dark Web. This can be treated no different than going into another neighborhood for police. Criminal justice programs are tasked with educating students on diverse and ethical issues related to police, courts and corrections. Similarly, students are educated on causes of crime, legal issues and criminal justice system responses to crime. The advent and expansion of the internet has, in many ways, changed the types of crime and methods of investigation that law enforcement and criminal justice practitioners will be tasked with. Criminal justice programs should begin to provide the foundational knowledge to future practitioners.

Table 2. National Cybersecurity Programs in Criminal Justice

School	*Program Type*	*Cyber courses in criminal justice*	*Distribution method*[1]
Boston University Metropolitan College	Master of Criminal Justice - Cybercrime Investigation & Cybersecurity Concentration	Cybercrime, Applied Digital Forensic Investigation, Security Policies and Procedures, Digital Forensics and Investigations	Both
City University of Seattle	Bachelor of Science in Criminal Justice – Cyber Forensics Investigation Emphasis	Cyber and Surveillance Law and Governance, Investigation of Cyber Crime, Risk Assessment and Prevention*	Both
Colorado Technical University	Bachelor of Science in Criminal Justice - Cybercrime and Security	Introduction to Cybercrime, Cybersecurity and Policy, Terrorism and Organized Crime, Internship or Cybercrime Capstone, Unix Fundamentals, Introduction to Computer Security, Principles of Network Security, Security Risk Management, Ethical Hacking, Operating System Security, Computer Forensics I, Computer Forensics II, Understanding Critical Infrastructures, Introduction to	Online

		Programming Logic, Fundamentals of Networking	
Indiana University of Pennsylvania	Bachelor of Science in Criminology – Minor in Cyber Security	Cybersecurity and Loss Prevention, Cybersecurity and the Law*	Unknown
Northeastern State University - Tahlequah	Bachelor of Science in Cyber Security	Introduction to Cyber Security, Digital Forensics I & II, Special Topics in Cyber Security, Cyber Security Senior Seminar*	Unknown
Strayer University	Bachelor of Science in Criminal Justice - Computer Security and Forensics; Cybersecurity Management	Introduction to Cybercrime, Cybersecurity and Policy, Cybercrime Capstone, Unix Fundamentals, Introduction to Computer Security, Principles of Network Security, Security Risk Management, Ethical Hacking, Operating System Security, Computer Forensics I, Computer Forensics II	Campus based

	Computer Forensics Certificate, Cyber Crime and Fraud Investigation Certificate, Cyber Network Defense Certificate, Cyber Operations Certificate, Online Master of Professional Study in Cyber Policy and Risk Analysis, Cyber Policy Certificate, Bachelor of Science in Cyber-security, Master of Science in Cyber-security, Cybersecurity Technologies Certificate	Cyber Technologies for Criminal Justice, Cybercrime Investigation and Forensics I, II, & III, Computer Hardware and Peripherals, Software Foundations for Cybersecurity, Information Security, Computer Network Investigations, Information System Threats, Attacks and Defenses, System Vulnerability Assessments*	
Utica College			Both

[1]*Distribution method = Campus based programs are offered completely on campus and in person; Online programs are offered solely online, and Both means that the program and/or courses are offered both on campus and online*

*Additional required and elective courses offered outside of the criminal justice department in programs such as computer science, information systems, and cybersecurity

The criminal justice system has a reputation for moving slowly and not being readily adaptive to change. Similarly, criminal justice programs at universities across the country fall into similar routine with the occasional addition of new classes, but generally are slow to incorporate new programs or extensive restructuring of courses. Security focused programs are an example of where criminal justice programs have failed in the past to keep up with the times. Many business departments created security courses and programs before criminal justice departments, despite the fact that criminal justice trained students would be better situated and legally trained to respond to these issues. Despite institutional constraints in implementing and developing new courses, the number of programs offering cyber related criminal justice programs and degrees continues to increase as should the availability of courses that will provide foundational knowledge of the Dark Web and Dark Web investigations among future criminal justice practitioners entering the workforce. Now is the time for criminal justice programs to take notice and to take an active part in the training of cybersecurity experts of tomorrow.

