Cybersecurity (GI) - Online Graduate

GI 512 Foundations and Historical Underpinnings of Information Assurance 6 Cr.
This seminar explores the historical foundations of information assurance from the early days of mainframes to the foundations of today's sophisticated networks and distributed computing systems. It examines the earliest thinking about data structures and domains, interoperability between different computing platforms and mechanisms for data transfer and proceeds to the emergence of encryption as a defense against early forms of computer crime. This seminar looks at privacy, policies, and security standards and regulatory requirements. Finally, the seminar addresses the underlying models that define information assurance and takes a first look at IA architecture.

GI 522 Information Assurance Technology 6 Cr.
This seminar focuses on the use of technological defenses against threats and exploitations of vulnerabilities in information systems. Topics include physical security measures, access controls, security elements of operating systems, network security measures, anti-malware tools, anti-spam measures, anti-piracy systems, software development methods supporting security, and security certifications for software products.

GI 532 Human Factors and Managing Risk 6 Cr.
This seminar focuses on the ways that business objectives, user attitudes and user activities significantly influence both the development of an information assurance program and its successful implementation. The first week focuses on Operations Security and why it is the foundation for an IA program and the key to the program's effectiveness. The following five weeks explore security awareness as a component of organizational culture: crafting the information assurance message; understanding ethical decision- making as a factor in security; understanding social psychology and how behaviors will influence the effectiveness of security activities; using employment practices and policies to support information security; and creating Acceptable Use and e-mail policies. The final four weeks examine different elements of Risk Management from basic principles through application. The NIST Special Publication 800-30 provides a solid foundation for the risk management issues. Two popular risk assessment processes, and several other processes that help identify risk will be discussed.

GI 542 Information Assurance Management and Analytics 6 Cr.
This seminar is arranged in four general areas beginning with examining and exploring the strategic and gradually narrowing down to the tactical level: Compliance -> Management, Leadership, & Policy Development -> Relationships & Adding Value -> Project Management. The curriculum explores the aspects, methods, and alternatives in information assurance management and compares/utilizes them with respect to non-IT-related management approaches and styles. Additionally, it explores alternatives in building support and consensus for projects and activities and focuses heavily on adding value to the organization. Developing an information assurance marketing plan is examined and is used to help identify techniques of improving the information assurance awareness. Analytics are explored both in terms of metrics and measuring business impact and problem solving and project management techniques and alternatives are included.

GI 551 Computer Forensic Investigations 6 Cr.
This course focuses on the spectrum of tools and techniques used to investigate digital incidents whether in a civil or criminal environment. Information assurance professionals are expected to have a broad understanding of digital incidents, their management, investigation and analysis. This seminar provides that broad understanding and places it in the context of other information assurance domains. These discussions of digital investigation and forensics cover topics from both the technical and management perspectives. This coverage aids the information assurance professional's understanding and application of domain-specific knowledge.

GI 554 Computer Security Incident Response Team Management 6 Cr.
Students will analyze and apply the key points in creating and managing a computer security incident response team (CSIRT), also sometimes known as a computer incident response team (CIRT) or a computer emergency response team (CERT). Major topics include establishing CSIRTs; responding to computer emergencies; securing the CSIRT; managing the CSIRT with respect to professionalism, setting priorities for triage, and protecting personnel against burnout; and learning from emergencies using the incident postmortem and by establishing continuous process improvement within the organization. Students will use their case study to apply their knowledge to real-world situations and will prepare recommendations for establishment of a new CSIRT or improvement of their existing CSIRT.

GI 556 Cyber Crime 6 Cr.
This course explores the nature of conflict in cyber space focusing on two major internet-based threats to the U.S. national security: cyber terrorism and cyber crime. The course addresses questions like: who is undertaking these cyber activities, what techniques they use, and what countermeasures can be adopted to mitigate their impact. The course is built around a risk management framework to help information leaders leverage the benefits of Internet technologies while minimizing the risks that such technologies pose to their organizations.

GI 557 Cyber Law 6 Cr.
This course explores a broad variety of federal statutory, common, and international laws that may impact the information technology professional. Because the overwhelming majority of cyber infrastructure is owned and operated by the private sector, the course focus is on those laws that affect the interaction between government and the private sector information technology industry, including the privacy rights so often implicated in modern data storage systems. The seminar starts with a look at "cyber law" and whether it is really a distinct legal discipline at all. It then moves into criminal, civil, regulatory, international and common laws with which today's information technology professional may come in contact. Throughout the course we will discuss how public policy and other factors impact the development, implementation, and interpretation of the law. Students will read, interpret and apply legal authorities and theories, a valuable skill for future information technology leaders if they are to stay in compliance with the ever-growing "cyber" legal framework.

GI 562 Vulnerability Management and Penetration Testing I 6 Cr.
This course introduces students to the penetration testing of computer networks. This is the first of two courses that address Vulnerability Management. The core of this course is the basics of penetration testing. Students utilize a virtual lab to gain experience through hands-on lab exercises. Students learn to use the well-known open-source Metasploit computer security project to understand security vulnerabilities and how to use this tool for penetration testing, testing the control tools and how to conduct monitoring of an enterprise. In the course students are introduced to: system security and vulnerability analysis, the most common system exploits and vulnerabilities, system “pivoting” and client-side exploits. In this seminar students are introduced to open-source tools, in particular, the Metasploit Framework(MSF). Students learn how to assess enterprise security controls and system vulnerability and learn to document their findings. This course is designed for penetration testers, system security and network administrators.

GI 563 Vulnerability Management II 6 Cr.
This course introduces students to advanced open-source tools used to conduct penetration testing of computer networks. This is the second of two courses that address Vulnerability Management. Students learn the rules of engagement, and how to conduct legal and ethical security tests and vulnerability assessments. Students utilize a virtual lab to gain experience through hands-on lab exercises. Students learn to use the well-known open-source tools (Metasploit , John the Ripper, Wireshark) to understand security vulnerabilities and how to use this tool for penetration testing, testing the control tools and how to conduct monitoring of an enterprise. In the course students are introduced to: system security and vulnerability analysis, the most common system exploits and vulnerabilities, system “pivoting” and client-side exploits.

GI 566 Critical Infra. Protection 6 Cr.
This course examines the security of information in computer and communications networks within infrastructure sectors critical to national security. These include the sectors of banking, securities and commodities markets, industrial supply chain, electrical/smart grid, energy, transportation, communications, water supply and health. Special attention is paid to the risk management of information in critical infrastructure environments through an analysis & synthesis of assets, threats, vulnerabilities, impacts, and countermeasures. Critical consideration is paid to the role of Supervisory Control and Data Acquisition (SCADA) systems in the flow of resources such as electric, water, and fuel.

GI 567 International Perspectives on Cyberspace 6 Cr.
This course explores the concept of “cyber” and “cyberspace” from an international perspective. It starts with a look at the technical nature of the internet from its very beginning. It then moves on to explore the various threats facing all nations, including the various threat actors and their motivations, capabilities and intentions. The course then looks at how technical aspects of cyberspace complicate policing and monitoring of activities. Policies, both U.S. and international are explored next, including a look at the prospects for international cooperation. A look at cyberdeterrence and cyberwar follows, as well as a more detailed look into the cyber policies and activities of certain state and non-state actors.

GI 588 No Norwich Equivalent 6 Cr.

GI 595 Residency 0 Cr.