**CYBR 610 Cyber Operations Management**

**Course Description**

The Cyber Operations Management course evaluates the current doctrine and planning procedures for strategies, policies, and case study reviews to successfully engineer, operate, and manage networks from small to global scale to protect from data theft, malware, intrusion attempts, and data leakage. This course will cover security operational design of the top level architecture security suite, internal network monitoring, data security, user training, and strategic best practices.

**CYBR 615 Strategic Cyber Intelligence**

**Course Description**

This course provides a comprehensive study of strategic cyber intelligence and organizational security. A focus on the strategic impact of audit and security requirements on the design and implementation of cyber security will be reviewed. Cyber warfare, both offensive and defensive, and their effects on critical infrastructure will also be a primary focus.

**CYBR 620 Legal Issues in Cyber Security**

**Course Description**

This course will review policy and legal concepts relating to cyber security and information management. It will examine laws, authorities, and the responsibilities of government and the private sector to protect data and privacy in the cyber domain. The course will provide the learner with the history and evolution of cyber laws and an analysis of terminology. The student will examine the ethical considerations of surveillance, cyber laws and policies.

Cyber law raises complex issues involving the characterization of acts (e.g., as a criminal matter or an act of war), and their attribution to responsible actors (e.g., individuals, non-state groups, and state actors) under domestic and international law. On one hand, an act might be characterized as a criminal matter in one jurisdiction, but not at the point of origin--raising issues for policymakers, lawyers and investigators. On the other hand, that same act could also be treated as economic espionage, terrorism or as an act of war--raising issues of international responsibility. In any case, the attribution problem raises technical and policy problems in identifying both the point of origin and the persons responsible for an event. Cyber practitioners must, therefore, have a general appreciation for the complex legal issues, to include the unsettled state of the law and the practical limitations in its application, often raised in addressing cybercrime.

**CYBR 625 Cyber Psychology**

**Course Description**

The course objectives stress three major topics: (1) the mindset and motivation of a hacker; (2) similarities and differences between the types of hackers-white, black and gray; and (3) technology and humans in terms of how human interaction affects cyber security.
CYBR 630 Offensive and Defensive Strategies

Course Description
Introduction to analytical software including data mining, statistical software, and analytical models are developed. The application of strategic analytics for predictive, trending, forecasting, intrusion, and prevention models of information management losses are proposed.

CYBR 635 Security and Information Data Analytics

Course Description
Introduction to analytical software including data mining, statistical software, and analytical models are developed. The application of strategic analytics for predictive, trending, forecasting, intrusion, and prevention models of information management losses are proposed.

CYBR 640 Strategic Investments in Information Security

Course Description
Various strategic financial models for the buy vs. build of security and information decision(s) is reviewed. Methods and techniques for fraud prevention, including operational risk assessment, fraud controls, data security, and compliance best practices and regulatory requirements are reviewed. Performance management processes, and information security program evaluations are analyzed in the context of building a portfolio of information technology investments.

CYBR 645 Enterprise Infrastructure Planning & Safeguarding

Course Description
An overview of strategic planning and safeguarding of enterprise level infrastructure is reviewed. Advanced planning methodologies are developed to adopt, implement, and manage technological ecosystems including software, hardware, networks, applications, data, communications, and other relevant infrastructure.
CYBR 650 Cyber Security Policy Implementation

Course Description
This course is designed to provide the knowledge and skills necessary to implement effective cyber security policy. The course investigates US domestic and foreign cyber security policy and how it affects cybercrime in the US. Main aspects of implementation covered in class will involve methods and guidelines for delivering cyber-security policy. The course addresses prototypical organizational goals in managing the development, maintenance, and replacement of cyber security policy. Students will engage in the use of the bottom up, top down, and the synthesis approach in implementing cyber security policy. The different arms of the government and how they approach cyber security implementation is also addressed.

CYBR 660 Cyber Capstone

Course Description
This capstone course integrates cyber security strategy, program management, leadership, and technological concepts. Graduate students will demonstrate the ability to effectively strategize, implement and sustain a Defense in Depth cyber security information management program. Students will be expected to synthesize security and information management research from a local and an international perspective of public and private agencies. The goal of this course is to encapsulate security theories and applications learned throughout the Masters in Cyber Security degree, by developing a strategic proposal demonstrating a security and information management strategy.