Criminal justice programs are generally the first stop for law enforcement officers of tomorrow. Educating students in Dark Web investigations will make them more marketable as well as better prepare them for the changing demands of the field they plan to enter. Cybersecurity in criminal justice also allows for the exploration of various legal and investigatory issues surrounding the enforcement of cybercrime laws. For example, a course in Crime on the Dark Web will provide students with an in-depth examination of cybercrimes, cyber criminals, legal requirements surrounding the collection and preservation of digital evidence on the internet, investigative techniques in the Dark Web, and criminological theories applicable to computer crime. This course introduces students to cyber offenses as well as the concept of securing digital information on the internet. It also incorporates common criminal justice themes and applies them to the digital environment providing future law enforcement officers with a desirable skillset. A course in Information Warfare, Security, and Risk Analysis would provide students with an in-depth examination of information warfare, the management of information security, and the analysis of risk within organizational contexts (Nodeland, Belshaw & Saber, 2019).

Criminal justice programs should provide experiential learning opportunities that will allow students to interact with the Dark Web and learn hands on skills for responding to cybercrime threats in a real-world setting. Lecture based courses are important in terms of providing instruction and foundational knowledge, but the utilization and development of online investigatory skills will better prepare students for daily life in the field. Experiential learning opportunities in the form of labs, simulations, video games, etc., will provide students with hands on training to prepare them for responding to and investigating cyberattacks. Prior additions to criminal justice programs have utilized this approach to provide students with hands on experience in a new area of specialization and foster an experiential learning environment (Conklin, 2006; Hoffman, Rosenberg, Dodge, & Ragsdale, 2005; Li, Zhao, & Shi, 2009; Mirrkovic & Benzel, 2012; Rowe, Lunt, & Ekstrom, 2011). Cybersecurity courses, in particular, would benefit from the inclusion of these types of experiences as a way of developing students' skill set. Opportunities may be in the classroom or come in the form of site visits or training courses.

Expectations of law enforcement in responding to cyberattacks will continue to grow. Future law enforcement professionals, and those pursuing continuing education, will benefit from offering cybersecurity courses while developing their real-world application of their investigatory skillset. Working within the parameters of the law, law enforcement is in the best position to collect evidence and build a prosecutable case

against cyber offenders. While computer and technical skills are important, law enforcement officers do not need to be able to write code to be able to investigate cyberattacks. Criminal justice based programs are in the best position to bridge the gap between traditional law enforcement expectations and responding to new cyber threats.

REFERENCES

Belshaw, S.H. (2012). Private investigation programs as an emerging trend in criminal justice education? A case study of Texas. *Journal of Criminal Justice Education, 23*(4), 462-480.

Belshaw, S, (2019/Accepted-In Press) Next Generation of Evidence Collecting: The Need for Digital Forensics in Criminal Justice Education. *Journal of Cyber Security Education, Research and Practice.*

Boleng, J., Schweitzer, D., & Gibson, D.S. (2007). Developing cyber warriors. In presentation, *Third International Conference on i-Warfare and Security*. US Air Force Academy, Colorado Springs, CO.

Brown, C., Crabbe, F., Doerr, R., Greenlaw, R., Hoffmeister, C., Monroe, J., Needham, D., Phillips, A., Pollman, A., Schall, S., Schultz, J., Simon, S., Stahl, D., & Standard, S. (2012). Anatomy, dissection, and mechanics of an introductory cyber-security course's curriculum at the United States Naval Academy. Paper presented at the *Proceedings of the 17th ACM annual conference on innovation and technology in computer science education*.

Cheung, R.S., Cohen, J.P., Lo, H.Z., and Elia, F. (2011). Challenge based learning in cybersecurity education. Paper presented at the *Proceedings of the 2011 International Conference on Security & Management.*

Chin, S.K., & Older, S. (2006). A rigorous approach to teaching access control. Paper presented at *Proceedings of the First Annual Conference on Education in Information Security*, New York.

Clark, K., Gerstenblith, Alonso, D., Wright, R., & Pandya, N. (2013). Inter-institutional partnerships: The development of a multidisciplinary/interprofessional course in forensics. *Journal of Criminal Justice Education, 24*(3), 357-373.

Cone, B.D., Irvine, C.E., Thompson, M.F., & Nguyen, T.D. (2007). A video game for cyber security training and awareness. *Computers & Security 26*, 63-72.

