GLOBAL SECURITY, CONFLICT, AND CYBERCRIME (GSCC1-GC)

GSCC1-GC 1005 Cyber Law (3 Credits)
This course will focus on the international law applicable to cyber operations. The first part of the course will examine cybercrime, discussing international theories of jurisdiction, unique challenges of investigating transnational cybercrimes, and the core international crimes. The second part of the course will examine peacetime cyber operations. Sovereignty, the prohibition on intervention, the prohibition on the use of force, and the principle of due diligence will be examined, as well as lawful State responses to internationally wrongful cyber acts, such as retorsion, countermeasures, the plea of necessity and self-defense in response to a cyber armed attack. The third part of the course will examine cyber operations that occur during armed conflict. Focus will be made on cyber targeting and international humanitarian law, including the requirement of distinction, proportionality, the prohibition on indiscriminate attacks, and precautions in attack.
Grading: GC SCPS Graded
Repeatable for additional credit: No

GSCC1-GC 1010 National & International Cyber Organizations (3 Credits)
Public and private cybercrime investigations differ in terms of the crimes that are involved, who conducts the investigation, and how the investigation is conducted. This course provides an in- depth analysis of national and international public and private cybercrime investigations: looking in particular at how they are conducted, formal and informal information sharing mechanisms, and the legal admissibility of digital evidence. The course will demonstrate how offender characteristics, motivation and modus operandi can be identified from the cybercrimes committed and the targets of the cybercrimes. Investigations involving computers, smartphones, gaming consoles and other digital technologies will be covered. In this course, particular emphasis will be placed on the barriers to the effective investigation of cybercriminals and enforcement of cybercrime laws, and the ways to overcome these barriers and deter cybercriminals from engaging in illicit activities.
Grading: GC SCPS Graded
Repeatable for additional credit: No

GSCC1-GC 1015 Cyberpower & Global Security (3 Credits)
Cyberpower is not about cybersecurity. Aside from all the obvious benefits of employing computers and network technology to compute, store, and transmit information, this course focuses on the exploitation of cyber insecurity to enable the attainment of state and non-state actors' strategic objectives. Although the technical and tactical capabilities required to conduct offensive cyber operations are well understood, less clear are how state and private actors link them to strategic objectives. This course provides students with an understanding of the impact cyber operations have on global security and statecraft.
Grading: GC SCPS Graded
Repeatable for additional credit: No

GSCC1-GC 1020 Infrastructure Security & Resilience (3 Credits)
Critical infrastructures are vital to nations, to such an extent that damage to one sector can have a debilitating impact on the functioning of society. Given the numerous threats facing critical infrastructure, and the dependencies and interdependencies of critical infrastructures, it is imperative that the vulnerabilities of these sectors be examined. This course identifies the threats to and vulnerabilities of critical infrastructure sectors. It also highlights the importance of international critical infrastructure protection and examines lessons learned from national and international cybersecurity incidents targeting critical infrastructures. Furthermore, this course proposes ways to secure critical infrastructure both in the U.S. and abroad.
Grading: GC SCPS Graded
Repeatable for additional credit: No

GSCC1-GC 1030 Mission Assurance or Continuity of Operations (3 Credits)
This course will focus on what can be done not only to protect operations from cyber disruptions but how businesses and organisations should prepare to continue their operations when they inevitably fall victim to a cyber incident. This course includes modules on what is a mission or operation, how to find an organisations cyber dependencies, cyber lexicon, vulnerabilities, threats, losses, hazards, analytic reduction, systems theory, the basics of cyber-attacks, and what a Primary, Alternate, Contingency and Emergency operations (PACE) plan should include. Successful completion of the course will allow the student to analyse the operations of an organisation, determine the cyber dependencies of the operations, create new resilient operations, determine appropriate controls to increase resiliency of current operations, develop a resilient PACE plan for a business's operations.
Grading: GC SCPS Graded
Repeatable for additional credit: No

GSCC1-GC 2010 Connected Communities (3 Credits)
Internet connected devices are everywhere! The course is modeled around a fictional municipality considering designating public money for a contract to integrate connected technologies into the community. Before doing so, the mayor's office convened a task force of government, industry, and community organizations to participate in the production of a connected communities strategy that will govern how the money is spent. This strategy will lay out the municipality's priorities, challenges, principles, and values related to this deployment. The assignments in the course will be cumulative and result in the production of a connected communities strategy for the fictional municipality. The goal of this course is to provide students with hands-on experience in considering the disparate characteristics and challenges of a municipality and of creating a strategy based on differing equities.
Grading: GC SCPS Graded
Repeatable for additional credit: No

