Cybersecurity (CYBER)

Courses

Please note: CYBER courses are only available for Information and Cybersecurity (MICS) students.

CYBER 200 Beyond the Code: Cybersecurity in Context 3 Units

Terms offered: Summer 2025, Spring 2025, Fall 2024
This course explores the most important elements beyond technology that shape the playing field on which cybersecurity problems emerge and are managed. The course emphasizes how ethical, legal, and economic frameworks enable and constrain security technologies and policies. It introduces some of the most important macro-elements (such as national security considerations and interests of nation-states) and micro-elements (such as behavioral economic insights into how people understand and interact with security features). Specific topics include policymaking, business models, legal frameworks, national security considerations, ethical issues, standards making, and the roles of users, government, and industry.

Rules & Requirements

Prerequisites: MICS students only

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of lecture per week

Summer: 14 weeks - 3 hours of lecture per week

Additional Details

Subject/Course Level: Cybersecurity/Graduate

Grading: Letter grade.

Formerly known as: Information and Cybersecurity W200

CYBER 202 Cryptography for Cyber and Network Security 3 Units

Terms offered: Summer 2025, Spring 2025, Fall 2024
This course focuses on both mathematical and practical foundations of cryptography. The course discusses asymmetric and symmetric cryptography, Kerchkoff's Principle, chosen and known plaintext attacks, public key infrastructure, X.509, SSL/TLS (https), and authentication protocols. The course will include an in-depth discussion of many different cryptosystems including the RSA, Rabin, DES, AES, Elliptic Curve, and SHA family cryptosystems. This course also introduces advanced topics of applied cryptography, including a brief introduction to homomorphic encrypted computation and secure multi-party computation to protect sensitive data during arbitrary computation, cryptocurrency and its cryptographic building blocks, and quantum computing.

Rules & Requirements

Prerequisites: MICS students only. CYBER 206

Credit Restrictions: Students will receive no credit for CYBER W202 after completing CYBER 202. A deficient grade in CYBER W202 may be removed by taking CYBER 202.

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of lecture per week

Summer: 14 weeks - 3 hours of lecture per week

Additional Details

Subject/Course Level: Cybersecurity/Graduate

Grading: Letter grade.

Formerly known as: Information and Cybersecurity W202

CYBER 204 Software Security 3 Units

Terms offered: Summer 2025, Spring 2025, Fall 2024
The course presents the challenges, principles, mechanisms and tools to make software secure. We will discuss the main causes of vulnerabilities and the means to avoid and defend against them. The focus is on secure programming practice, including specifics for various languages, but also covering system-level defenses (architectural approaches and run-time enforcement). We will also apply software analysis and vulnerability detection tools in different scenarios.

Objectives & Outcomes

Course Objectives: *Apply and manage secure coding practices throughout software project development

*Gain a good comprehension of the landscape of software security vulnerabilities, with specifics for various programming languages and types of software applications

*Gain the ability to analyze the security of a software system and convincingly advocate about the significance of vulnerabilities

*Know representative tools for software security analysis and testing, use them in practice and understand their capabilities and limitations

*Recognize insecure programming patterns and know how to replace them with secure alternatives

Student Learning Outcomes: Students will be able to apply and manage secure coding practices throughout software project development
Students will be able to recognize insecure programming patterns and know how to replace them with secure alternatives
Students will gain a good comprehension of the landscape of software security vulnerabilities, with specifics for various programming languages and types of software applications
Students will gain the ability to analyze the security of a software system and convincingly advocate about the significance of vulnerabilities
Students will know representative tools for software security analysis and testing, use them in practice and understand their capabilities and limitations

Rules & Requirements

Prerequisites: MICS students only. CYBER 206

Credit Restrictions: Students will receive no credit for CYBER W204 after completing CYBER 204. A deficient grade in CYBER W204 may be removed by taking CYBER 204.

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of lecture per week

Summer: 14 weeks - 3 hours of lecture per week

Additional Details

Subject/Course Level: Cybersecurity/Graduate

Grading: Letter grade.