Conklin, A. (2006). Cyber defense competitions and information security education: An active learning solution for a capstone course. Paper presented at the *Proceedings of the 39th Hawaii International Conference on System Science*, Hawaii.

Cybersecurity Education & Career Development. (n.d.). In *Official Website of the Department of Homeland Security*. Retrieved March 2, 2017. https://www.dhs.gov/topic/cybersecurity-education-career-development

Dhillon. H. & Hentea, M. (2005). Getting a cybersecurity program started on low budget. Paper presented at P*roceedings of the 43rd ACM Southeast Conference*, Georgia.

Explore Terms: A Glossary of Common Cybersecurity Terminology. (n.d.). In *National Initiative for Cybersecurity Careers and Studies*. Retrieved March 23, 2017, from https://niccs.us-cert.gov/glossary

Finklea, Kristin (2017). Dark Web. Congressional Research Service https://fas.org/sgp/crs/misc/R44101.pdf

Guccione, D. (2019), What is the Dark Web? How to access it and what you'll find. THE STATE OF CYBERSECURITY. Website retrieved on April 3, 2019 at https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html

Hentea, M., Dhillon, H, & Dhillon, M. (2006). Towards changes in information security education. *Journal of Information Technology Education, 5*, 221-233.

Hoffman, L.J., Rosenberg, T., Dodge, R., & Ragsdale, D. (2005). Exploring a national cybersecurity exercise for universities. *IEEE Security & Privacy*, *3*(5), 27-33.

Jensen. B.K., Cline, M., & Guynes, C.S. (2006). Teaching the undergraduate CS Information security course. *The SIGCSE Bulletin*, *38*(2), 61-63.

Katz, F.H. (2010). Curriculum and pedagogical effects of the creation of a minor in cyber security. In *2010 Information Security Curriculum Development Conference*, (pp. 49-51). ACM.

Kessler, G. C., & Ramsay, J. (2013). Paradigms for cybersecurity education in a homeland security program. *Journal of Homeland Security Education*, *2*, 35.

Kooi, B. & Hinduja, S. (2008). Teaching security courses experientially. *Journal of Criminal Justice Education, 19*(2), 290-307.

LeClair, D., Abraham, S, & Shih, L. (2013). An interdisciplinary approach to educating an effective cybersecurity workforce. Paper presented at *Proceedings of the 2013 on InfoSecCD'13: Information Security Curriculum Development Conference*.

Li, J., Zhao, Y., & Shi, L. (2009). Interactive teaching methods in information security course. Paper presented at *Scalable Computing and Communications; Eighth International Conference on Embedded Computing, 3009. SCALCOM-EMBEDDEDCOM'09. International Conference.*

Logan, P. Y. (2002). Crafting an undergraduate information security emphasis within information technology. *Journal of Information Systems Education*, *13*(3), 177.

McGettrick, A. (2013). Toward effective cybersecurity education. *IEEE Security & Privacy, 11*(6), 66-68.

McGuire, T. J., & Murff, K. N. (2006). Issues in the development of a digital forensics curriculum. *Journal of Computing Sciences in Colleges*, *22*(2), 274-280.

Micco, M., & Rossman, H. (2002, February). Building a cyberwar lab: lessons learned: Teaching cybersecurity principles to undergraduates. In *ACM SIGCSE Bulletin* (Vol. 34, No. 1, pp. 23-27). ACM.

Mink, M., & Freiling, F. C. (2006). Is attack better than defense?: teaching information security the right way. Paper presented at*Proceedings of the 3rd annual conference on Information Security curriculum development*.

Mirkovic, J., & Benzel, T. (2012). Teaching cybersecurity with DeterLab. *IEEE Security & Privacy*, *10*(1), 73-76.

Namin, A. S., Aguirre-Muñoz, Z., & Jones, K. S. (2016). *Teaching Cybersecurity through Competition.* Paper presented at Annual International Conference On Computer Science Education: Innovation & Technology.

Nodeland, B., Belshaw, S., & Saber M. (2018). Teaching Cyber Security to Criminal Justice Majors. *Journal of Criminal Justice Education*. https://doi.org/10.1080/10511253.2018.1439513

O'Leary, M. (2006). A laboratory based capstone course in computer security for undergraduates. In *ACM SIGCSE Bulletin* (Vol. 38, No. 1, pp. 2-6). ACM.

