BOR6342: Cybersecurity and Constitutional Issues

Course Description/Overview

This course examines the scope of cybercrime and its impact on today's system of criminal justice. Topics to be studied include: cybercrime and the Bill of Rights, computer-based economic crime, electronic commerce, ethical challenges, and the Computer Fraud and Abuse Act. Included will be an analysis of the legal considerations facing law enforcement and cybersecurity professionals who deal with the problems of discovering, investigating, and prosecuting cybercrime.

Course Bibliography and Required Readings:

Digital Evidence and Computer Crime (3rd edition)
Author: Casey, Eoghan
Date: 2011
ISBN (hard cover): 978-0-12-374268-1

There is no electronic version at this time. Relatively inexpensive copies may be acquired from online booksellers.

Course Objectives/Learning Outcomes

Students will gain knowledge about the way in which cybersecurity, and the computer itself, has affected - and has been affected by - the criminal justice system, law enforcement professionals, and the community-at-large.

More specifically, it is expected that each student will:

Objective One: Become conversant with terminology of the world of "cyberspace, "with emphasis on terms and concepts pertinent to the application of computerization within the criminal justice system.

Objective Two: Be able to discuss the impact that specific security issues related to cybertecbnology have had on the criminal justice system in particular, and upon modem society in general, in the context of past, present, and future developments.

Objective Three: Be able to identify and analyze provisions of the United States Constitution, with special emphasis on The Bill of Rights, which underlie the basis upon which the criminal justice system must deal with "cybercrime, "and those who commit such criminal acts.

Objective Four: Be able to distinguish the particular attributes of a computer-based economic system which tend to facilitate fraud and other criminal acts by those with criminal intent.

Objective Five: Be able to compare and contrast and, more significantly, understand those efforts undertaken by the Legislative and Executive branches of both state and federal government to thwart crimes facilitated by or, in some instances, only made possible by the use of computers.

Objective Six: Be able to trace the history of development of the law enforcement community's efforts at policing the unlawful use of computers.

Objective Seven: Be able to identify the ethical challenges to be considered by those within the law enforcement field who are working to thwart cybertech crime.

Objective Eight: Be able to anticipate changes in laws and legal procedures that may likely occur as the criminal justice system attempts to forestall further incursions by deviants into the world of cybertech security.

Grading Policies

This course uses weekly discussions to measure the student's comprehension of the presented materials. There is an extensive amount of reading assigned that will drive student responses to discussion questions and the student should be prepared to spend upwards of six (6) hours each week on this course. Additionally, where possible, videos are utilized to enhance student learning.

Assignment	Percent of Grade	Due
Participation in the Discussion Board	100%	Weekly Your initial post are due by 11:59 P.M. CST Saturday, of each week. Respond to at least 2 posts from other students due by 11:59 P.M. CST Sunday, the end of each week. A robust posting of 250-300 words is expected in your initial discussion thread. Your posting will be graded using the Discussion Rubric.

Angelo State University employs a letter grade system. Grades in this course are determined on a percentage scale:

A = 90 – 100 %
B = 80 – 89 %
C = 70 – 79 %
F = 59 % and below.

Rubrics

Discussion forums will be graded using a standardized rubric. It is recommended that you be familiar with these grading criteria and keep them in mind as you complete the writing assignments. There are two rubrics. Click the link to download the PDF document:

Discussion Rubric

Course Organization:

Module 1: **Computer Basics for Digital Investigators**)
This lesson is designed to develop a basic understanding of how computers operate and how data is

stored is a fundamental skill for forensic examiners. This includes understanding and controlling the boot process, recovering data, and analyzing data.

Network Basics for Digital Investigators
All digital investigators require some understanding of networks since most computers we encounter are connected to one. In fact, computers have become network-centered and it is no longer sufficient to only think of digital evidence on storage media. To comprehend traces of Internet activities left on personal computers and to establish continuity of offense, digital investigators require knowledge of evidence that exists on surrounding networks. These sources include server logs, network devices, and traffic on both wired and wireless networks.

Module 2: **Language of Computer Crime Investigation**
Since the late 1980s there have been significant advances in investigating crime involving computers. In addition to advances in tool development, there have been refinements in the law, computer crime categories, and digital investigative methods and theory. However, because it is still an emerging field, cybersecurity requires additional development and refinement.

Cybercrime Law
This lesson contains a significant amount of material that can form the foundation for more than one lesson. The ultimate aim is to have students compare the policies and laws in the US and EU, and highlight the similarities and differences between them in the following areas: •Fraud, forgery, intrusions, and other computer abuse •Child pornography •Privacy •Search and seizure •Jurisdiction

Module 3: **Foundations of Digital Forensics**
It is easy to get lost in the maze of terms and technology of cybersecurity. To make the case for digging into it and learning how to gather and preserve evidence, watch the video by clicking (shift-click) on the icon at the left. This is a case of evidence concerning child pornography involving teacher's aid in Brooklyn NY

Digital Evidence in the Courtroom
The foundation of a case involving digital evidence is proper evidence handling from proper practices of seizing, storing, and accessing evidence, and verification that evidence was properly handled. It is important to emphasize that digital investigators will be presenting their findings to a non- technical audience. Therefore, is imperative that digital investigators are able to convey complex concepts in easier to understand terms.

Module 4: **Conducting Digital Investigations**
Your text present a twelve-step model for the investigative process. Following these twelve steps will increase the likelihood that an investigation will lead to the truth and will serve justice. More specifically, the ultimate aim of the model covered in this lesson is to help investigators ascend a sequence of steps that are generally accepted, reliable, and repeatable, and lead to logical, well-documented conclusions of high integrity.

