College of Information Science

Master of Science in Cyber & Information Operations
Course Rotation Chart

Semesters Typically Offered (Subject to change):

Course	Fall	Spring	Summer
CYBV 500: Security Programming	**7-week 1**	**7-week 1**	**7-week 1**
CYBV 501: Principles of Cybersecurity	**7-week 1**	**7-week 1**	**7-week 1**
CYBV 523: Covert Python	**7-week 2**	**7-week 2**	**7-week 2**
CYBV 525: Cyber-Physical Systems	**7-week 1**		
CYBV 528: Operational Tradecraft in the Information Environment		**7-week 1**	
CYBV 529: Cyber Law, Ethics and Policy	**7-week 2**	**7-week 2**	**7-week 2**
CYBV 535: Secure Critical Infrastructures with Artificial Intelligence	**7-week 2**		
CYBV 579: Cloud Security	**7-week 1**	**7-week 1**	**7-week 1**
CYBV 626: Traffic Analysis	**7-week 1**	**7-week 1**	**7-week 1**
CYBV 660: Zero Trust Defensive Techniques	**7-week 2**	**7-week 2**	**7-week 2**
CYBV 680: Information Warfare		**7-week 2**	
CYBV 685: Advanced Computational Propaganda	**7-week 2**	**7-week 2**	**7-week 2**
CYBV 909: Master's Report in Cyber & Information Operations	**13 weeks**	**15 weeks**	**15 weeks**
CYBV 910: Master's Thesis in Cyber & Information Operations*	**13 weeks**	**15 weeks**	**15 weeks**

CYBV 910 only offered if needed for a graduating thesis student
****NOTE: Courses are offered in 7 ½ week format unless notated as a 13/15-week course****

Course Descriptions

CYBV 500: Security Programming
Advances the concepts and principles of development of practical applications supporting cybersecurity and digital investigation activities created through Python programming. Students will build on programming fundamentals using Python elements, secure programming standards, and developing applications for cybersecurity. Examining application requirements students will develop, debug, execute, and deploy Python scripts.

CYBV 501: Principles of Cybersecurity
Advances the concepts and principles of cybersecurity across different disciplines, threats, and technologies. Exposes foundational knowledge and importance of Confidentiality, Integrity, and Availability (CIA Triad) concerning threats, vulnerabilities, and controls. Students will examine cybersecurity attackers' techniques, skills, motives, and vulnerabilities within programming, operating systems, networks, data, and web interfaces.

CYBV 523: Covert Python
This course examines cyber and intelligence operations that employ the black arts of covert communications, steganography, and data hiding that criminals and terrorist organizations use to carry out their operations. The course explores historical cases and recent cyber-attacks and intelligence operations that employ covert communications, steganography, and advanced data exfiltration methods. Students will use a host of python scripts to detect and disrupt these operations along with the examination and development of advanced offensive covert communication concepts.

CYBV 525: Cyber-Physical Systems
This is a graduate-level course that delves deeply into Cyber-Physical Systems (CPS) with a strong emphasis on security. Cyber-Physical Systems (CPS) integrate computation, communication, and control into physical processes. Students will explore topics in CPS design, modeling, analysis, and security while also developing essential research skills. Topics include the interaction between cyber and physical components, system architecture, security threats, and mitigation strategies.

CYBV 528: Operational Tradecraft in the Information Environment
Students explore the principles, strategies, and techniques involved in operating within the information environment by examining the role the information environment has in shaping public opinion, influencing decision-making, and conducting various operations. This masters level course is designed to provide students with a comprehensive understanding of deception, counter-deception, counterintelligence, and psychological operations and the strategies, techniques, and tactics employed in the cyber domain to operate effectively within the information environment.

CYBV 529: Cyber Law, Ethics and Policy
CYBV529 will provide students with an advanced look at the ethical, legal, and policy issues that arise in the field of cyber and technology. A variety of ethical, legal and policy issues both from history and current events will be presented. Students will gain the knowledge to operate in the current cyber and technology landscape, and the tools to analyze and respond to issues in this complex and evolving landscape.

CYBV 535: Secure Critical Infrastructures with Artificial Intelligence
This course delves into the application of Artificial Intelligence (AI) and Machine Learning (ML) to enhance the security of critical infrastructures. As our reliance on modern intelligent systems, advanced cellular communications, vehicular networks, satellite communications, and other cyber-physical systems grows, the need for robust security measures becomes paramount. This course provides an in-depth exploration of how AI and ML can be harnessed to safeguard these vital systems. Topics include threat intelligence, intrusion detection, malware detection, and the protection of generative AI and large language models.

CYBV 579: Cloud Security
This course provides an in-depth study of the theory and best practice application of cloud security. Topics include platform,

infrastructure and application security; cloud security operations; cloud governance, risk, and compliance management; cloud vulnerability assessment and penetration testing; cloud digital forensics and incident response management. The course also analyzes the application of SecDevOps/DevSecOps principles across the spectrum, including container security and the concept of "Shifting Security Left," whereby security testing and validation are introduced earlier in the software development life cycle.

CYBV 626: Traffic Analysis
This course examines the methods by which today's security protocols and their implementations are deemed secure and reliable. Students work to identify the mechanisms that make communications systems secure and consider how to assess the effectiveness of existing controls. The course takes a forward-looking approach and challenges students to consider problems such as the realization of quantum cryptography and the continued expansion of the Internet of Things (IoT). Students will examine and research methods for quantifying the level of protection provided by existing protocols, including formalized approaches to this type of assessment.

CYBV 660: Zero Trust Defensive Techniques
This course explores the implementation of Zero Trust Architecture (ZTA) principles in a legacy network. Students will address the quantification of effectiveness as ZTA is incrementally implemented in design and architecture, then proceed to addressing cloud data security, cloud platform and infrastructure security, cloud application security, cloud security operations, cloud risk management and compliance management. ZTA guidelines set forth by the National Institute of Standards and Technology (NIST), Center for Internet Security (CIS), industry accepted best-practices, and data-driven applications in cybersecurity will be leveraged through this course.

CYBV 680: Advanced Computational Propaganda
Computational propaganda is a form of manipulation that targets political, social, economic, environmental, and religious issues leveraging social media platforms. The perpetrators use fake personas, automated bots, artificial intelligence algorithms and large data to manipulate public opinion. Students will examine the fundamentals of both propaganda and the automation of propaganda using advanced computational methods. Students will research the history of propaganda and the methods used to manipulate subjects. Leveraging what students have learned during the creation of computational propaganda, students will then turn the tables and develop methods to identify and uncover computational propaganda within social media platforms.

CYBV 685: Information Warfare
CYBV 685 will provide students with an in-depth examination of information warfare and how it is the driving force behind the emergence of a new fifth generation of warfare (5GW). Students will learn how the control, manipulation, and amplification of narratives within social media and cyberspace is used to shift public opinion and achieve strategic goals. An extensive analysis of real-world case studies combined with interactive practical exercises will be used to help students master the principles of cognitive maneuver and how it is applied in hybrid, irregular, and unrestricted warfare.

CYBV 909: Masters Report in Cyber & Information Operations
Individual study or special project or formal report thereof submitted in lieu of thesis.

CYBV 910: Masters Thesis in Cyber & Information Operations
Research for the master's thesis (whether library research, laboratory or field observation or research, artistic creation, or thesis writing).