Online Cybersecurity Bachelor's Degree. (n.d.). In *U.S. News and World Report*. Retrieved March 2, 2017. https://www.usnews.com/education/online-education/cybersecuritybachelors degree#coursework

Patriciu, V. V., & Furtuna, A. C. (2009). Guide for designing cybersecurity exercises. In *Proceedings of the 8th WSEAS International Conference on E-Activities and information security and privacy* (pp. 172-177). World Scientific and Engineering Academy and Society (WSEAS).

Reuters. "Target Settles 2013 Hacked Customer Data Breach For $18.5 Million." *NBCNews*, NBC, 24 May 2017, https://www.nbcnews.com/business/business-news/target-settles- 2013-hacked-customer-data-breach-18-5-million-n764031. Accessed 2 Jan. 2018.

Rowe, D. C., Lunt, B. M., & Ekstrom, J. J. (2011). The role of cyber-security in Information technology education. Paper presented at *Proceedings of the 2011 conference on Information technology education*.

Sadiku, M. N., Tembely, M., & Musa, S. M. (2017). Identity Theft. *International Journal of Engineering Research*, *6*(9), 422-424.

Salah, K., Hammoud, M., & Zeadally, S. (2015). Teaching Cybersecurity Using the Cloud. *IEEE Transactions on Learning Technologies*, *8*(4), 383-392.

Schneider, F. B. (2013). Cybersecurity education in universities. *IEEE Security & Privacy*, *11*(4), 3-4.

Sharma, S.K, & Sefchek, J. (2007). Teaching information systems security courses: A hands-on approach. *Computers & Security*, *26*, 290-299.

Shumba, R. (2004). Towards a more effective way of teaching a cybersecurity basics course. *ACM SIGCSE Bulletin*, *36*(4), 108-111.

Smith, C. F., & Choo, T. (2016). Revisiting security administration in the classroom: A decade later. *Security Journal*, *29*(2), 198-212.

Sohn, S. Y., Park, H.Y., & Chang, I.S. (2009). Assessment of a complementary cyber Learning system to offline teaching. *Expert Systems with Applications, 36*, 6485-6491.

Solms, R.V., & Niekerk, J.V. (2013). Form information security to cybersecurity. *Computers & Security, 38*, 97-102.

Stewart, K. E., Humphries, J. W., & Andel, T. R. (2009). Developing a virtualization platform for courses in networking, systems administration and cybersecurity education. Paper presented at *Proceedings of the 2009 Spring Simulation Multiconference*.

Tomasic, M. (2019, August 1). Experts: Capital One data breach latest example of constant cybersecurity threats. In *TRIB LIVE*. Retrieved from https://triblive.com/local/westmoreland/experts-capital-one-data-breach-latest-example-of-constant-cyber-security-threats/

TOR Project (2019). The TOR Project. Retrieved April 20, 2018, from https://www.torproject.org/about/history/

White, S.K. (2016). *Top U.S. universities failing at cybersecurity education*. Retrieved March 2, 2017. http://www.cio.com/article/3060813/it-skills-training/top-u-s-universities-failingat cybersecurity-education.html

Whitman, M. E., & Mattord, H. J. (2004). Designing and teaching information security curriculum. Paper presented at *Proceedings of the 1st annual conference on Information security curriculum development*.

Appendix 1: Syllabus Recommendations

Upon completion of a Dark Web class, the students should be expected to: (1) be able to differentiate between theoretical and cross-disciplinary approaches to the Dark Web; (2) be able to analyze the evolution of the Dark Web in the context of emerging threats; (3) be able to distinguish and classify the forms of cybercriminal activity through the Dark Web, and the technological and social engineering methods used to undertake such crimes; (4) be able to investigate assumptions about the behaviors and roles of offenders and victims in the Dark Web; (5) be able to analyze and assess the impact of cybercrime, along with the mitigating techniques used to defend against cybercrime; (6) and be able to discuss, analyze and apply Dark Web -related research and applications.