GSCC1-GC 2020 Open Source Intelligence (3 Credits)
Intelligence is vital to national security, economic security and U.S. foreign policy. Intelligence is also valuable to businesses and is an integral part of their operations. Using a multi-disciplinary approach, this course examines open source intelligence obtained by searching and analyzing publicly available information through data mining, advanced web searches, and other information gathering strategies. It also explores the manner in which important information is identified, collected, analyzed, synthesized, and interpreted from a wide variety of sources. It then considers how this information is used to identify targets and vulnerabilities of targets, and to assess the capabilities of cybercriminals, terrorists, nations, and hostile elements. This course also covers social media forensics, looking in particular at: the type of data collected by social media sites; the type of evidence sought and its use by law enforcement and intelligence agencies for the purpose of data mining, intelligence gathering and investigating criminal activity; and the manner in which data can be gleaned from social media sites
Grading: GC SCPS Graded
Repeatable for additional credit: No

GSCC1-GC 2025 Cyberfeminism, Gender Roles, and Gendered Perspectives on Cyberspace (3 Credits)
Women worldwide are affected by the social, economic, political, and cultural conditions created by the Internet, computers, and related technology. Cyberfeminism examines the impacts of these conditions on women through the lens of feminism. This course explores two general schools of thought in cyberfeminism: cyberutopianism, which holds that cyberspace is a liberating environment for women, and cyberdystopianism that views cyberspace as another forum within which women can be oppressed. This course further considers the relationship between digital technology, cyberculture, and gender. Special attention is paid to various feminist ideologies and movements associated with cyberfeminism, the role of gender in cyberspace, and gendered perspectives on cyberspace.
Grading: GC SCPS Graded
Repeatable for additional credit: No

GSCC1-GC 2030 Cyber Leadership, Risk Oversight and Resilience (3 Credits)
This course provides both a big picture strategic overview and an in-depth tactical understanding of what every type of organization – business, nonprofit, government, international agency or university – and their leaders and managers need to do to build internal governance, culture, risk, business continuity and crisis and reputation management for organizational resilience, mission assurance and stakeholder protection and value creation in this era of cyber-uncertainty, insecurity and opportunity. Key interconnected themes examined include the role of governance (the board of directors) in cyber-risk oversight, the role of leadership (the CEO and executive management) in proactive cyber-security management, the roles and responsibilities of key experts (legal, risk, finance, compliance, audit, public relations/communications, strategy, technology, security, human resources) and the criticality of inter-disciplinary and public/private collaboration.
Grading: GC SCPS Graded
Repeatable for additional credit: No

GSCC1-GC 2225 National Security and Emerging Tech (3 Credits)
Constant cyber warfare, espionage, and theft of intellectual property are central instruments of statecraft for nation-states globally. Every geopolitical era has a central asset or idea that is being competed over and today, we are competing over emerging technology. The most valuable geopolitical assets today are intellectual property, source code, and data. Nations go to war to protect their interests and today national interests surround the development, operation, and economy of emerging technologies. In this course, we will discuss the impacts of artificial intelligence, quantum information science, space, and telecommunications on geopolitical decision making. We will do hands-on exercises on cyber intellectual property theft and hold mock National Security Council meetings to demonstrate how the policies that drive our national priorities are created. Students should expect to learn the policy and national security implications of critical emerging technologies, how those technologies are under threat from non-traditional and espionage collection, and how policy is made to confront those risks.
Grading: GC SCPS Graded
Repeatable for additional credit: No

GSCC1-GC 2235 Cyber Threat Intelligence Analysis (3 Credits)
Cyber Threat Intelligence Analysis (CTIA) is a method-driven course that uses a holistic "human centered" approach beginning with the understanding of traditional analytics, ethics, and intelligence lifecycle applied in cyberspace. The course covers concepts from planning and building a threat intelligence project and using kill chain methodologies for discovery of cyber threats to developing CTI requirements and producing a collection plan. CTIA involves practitioner exercises and labs, to include threat modeling and development of a CTI report for dissemination, briefing, and sharing relevant data and information with stakeholders. These concepts are essential to building an effective cyber threat intelligence program and, when used properly, can secure an organization from future threats like espionage, cybercrime, and other disruptive cyber activities to include disinformation campaigns.
Grading: GC SCPS Graded
Repeatable for additional credit: No

