MASTER'S DEGREE IN CYBERSECURITY

Cyber Intelligence Concentration Course Guide

CORE COURSES (12 CREDIT HOURS)

Information Security & Risk Management
(3 Credit Hours)

Recent years have seen an unfortunate and disruptive growth in the number of cyber-attacks. To help curb this major societal issue, there has been an increase in calls for well-trained cybersecurity professionals. However, individuals often lack key skills such as planning/implementing/upgrading/monitoring emerging technologies, incident response, security controls and basic systems administration. Moreover, candidates often lack the non-technical skills of researching and reading new technologies, regulatory compliance, internal security policies, standards and procedures. This hands-on, introductory course is backward engineered with DHS/NSA key knowledge unit requirements for maintaining the Center for Academic Excellence for Cyber Defense (CAE-CD) and aims to alleviate these concerns and help students become excellent candidates in the field. Course topics include the importance of information security and related business concerns;
key definitions and terminology for information security; major categories of information security threats; common information security controls; implementing the basic information security controls; legal provisions regarding information security and the methodological implications for INFOSEC arising from these legal provisions; standard methodologies for complying with legal requirements for IT general controls; and IT risk management in organizations. Students will develop valuable skills, such as critical thinking, currently in demand for cybersecurity professionals. Upon completion of this course, students will have a strong foundation for advanced studies, including cybersecurity certifications such as Certified Ethical Hacker (CEH), Certified Information Security Manager (CISM), Security+, Certified Information Systems Security Professional (CISSP) and SANS GIAC Security Essentials (GSEC).

Special Topics: Applied Cryptography
(3 Credit Hours)

Cryptography is the art and science of securing information in a broad sense. It includes not only the design and analysis of methods for data encryption to ensure confidentiality but also the solutions for authentication, secure distributed computation and more. This course provides an overview of applied cryptography. It introduces the necessary mathematical tools of applied cryptography and shows how they are applied to design algorithms and protocols to secure information. The course starts with a review of mathematical foundations of cryptography, focusing on number theory, probability and statistics. Then, an overarching applied framework of principles for secure system design will be provided. This course also will introduce the applied context of cybersecurity and describe the nature of attacks against networks and systems, along with the history and modern concepts of cryptography. In the discussion of symmetric encryption, you will learn about the difference between stream and block ciphers. You will also see examples of asymmetric encryption schemes, hash functions, digital signature schemes and key establishment protocols. The course concludes by considering how these concepts are applied in practice, such as in public-key infrastructures and in IPSec. The course concludes with a brief introduction to the use of firewalls and intrusion detection systems. Software used includes VirtualBox, Hex Editor and OpenSSL.

Phone: (813) 974-7899 | Email: Tyoung6@usf.edu
4202 E. Fowler Ave., LIB608, Tampa, FL 33620

UNIVERSITY of SOUTH FLORIDA

MASTERS DEGREE IN CYBERSECURITY

Cyber Intelligence Concentration Course Guide

Data Network, Systems and Security

(3 Credit Hours)

The goal of this course is to provide a technical introduction to data networks. The course is comprised of a series of modules and will include projects, quizzes and a final exam. The course will start with an overview of database management and operating system technologies, which are critical to network operation and security. Key concepts and technologies in data networks will then be introduced, including layered architectures and topologies. The main elements in information technology networks will then be detailed, including routers, switches, gateways, servers, workstations and storage devices. Monitoring tools and protocols also will be covered, including data transport and addressing. The course will then look at network management and performance optimization, as well as troubleshooting and congestion control. Finally, network security topics will be covered, including encryption, authentication, firewalls and intrusion detection, security management tools and threat scenarios. This material will provide a basis for learning how to install, configure, maintain, upgrade and troubleshoot networks.

Decision Processes for Business Continuity and Disaster Recovery

(3 Credit Hours)

This course introduces students to decision making and risk assessment skills to plan for and respond effectively to disasters affecting our information systems and critical infrastructures with the goal of maintaining business continuity. Course objectives will be accomplished by helping students develop quantitative skills and frameworks to make decisions and assess risks and apply these skills in the service of protecting critical infrastructure. Students will use @Risk by Palisade, an advanced risk analysis software using Monte Carlo simulation, Microsoft Excel and Microsoft Project.