Suggested books would be:
1. Sion Retzkin Hands-On Dark Web Analysis: Learn what goes on in the Dark Web, and how to work with it. Publisher: Packt Publishing (December 26, 2018) ISBN-10: 178913336X
ISBN-13: 978-1789133363

2. Jamie Bartlett. The Dark Net. Publisher: Melville House; Reprint edition (May 10, 2016) ISBN-10: 1612195210 ISBN-13: 978-1612195216

Illicit Drugs and the Dark Web

Spring 2016

CJ 5800 (900) 3 S.H.

Course Objectives
Upon successful completion of this course students will be able to:

- Demonstrate a working understanding of the origins and evolution of conventional drug routes
- Articulate an understanding of the nature and characteristics of the first underground drug communities
- Explain the role of cryptomarkets in the distribution of illicit drugs
- Identify and explain the different approaches taken towards regulating conventional versus on-line drug distribution networks
- Discuss current and future trends in cybercrime and the Dark net as they pertain to illicit drugs

COURSE INFORMATION AND SCHEDULE

The course is divided into learning weeks. It is my expectation that you will read all the listed reading for each week. The weekly reading list is considered the absolute minimum necessary to progress successfully through the course. It is strongly recommended that you do considerably more reading than the minimum.

WEEKLY SCHEDULE
Books: TDN → The Dark Net (Bartlett 2014)

DONDN → Drugs on the Dark Net (Martin 2014)

Additional Material: (See each individual week under the Course Content section)

Week 1:	Jan. 16 – Jan 21	**Introduction to the course:** From traditional drug routes to the Silk Road Introduction to the addressed terms & definitions https://inpud.wordpress.com/timeline-of-events-in-the-history-of-drugs/
Week 2:	Jan 22 – Jan 28	**Conventional Drug routes:** Marijuana / Amphetamines Additional material
Week 3:	Jan 29 – Feb 4	**Conventional Drug routes:** Cocaine & Heroin Additional material
Week 4:	Feb 5 – Feb 11	**History of the Internet & first underground communities** **Normality and deviance on the net:** Applications of the Durkheimian 'deviance' online Additional material
Week 5:	Feb 12 – Feb 18	**Social Media and Drug Markets:** EMCDDA: The internet and drug markets (Chapter 12) & further selected sources from the Chapter's references
Week 6:	Feb 19 – Feb 25	**Conceptualizing Cryptomarkets** DONDN p. 5 -25 & - Martin, J. (2014). Lost on the Silk Road: Online drug distribution and the 'cryptomarket'. Criminology and Criminal Justice, 14(3), 351-367.
Week 7:	Feb 26 – Mar 4	**Cryptomarkets Operations** DONDN p.25-46
Week 8:	Mar 5 – Mar 11	**Mid-Term Question Response**
Week 9:	Mar 12 – Mar 18	**SPRING BREAK**
Week 10:	Mar 19 – Mar 25	**Bitcoins / Cryptocurrencies in the dark net** DONDN p.25-46 & Additional material

Week 11:	Mar 26 – Apr 1	**Conventional vs Online Drug Distribution Networks** DONDN p. 47 – 60 & TDN Chap. 5
Week 12:	Apr 2 – Apr 8	**Conventional vs Online Drug Distribution Networks** DONDN p. 47 – 60 & 1. Barratt, M. J., Ferris, J. A., & Winstock, A. R. (2014). Use of Silk Road, the online drug marketplace, in the United Kingdom, Australia and the United States. Addiction, 109(5), 774-783.
Week 13:	Apr 9 – Apr 15	**Cryptomarkets & Law Enforcement** DONDN p. 61 – 79
Week 14:	Apr 16 – Apr 22	**Global law enforcement and legal responses nationally & internationally** Additional material
Week 15:	Apr 23 – Apr 29	**Current & Future trends in cybercrime and Dark Net** Additional material
Week 16:	Apr 30 – May 6	**Final Question Response Preparation Week**
Week 17:	May 7 – May 8	**Final Question Response Submission**

ASSESSMENTS AND GRADING:

1. Students are required to respond to weekly Discussion Board questions. In addition you must also respond to another students response so that in total you will write one question response of not less than 500 words and one response to another student of not less than 250 words for each discussion board posted. Your initial post is due no later than **11:59pm on Thursday** of each week, and your response to another student's post is due no later than **11:59pm on Sunday** of each week.