GSCC1-GC 2245 The Economics of Cybersecurity (3 Credits)
This elective is designed to examine the economic phenomena we see in the cyber environment today. The course will take an interdisciplinary approach to examine the initial basis for action or inaction with economics providing explanations for market behavior and outcomes. The purpose of this course will be to explain the role economics plays in cybersecurity, supply chains for cyber dependent systems, cryptocurrencies, and the measurement of cyber risk. Students will leave this course with a clearer understanding of various core topics of modern economics to include common market failures and behavioral economics. Insight from these topics can inform strategies to address the myriad of cyber issues plaguing the US today.
Grading: GC SCPS Graded
Repeatable for additional credit: No

GSCC1-GC 2510 Cyber: Technical, Operational & Strategic Perspectives (3 Credits)
This course provides a structured approach for students without a technical background to understand technical, operational and strategic elements of cyberspace across a variety of technical ecosystems. In the first part of the course we will develop a foundational knowledge of the technical components of cyberspace, the missions they support, and frameworks used to secure technology from malign actors. Through lectures and readings on current events, students will gain an understanding of how vulnerabilities are exploited by threat actors, and the challenges defenders face in assuring an organization's core mission and processes. Throughout the course, students will work in small groups to analyze case studies of cyber breaches to deconstruct and evaluate specific operational impacts of cybersecurity lapses. Students will be equipped with the lexicon, grammar and logic necessary to analyze the full spectrum of cyber operations within strategic contexts.
Grading: GC SCPS Graded
Repeatable for additional credit: No

GSCC1-GC 2900 Greece - Great Power Competition and US Grand Strategy in the Eastern Mediterranean (3 Credits)
Greece is at the epicenter of a region that has seen a staggering array of wars, revolutions, and coups since World War II. Greece's geographic position in the Eastern Mediterranean and Aegean Sea makes it an important strategic ally of the United States both economically and geopolitically. The Eastern Med region contains substantial hydrocarbon reserves, which could transform the economy of countries like Egypt, Cyprus and Israel. But it also has a long history of conflict, and is an area of intense competition between great powers in the region including the US, Russia China as well as regional powers such as Greece and Turkey. Activities of these nation-states have been accompanied by a series of small-scale conflicts over control over telecommunications infrastructure, natural resources and military basing. As the region re-emerges as a significant theater of global and regional security, the balance of power among regional players is being disturbed. Within this context, the GFI Greece will help students better understand the global security, conflict and cyber challenges facing the world today.
Grading: GC SCPS Graded
Repeatable for additional credit: No

GSCC1-GC 3000 Cyber Practicum (3 Credits)
This practicum provides students the opportunity to design and develop solutions aligned to real-world problems of a selected public or private sector entity. Students will apply their knowledge and skills gained throughout the MSGSCC curriculum to design solutions to mitigate, prevent, respond and recover from significant cyber incidents while assuring continuity of operations. Students will be mentored by members of the faculty and chosen organization, assume various job roles in the sector, and work collectively to solve a simulated cyber crisis. The ultimate goal of the course is for students to design and present, in teams, solutions utilizing industry standard cyber risk and assurance frameworks along with developing essential job transferable competencies in cyber crisis management.
Grading: GC SCPS Graded
Repeatable for additional credit: No

GSCC1-GC 3900 Graduate Thesis or Capstone Project (3 Credits)
The Independent Research Study should focus on an issue of interest to the student that directly relates to the student's area of specialization. In cases where the topic rests or touches on more than one field, a teamwork project may be substituted for the independent study. Members of the team will be required to contribute material on the selected topic from the vantage point of their respective concentrations. Students will have latitude in selecting their topic but all topics, whether for individual study or a team undertaking, will need faculty approval and will be conducted under the stewardship of one faculty person. The study may be a traditional research paper of a case study based on primary research, extensive interviews, and profiles of the protagonists, be they individuals or institutions and should reflect high standards of scholarship.
Grading: GC SCPS Graded
Repeatable for additional credit: No