CONCENTRATION COURSES (18 CREDIT HOURS)

Advanced Professional & Technical Communication for Analysts

(3 Credit Hours)

This course will introduce students to a specific writing style, the one preferred in the U.S. Intelligence Community (IC) and by other U.S. government agencies. Students will learn techniques for conducting research and identifying credible sources, organizing large amounts of information, proofreading, and writing clearly, concisely and correctly. Fundamentals of English grammar, such as good sentence structure, correct punctuation and the development of coherent arguments, are topics highlighted in this course. Written exercises will focus on writing concise and focused information reports and other types of documents commonly used in the IC. This "problem-based learning" course will enhance students' ability to effectively communicate – in written products and oral briefings – the results of detailed intelligence/information analytic work.

Information Strategy and Decision-Making

(3 Credit Hours)

This course focuses on the human dimensions of analytic and strategic thought. It explores the complexity of human judgment and cognition and their roles in analyzing information. Students will examine analytic methodology as a form of problem-solving – a process of matching "data" and approaches to specific questions. The scientific method is used as an analogue for critical analysis, exploring how to generate and evaluate hypotheses in everyday life, how to understand the relative merits and limitations of qualitative and quantitative research methods, and how to apply statistical reasoning and inference to forecast outcomes. Finally, students will review a range of assessment methods and tools for structuring problems and evaluating courses of action.

Phone: (813) 974-7899 | Email: Tyoung6@usf.edu
4202 E. Fowler Ave., LIB608, Tampa, FL 33620

UNIVERSITY of SOUTH FLORIDA

MASTERS DEGREE IN CYBERSECURITY

Cyber Intelligence Concentration Course Guide

Core Concepts in Intelligence
(3 Credit Hours)

This course broadly explores the nature, scope and function of "intelligence" and specifically reviews the organization, activities and procedures of the U.S. Intelligence Community. It begins with a look at the history of intelligence, how it is defined and how it is used. It reviews the 17 agencies comprising the U.S. Intelligence Community and their roles, along with the operation of legislative intelligence oversight committees. It highlights some of the most common and pressing ethical issues in intelligence analysis and operations, then describes in detail the processes of intelligence planning, collection and analysis. Finally, issues of counterintelligence and security are introduced.

Advanced Intelligence Analytic Methods
(3 Credit Hours)

This course will provide a foundation for analytic and quantitative reasoning. It focuses on advanced, applied skills for problem analysis, problem solving and decision making. It is designed to help the student apply the rigor of the scientific method to strategy and information analysis. The course will draw on the decision sciences to teach students about the strengths and limitations of human judgment and decision making and in algorithmic models and simulations, and how to mitigate the impact of bias in each. Students will also be introduced to several structured analytic techniques commonly used in intelligence analysis.

Advanced Cyber Intelligence
(3 Credit Hours)

Prerequisite: Cyber Intelligence

This course builds on the foundations of Cyber Intelligence and focuses on applying intelligence analytic methods to plan, collect, process, analyze, produce and disseminate cyber intelligence products. Students will learn to apply intelligence analytic methods to create actionable intelligence products that support a cybersecurity mission.

Cyber Intelligence
(3 Credit Hours)

This course builds a foundation for understanding how cyber intelligence and counterintelligence can support cybersecurity and contribute more broadly to an enterprise or national security mission. It traces the history of cyber threats; evaluates the different forms of cyber conflict from hacktivism to cyber warfare; identifies and describes some of the key states and non-state actors posing a threat to cybersecurity; describes what is currently known about "insider threats" to information systems; examines how espionage (national and corporate) is evolving in the cyber realm; reviews research on cyber behavior and its implications for the "human dimension" of cybersecurity; and explores how to integrate technical, social and strategic data in cyber threat analysis.

PRACTICUM (3 CREDIT HOURS)

Supervised Field Work
(3 Credit Hours)

The MS in Cybersecurity curriculum requires 3 credit hours of "experiential learning" or a practicum that allows students to apply knowledge from their program and to critically consider and address issues relevant to the cybersecurity field. Students will produce and submit a tangible outcome or artifact to document their experience. This can be in the form of an internship report, an essay, an assessment report, an app or any other concrete outcome.

Phone: (813) 974-7899 | Email: Tyoung6@usf.edu
4202 E. Fowler Ave., LIB608, Tampa, FL 33620

UNIVERSITY of SOUTH FLORIDA