Modus Operandi, Motive, and Technology
Investigatory reconstruction provides a methodology for gaining a better understanding of a crime and focusing an investigation. Objectively reviewing available evidence provides a greater understanding of the case..

Module 5: **Violent Crime and Digital Evidence**
You should understand that technology, for the most part, is not inherently good or bad – it simply is. It is the application of that technology that is important. Criminals are quick to see how a new technology can be adapted to their purposes. The forensic examiner's job is to analyze that new technology, first of all to see how the technology was implemented, and second of all to determine if the technology has any value as a tool in a forensic investigation.

Digital Evidence as Alibi

With people spending an increasing amount of time using mobile devices, computers, and networks, there are bound to be more alibis that depend on digital evidence. Digital evidence will rarely show that someone was at a specific location at a specific time; however, it can show that the device was at that location. Through the use of other supporting evidence, such as a phone call in progress or an e-mail sent, the device can be associated with an individual.

Module 6:

Computer Intrusions

Just as a company's most valuable assets may be the data on its computers, failure to protect those assets may result in financial loss, regulatory sanctions, and reputational harm. More than one company has been forced into bankruptcy when the computer containing their company information crashed. A common truth is that criminals tend to steal things of value. Therefore, a company's information may be a target.

Applying Forensic Science to Computers

Computer technology continues to evolve rapidly but the fundamental components have changed little. Because processes at the top level have not changed rapidly, it is both possible and reasonable to develop SOPs to be used in the field.

Module 7:

Applying Forensic Science to Networks

As discussed in earlier lessons, when handling digital evidence it is necessary to establish chain of custody, document the state of items in situ, and take other steps to preserve the evidence so that it can be authenticated at a later date.

Digital Evidence on the Internet

The Internet is both an attractive venue for criminal activities and a powerful investigative tool. This lesson discusses both aspects to give investigators intelligence about how criminals operate online, and to help investigators use digital evidence on the Internet to apprehend offenders. The main Internet services are covered, including the Web, e-mail, newsgroups, Internet chat, and P2P. New services are emerging that extend the capabilities of the Internet, providing criminals with new opportunities, and making digital investigations more challenging. Therefore, in addition to becoming familiar with existing Internet services, students need to learn how to explore new technologies from an evidentiary and investigative viewpoint, as well as from a criminal viewpoint.

Module 8:

Digital Evidence on Physical and Data-Link Layers

This lesson expands on the overview provided in lesson 3, describing network technologies in more detail, focusing on Ethernet. Tools and techniques for preserving, examining, and analyzing network traffic are presented.

Digital Evidence at the Network and Transport Layers

This lesson expands on the overview provided in lesson 3, describing TCP/IP in more detail and demonstrating the usefulness of IP addresses in investigations. Because TCP/IP forms such an integral part of the Internet, information related to these layers are too numerous to describe individually. The glue that holds a network together gets stuck in many places for digital investigators to recover. Case examples are provided to improve students' familiarity with the many types of evidence that contain data relating to the transport and network layers.

Communication

Participation

In this class ***everyone***, brings something to the table. Your ideas and thoughts do count, not only to me, but the entire class. Feel free to ask questions either via e-mail or the discussion board. **Check the discussion board regularly.**

Many student questions are applicable to the class as a whole, as are the responses. You may be surprised how many of your classmates have the same questions and concerns as you. I may simply post your particular question on the discussion board and allow your classmates to provide the answer through their own posts.

To some, this may be their first online class and naturally, it could seem somewhat intimidating. As a class, we are together to help each other with this learning process and share our collective knowledge on how best to communicate; how to resolve technical issues that may arise (if we have the expertise), and to assist each other to find answers to our questions.

We will learn and work as a team.

Courtesy and Respect

Courtesy and Respect are essential ingredients to this course. We respect each other's opinions and respect their point of view at all times while in our class sessions. The use of profanity & harassment of any form is strictly prohibited (Zero Tolerance), as are those remarks concerning one's ethnicity, life style, race (ethnicity), religion, etc., violations of these rules will result in immediate dismissal from the course.

Office Hours/Contacting the Instructor

See the Instructor Information section for contact information.

University Policies

Academic Integrity

Angelo State University expects its students to maintain complete honesty and integrity in their academic pursuits. Students are responsible for understanding and complying with the university Academic Honor Code and the ASU Student Handbook.

Accommodations for Disability

ASU is committed to the principle that no qualified individual with a disability shall, on the basis of disability, be excluded from participation in or be denied the benefits of the services, programs or activities of the university, or be subjected to discrimination by the university, as provided by the Americans with Disabilities Act of 1990 (ADA), the Americans with Disabilities Act Amendments of 2008 (ADAAA), and subsequent legislation.

Student Affairs is the designated campus department charged with the responsibility of reviewing and authorizing requests for reasonable accommodations based on a disability, and it is the student’s responsibility to initiate such a request by emailing studentservices@angelo.edu, or by contacting:

Office of Student Affairs
University Center, Suite 112
325-942-2047 Office
325-942-2211 FAX

Student absence for religious holidays

A student who intends to observe a religious holy day should make that intention known in writing to the instructor prior to the absence. A student who is absent from classes for the observance of a religious holy day shall be allowed to take an examination or complete an assignment scheduled for that day within a reasonable time after the absence.