Discussion board submission will be graded based upon the following criteria. A timely, well-structured and reasoned DB entry that complies with the word count contains no grammatical or punctuation errors and provides the reader with at least two further sources for research, other than the course textbooks will receive maximum points. A timely written response to another student's post that complies with the word count contains no grammatical or punctuation errors and provides the reader with at least two further sources for research, other than the course textbook will receive maximum points.

Each DB is graded out of 10. There are eleven DB questions to respond to. Failure to participate in one or more discussion boards will result in lowering the final course grade one full letter grade, e.g. from B to C, etc. 110 points of the total grade for class

Level of Achievement	Discussion Points	Comprehension
Very Good Pass	10pts	Demonstrates complete understanding of the issue/s. Supports position with numerous, relevant sources. Backs argument with justifications and authority. Uses informed ideas to support conclusion. Clear evidence of critical discussion. No errors.
Good Pass	8-9pts	Demonstrates an adequate understanding of the issue. Uses minimum number of sources to back position. Limited number of ideas utilized to support conclusion. Overall less engaging and thorough than an a Very Good Pass.
Adequate to Pass	6-7pts	Does not demonstrate an accurate understanding of issue/s. Makes minimum effort to use sources and data. Does not demonstrate informed ideas that illuminate the answers but makes an effort.
Deficient	5pts or below	Inaccuracies. Minimal effort demonstrated. Does not demonstrate ability to develop ideas or higher level learning. Insufficient sources cited.

2. Submit one mid-term paper in response to a question posted by the professor. The question will be drawn from the materials covered in weeks 1-7. Students will respond to one question from a choice of two. Questions will be posted in the course materials as stated in the course calendar. Response papers must reflect research and reading undertaken by the student and will contain all sources and references. The response paper will be not less than 6 pages (excluding references). Papers are to be submitted in Arial Font 12. Footnoted and with Bibliography. Referencing is to be Numeric.
40 points of total grade for class

Level of Achievement	Midterm Points	Comprehension
Very Good Pass	35-40pts	Demonstrates complete understanding of the issue/s. Supports position with numerous, relevant sources. Backs argument with justifications and authority. Uses informed ideas to support conclusion. Clear evidence of critical discussion. No errors.
Good Pass	30-34pts	Demonstrates an adequate understanding of the issue. Uses minimum number of sources to back position. Limited number of ideas utilized to support conclusion. Overall less engaging and thorough than an a Very Good Pass.
Adequate to Pass	24-29pts	Does not demonstrate an accurate understanding of issue/s. Makes minimum effort to use sources and data. Does not demonstrate informed ideas that illuminate the answers but makes an effort.

Deficient	23 or below	Inaccuracies. Minimal effort demonstrated. Does not demonstrate ability to develop ideas or higher level learning. Insufficient sources cited.

3. Submit one final paper in response to a question posted by the professor. The question will be drawn from the materials covered throughout the course. Students will respond to one question from a choice of two. Questions will be posted in the course materials as stated in the course calendar. Response papers must reflect research and reading undertaken by the student and will contain all sources and references. The response paper will be not less than 8 pages (excluding references). Papers are to be submitted in Arial Font 12. Footnoted and with Bibliography. Referencing is to be Numeric.

50 points of total grade for class

Level of Achievement	**Final Paper Points**	**Comprehension**
Very Good Pass	45-50pts	Demonstrates complete understanding of the issue/s. Supports position with numerous, relevant sources. Backs argument with justifications and authority. Uses informed ideas to support conclusion. Clear evidence of critical discussion. No errors.
Good Pass	40-44pts	Demonstrates an adequate understanding of the issue. Uses minimum number of sources to back position. Limited number of ideas utilized to support conclusion. Overall less engaging and thorough than an a Very Good Pass.
Adequate to Pass	30-39pts	Does not demonstrate an accurate understanding of issue/s. Makes minimum effort to use sources and data. Does not demonstrate informed ideas that illuminate the answers but makes an effort.
Deficient	29pts or below	Inaccuracies. Minimal effort demonstrated. Does not demonstrate ability to develop ideas or higher level learning. Insufficient sources cited.

Grades:
A 180-200 points
B 160-179.99 points
C 140-159.99 points
D 120-139.99 points
F Below 120 points

Grades and feedback will be returned no later than one week after the due date of a discussion or assignment. During busy times of the semester it may take longer, but I will notify the class by announcement if more time is required.