Formerly known as: Information and Cybersecurity W204

CYBER 206 Mathematics and Programming for Cybersecurity 3 Units

Terms offered: Summer 2025, Spring 2025, Fall 2024
This course is designed to provide students with the foundational math and programming skills required to be successful in the Master of Information and Cybersecurity (MICS) program. Upon completion of this course, students will be able to write programs in Python and will gain experience reading and interpreting C programs. Students will receive a comprehensive overview of algebraic principles and will explore quantitative concepts needed for cryptography. Additionally, this course will prepare students to apply logical thinking and decompose complex problems to create programmatic solutions.

Objectives & Outcomes

Student Learning Outcomes: Apply algebraic rules to evaluate functions and solve equations.
Decompose a discrete math problem into a computer program.
Demonstrate a working knowledge of basic programming skills to include setup and use of integrated development environments, applied Python, and comprehension of programs written in C.

Rules & Requirements

Prerequisites: MICS students only

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of lecture per week

Summer: 14 weeks - 3 hours of lecture per week

Additional Details

Subject/Course Level: Cybersecurity/Graduate

Grading: Letter grade.

Formerly known as: Information and Cybersecurity W206

CYBER 207 Artificial Intelligence (AI) and Machine Learning (ML) in Cybersecurity 3 Units

Terms offered: Summer 2025, Spring 2025, Fall 2024
Artificial intelligence and machine learning is a rapidly growing field at the intersection of computer science and statistics concerned with finding patterns in data. It is responsible for tremendous advances in technology, from personalized product recommendations to speech recognition in cell phones. This course provides a broad introduction to the key ideas in machine learning, with a focus on applications and concepts relevant to cybersecurity. The emphasis will be on intuition and practical examples rather than theoretical results, though some experience with probability, statistics, and linear algebra will be important.
Objectives & Outcomes

Student Learning Outcomes: Direct their own learning in new and emerging machine learning tools and approaches by navigating API documentation and engaging in experimentation.
Demonstrate a familiarity with a wide range of concepts in the field of machine learning and neural networks in particular.
Demonstrate proficiency with existing coding languages (e.g., Python), packages related to machine learning (numpy, matplotlib, scikit-learn, and tensorflow), and the application of appropriate machine learning approaches for data science problems and questions.
Evaluate and implement simple machine learning solutions used in the context of security.
Understand and apply the concepts of machine learning using techniques and tools common in industry.

Rules & Requirements

Prerequisites: MICS students only. CYBER 206

Credit Restrictions: Students will receive no credit for CYBER W207 after completing CYBER 207. A deficient grade in CYBER W207 may be removed by taking CYBER 207.

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of lecture per week

Summer: 14 weeks - 3 hours of lecture per week

Additional Details

Subject/Course Level: Cybersecurity/Graduate

Grading: Letter grade.

Formerly known as: Information and Cybersecurity W207

CYBER 210 Network Security 3 Units

Terms offered: Summer 2025, Spring 2025, Fall 2024
Introduction to networking and security as applied to networks. Exercises cover network programming in a language of the student's choice, understanding and analyzing packet traces using tools like wireshark and mitmproxy, as well as applying security principles to analyze and determine network security. After this course, the student will have a fundamental understanding of networking, TLS and security as it applies to networked systems.
Rules & Requirements

Prerequisites: MICS students only. CYBER 206

Credit Restrictions: Students will receive no credit for CYBER W210 after completing CYBER 210. A deficient grade in CYBER W210 may be removed by taking CYBER 210.

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of lecture per week

Summer: 14 weeks - 3 hours of lecture per week

Additional Details

Subject/Course Level: Cybersecurity/Graduate

Grading: Letter grade.

Formerly known as: Information and Cybersecurity W210

CYBER 211 Operating System Security 3 Units

Terms offered: Summer 2025, Spring 2025, Fall 2024
This survey of operating system security compares approaches to security taken among several modern operating systems. The course will teach how to conceptualize design issues, principles, and good practices in securing systems in today’s increasingly diverse and complex computing ecosystem, which extends from things and personal devices to enterprises, with processing increasingly in the cloud. We will approach operating systems individually and then build on them so that students learn techniques for establishing trust across a set of interoperating systems.
Rules & Requirements

Prerequisites: MICS students only. CYBER 206

Credit Restrictions: Students will receive no credit for CYBER W211 after completing CYBER 211. A deficient grade in CYBER W211 may be removed by taking CYBER 211.

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of lecture per week

Summer: 14 weeks - 3 hours of lecture per week

Additional Details

Subject/Course Level: Cybersecurity/Graduate

Grading: Letter grade.

Formerly known as: Information and Cybersecurity W211

CYBER 215 Usable Privacy and Security Research 3 Units

Terms offered: Summer 2025, Spring 2025, Fall 2024

This course introduces students to both the theory and practice of designing user-centered privacy and security systems, with an emphasis on empirical research. You will learn to plan and conduct behavioral studies—ranging from lab and field experiments to interviews and surveys—that shed light on how users interact with privacy and security features. As part of the class, you will complete IRB training, design and run pilot studies, read and present classic papers in the field, analyze qualitative and quantitative data, and apply evidence-based insights to improve system usability. By the end of this course, you will gain practical skills for building more secure and privacy-protective software.

Objectives & Outcomes

Student Learning Outcomes: Develop skills for reading research papers, evaluating their findings, and identifying their limitations.
Identify human factors issues that impact the security and privacy of systems.
Improve communication, collaboration, and leadership skills through multiple assignments and class presentations.
Increase technical knowledge of various security domains through discussion and presentation of research findings in usable security and privacy.
Learn multiple experimental approaches to evaluating human factors issues in security and privacy.

Rules & Requirements

Prerequisites: MICS students only. CYBER 200

Credit Restrictions: Students will receive no credit for CYBER W215 after completing CYBER 215. A deficient grade in CYBER W215 may be removed by taking CYBER 215.

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of lecture per week

Summer: 14 weeks - 3 hours of lecture per week

Additional Details

Subject/Course Level: Cybersecurity/Graduate

Grading: Letter grade.

Formerly known as: Information and Cybersecurity W215

CYBER 220 Managing Cyber Risk 3 Units

Terms offered: Summer 2025, Spring 2025, Fall 2024

This course offers valuable perspective for both the non-technical business manager and the technical cybersecurity or IT manager. It is the vital connector between the technical world of threats, vulnerabilities, and exploits, and the business world of board-level objectives, enterprise risk management, and organizational leadership. Now more than ever, managers have a need and responsibility to understand cyber risk.
Just as financial risks and other operational risks have to be effectively managed within an organization, cyber risk has to be managed. It spans far beyond information technology, with broad implications in the areas of organizational behavior, financial risk modeling, legal issues, and executive leadership.

Objectives & Outcomes

Student Learning Outcomes: Compare and employ approaches to cyber risk management and measurement.
Develop a basic cybersecurity strategic plan and understand how it aligns with the core business value of the company.
Navigate corporate structures to create a strong cyber security program and obtain senior leadership buy-in.
Understand security product verticals, identify common use cases for those products, and define requirements for acquiring solutions relevant to a business use case.
Understand the basic principles and best practices of responding to a cybersecurity incident

Rules & Requirements

Prerequisites: MICS students only. CYBER 200

Credit Restrictions: Students will receive no credit for CYBER W220 after completing CYBER 220. A deficient grade in CYBER W220 may be removed by taking CYBER 220.

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of lecture per week

Summer: 14 weeks - 3 hours of lecture per week

Additional Details

Subject/Course Level: Cybersecurity/Graduate

Grading: Letter grade.

Formerly known as: Information and Cybersecurity W220

CYBER 233 Privacy Engineering 3 Units

Terms offered: Spring 2025, Fall 2024, Spring 2024

This course surveys privacy mechanisms applicable to systems engineering, with a particular focus on the inference threat arising due to advancements in artificial intelligence and machine learning. We will briefly discuss the history of privacy and compare two major examples of general legal frameworks for privacy from the United States and the European Union. We then survey three design frameworks of privacy that may be used to guide the design of privacy-aware information systems. Finally, we survey threat-specific technical privacy frameworks and discuss their applicability in different settings, including statistical privacy with randomized responses, anonymization techniques, semantic privacy models, and technical privacy mechanisms.

Objectives & Outcomes

Student Learning Outcomes: Students should be able to implement such privacy paradigms, and embed them in information systems during the design process and the implementation phase.
Students should be familiar with the different technical paradigms of privacy that are applicable for systems engineering.
Students should develop critical thinking about the strengths and weaknesses of the different privacy paradigms.
Students should possess the ability to read literature in the field to stay updated about the state of the art.

Rules & Requirements

Prerequisites: MICS students only. CYBER 206

Credit Restrictions: Students will receive no credit for CYBER W233 after completing CYBER 233. A deficient grade in CYBER W233 may be removed by taking CYBER 233.

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of lecture per week

Summer: 14 weeks - 3 hours of lecture per week

Additional Details

Subject/Course Level: Cybersecurity/Graduate

Grading: Letter grade.

Formerly known as: Information and Cybersecurity W233

CYBER 242 New Domains of Competition: Cybersecurity and Public Policy 3 Units

Terms offered: Spring 2025, Fall 2024, Summer 2024

Cybersecurity is a primary national security and public policy concern. The government, military and private sector have various roles and responsibilities with regard to the protection of the cyber domain. In this course, students critically evaluate these roles and responsibilities, the manner in which government networks, systems, and data are secured, and the ability of national and international cybersecurity strategies and partnerships to mitigate the security risks introduced by society's increased reliance on information.

Objectives & Outcomes

Course Objectives: Critically assess national and international cybersecurity strategies
Describe and evaluate national and international public-private partnerships.
Discuss the developments in the cyber domain and and its protection within the context of national security.

Identify lessons learned and recommend ways to improve national and international approaches to cybersecurity.
Identify the roles and responsibilities of the military, government, and the private sector in cybersecurity.
Utilize an evidence-based approach to analyze the security of government networks and systems and privacy of retained data.

Rules & Requirements

Prerequisites: MICS students only. CYBER 200

Credit Restrictions: Students will receive no credit for CYBER W242 after completing CYBER 242. A deficient grade in CYBER W242 may be removed by taking CYBER 242.

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of lecture per week

Summer: 14 weeks - 3 hours of lecture per week

Additional Details

Subject/Course Level: Cybersecurity/Graduate

Grading: Letter grade.

Formerly known as: Information and Cybersecurity W242

CYBER 252 Security Operations 3 Units

Terms offered: Summer 2025, Spring 2025, Fall 2024
This course will focus on understanding key areas within Security Operations from a management perspective. Upon completion of this course, students will understand implementation and maintenance best practices for security operations services such as incident response, internal investigations, security analysis, threat intelligence and digital forensics. Students will not only get hands-on experience within each discipline but will also understand how to recruit and train others within a security operations center or security team.
Objectives & Outcomes

Course Objectives: Demonstrate data analysis as it pertains to identifying and responding to cyber-attacks.
Effectively apply knowledge in simulated real-world conditions to protect and defend complex networks and infrastructures, including in the cloud.
Implement incident response and digital forensics techniques.

Rules & Requirements

Prerequisites: MICS students only. CYBER 200, CYBER 204, and CYBER 210

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of lecture per week

Summer: 14 weeks - 3 hours of lecture per week

Additional Details

Subject/Course Level: Cybersecurity/Graduate

Grading: Letter grade.

CYBER 284 Web Application Security Assessment 3 Units

Terms offered: Summer 2025, Spring 2025, Fall 2024
Web applications play a vital role in every modern organization. If an organization does not properly test its web applications to identify security flaws, adversaries may be able to compromise these applications damaging functionality and accessing sensitive data. The focus of this course is on developing practical web application security testing skills required to assess a web application's security posture and convincingly demonstrate the business impact of discovered vulnerabilities, if exploited. The course includes both lectures and a variety of demonstrations and hands-on exercises in finding web application security vulnerabilities. During the course, students learn about assessment tools and methodologies.
Objectives & Outcomes

Course Objectives: Develop skills in writing web application security assessment reports
Discover and exploit key web application flaws
Gain a good comprehension of web application security vulnerabilities
Learn to apply a repeatable methodology to deliver enterprise-level web application security assessment
Learn to explain potential impact of web application vulnerabilities

Rules & Requirements

Prerequisites: MICS students only. CYBER 204

Repeat rules: Course may be repeated for credit with instructor consent.

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of lecture per week

Summer: 14 weeks - 3 hours of lecture per week

Additional Details

Subject/Course Level: Cybersecurity/Graduate

Grading: Letter grade.

CYBER 289 Public Interest Cybersecurity: The Cybersecurity Clinic Practicum 3 Units

Terms offered: Summer 2025, Fall 2024, Spring 2024
This course provides students with real-world experience assisting politically vulnerable organizations and persons around the world to develop and implement sound cybersecurity practices. In the classroom, students study basic theories and practices of digital security, intricacies of protecting largely under-resourced organizations, and tools needed to manage risk in complex political, sociological, legal, and ethical contexts. In the clinic, students work in teams supervised by Clinic staff to provide direct cybersecurity assistance to civil society organizations. We emphasize pragmatic, workable solutions that take into account the unique needs of each partner organization.

Rules & Requirements

Prerequisites: MICS students only

Credit Restrictions: Students will receive no credit for CYBER W289 after completing CYBER 289. A deficient grade in CYBER W289 may be removed by taking CYBER 289.

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of lecture per week

Summer: 14 weeks - 3 hours of lecture per week

Additional Details

Subject/Course Level: Cybersecurity/Graduate

Grading: Letter grade.

Formerly known as: Information and Cybersecurity W289

CYBER 290 Special Topics 3 Units

Terms offered: Fall 2022, Summer 2022, Fall 2021
Specific topics, may vary from section to section, year to year.

Rules & Requirements

Prerequisites: MICS students only

Repeat rules: Course may be repeated for credit when topic changes. Students may enroll in multiple sections of this course within the same semester.

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of lecture per week

Summer: 14 weeks - 3 hours of lecture per week

Additional Details

Subject/Course Level: Cybersecurity/Graduate

Grading: Letter grade.

CYBER 295 Capstone 3 Units

Terms offered: Summer 2025, Spring 2025, Fall 2024
This capstone course will cement skills and knowledge learned throughout the Master of Information and Cybersecurity program: core cybersecurity technical skills, understanding of the societal factors that impact the cybersecurity domain and how cybersecurity issues impact humans, and professional skills such as problem-solving, communication, influencing, collaboration, and group management – to prepare students for success in the field. The centerpiece is a semester-long group project in which teams of students propose and select a complex cybersecurity issue and apply multi-faceted analysis and problem-solving to identify, assess, and manage risk and deliver impact.

Objectives & Outcomes

Student Learning Outcomes: Engage in a highly collaborative process of idea generation, information sharing, and feedback that replicates key aspects of managing cybersecurity in an organizational setting.
Learn or reinforce communication, influencing, and management skills.
Practice using multi-faceted problem-solving skills to address complex cybersecurity issues.

Rules & Requirements

Prerequisites: MICS students only. CYBER 200, CYBER 202, CYBER 204, CYBER 206, and CYBER 210. Must be taken in final term of the MICS program

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of lecture per week

Summer: 14 weeks - 3 hours of lecture per week

Additional Details

Subject/Course Level: Cybersecurity/Graduate

Grading: Letter grade.

Formerly known as: Information and Cybersecurity W295