

GLOBAL SECURITY, CONFLICT, AND CYBER CRIME (MS)

Department Website (<https://www.sps.nyu.edu/homepage/academics/masters-degrees/ms-in-global-security-conflict-and-cybercrime.html>)

NYSED: 39554 HEGIS: 2299.00 CIP: 29.0207

Program Description

The 36-credit Master of Science in Global Security, Conflict, and Cyber Crime (MSGSCC), offered by the NYU SPS Center for Global Affairs, provides a unique perspective and a competitive advantage by focusing on cyber conflict through the lens of the social sciences. The program prepares you to enter the fast-changing world of international security and explores the fields of cyber espionage, cyber criminology, cyber warfare, and intelligence analysis, affording you the opportunity to gain a deep understanding of cyber security policy, while acquiring the skills to develop and execute cyber security and risk management strategies. It provides the benefits, resources, and prestige of earning your degree at NYU, while learning from top thought leaders in the field.

The Master of Science in Global Security, Conflict, and Cybercrime, offered by the Center for Global Affairs (CGA), prepares students to address transnational security issues arising from cybercrime, cyberconflict, and cyberwar. The program, which can be completed on a full- or part-time basis, approaches cyber issues from a variety of interdisciplinary perspectives. It is designed to prepare individuals for cyber-related positions across the private sector, public sector, and non-governmental organizations. Courses are taught by experienced scholar and practitioner faculty members who bring their wealth of knowledge, real-world experience, and networks to the classroom.

Admissions

Admission to master's programs at the NYU School of Professional Studies requires the completion of a U.S. bachelor's degree or its international equivalent. Admissions decisions are made through a holistic review process. Visit the SPS Admissions website (<https://www.sps.nyu.edu/homepage/admissions/admissions-criteria-and-deadlines/graduate-programs.html>) for detailed application requirements and deadlines.

Program Requirements

The program requires the completion of 36 credits, comprised of the following:

| Course | Title | Credits |
|-------------------------------|--|---------|
| Core Curriculum | | |
| GLOB1-GC 2510 | Cyberspace: Technical, Operational, and Strategic Perspectives | 3 |
| GSCC1-GC 1005 | Cyber Law | 3 |
| GSCC1-GC 1010 | National & International Cyber Organizations | 3 |
| GSCC1-GC 1015 | Cyberpower & Global Security | 3 |
| GSCC1-GC 1020 | Infrastructure Security & Resilience | 3 |
| GSCC1-GC 1030 | Mission Assurance or Continuity of Operations | 3 |
| Electives | | |
| Select five of the following: | | 15 |

| | |
|---------------|---|
| GSCC1-GC 2010 | Connected Communities |
| GSCC1-GC 2030 | Cyber Leadership, Risk Oversight and Resilience |
| GSCC1-GC 2035 | Cyber Ethics |
| GLOB1-GC 2515 | Applied Statistics and Data Analysis |
| GLOB1-GC 2516 | Advanced Data Analysis for Global Affairs |
| GLOB1-GC 3035 | Analytic Skills for Global Affairs |
| GSCC1-GC 2025 | Gender Issues in the Cyber Era |
| GSCC1-GC 2235 | Cyber Threat Intelligence Analysis |
| GLOB1-GC 2051 | Disinformation and Narrative Warfare |
| GSCC1-GC 2245 | The Economics of Cybersecurity |
| GLOB1-GC 2600 | Espionage and Economic Power |
| GLOB1-GC 2047 | The Future of War |
| GLOB1-GC 2070 | Intelligence and Counterintelligence |
| GLOB1-GC 2518 | Geographic Information Systems for Global Affairs |
| GLOB1-GC 2650 | Global Risk |
| GSCC1-GC 2900 | Greece - Great Power Competition and US Grand Strategy in the Eastern Mediterranean |
| GLOB1-GC 3915 | Independent Study |
| GLOB1-GC 1000 | International Relations in The Post-Cold War Era |
| GLOB1-GC 3905 | Internship |
| GSCC1-GC 2225 | National Security and Emerging Tech |
| GSCC1-GC 2020 | Open Source Intelligence |
| GLOB1-GC 3060 | Political Risk: A Multi-Dimensional Analysis |
| GLOB1-GC 2425 | Private Sector Partnerships |
| GLOB1-GC 3064 | Responding to Emergencies in the Global System |
| GSCC1-GC 2500 | Special Topics |
| GLOB1-GC 2065 | Transnational Crime |
| GLOB1-GC 2080 | Transnational Terrorism |
| GLOB1-GC 2000 | Transnational Security |

| | | |
|---------------------------------------|---|-----------|
| GLOB1-GC 2055 | Arms Control, Non-Proliferation, and Disarmament of Weapons of Mass Destruction | |
| GLOB1-GC 2645 | The United Nations and 21st Century Challenges | |
| GLOB1-GC 2151 | Monitoring, Evaluation and Learning for Global Affairs | |
| GLOB1-GC 2520 | Advanced Colloquium (Transnational Security) | |
| Capstone, Thesis, or Practicum | | |
| GSCC1-GC 3900 | Graduate Thesis or Capstone Project | 3 |
| or GSCC1-GC 3000 | Cyber Practicum | |
| or GLOB1-GC 3920 | Consulting Practicum | |
| Total Credits | | 36 |

Sample Plan of Study

Part-Time

| Course | Title | Credits |
|--------------------------|--|-----------|
| 1st Semester/Term | | |
| GSCC1-GC 2510 | Cyber: Technical, Operational & Strategic Perspectives | 3 |
| GSCC1-GC 1010 | National & International Cyber Organizations | 3 |
| Credits | | 6 |
| 2nd Semester/Term | | |
| GSCC1-GC 1030 | Mission Assurance or Continuity of Operations | 3 |
| GSCC1-GC 1020 | Infrastructure Security & Resilience | 3 |
| Credits | | 6 |
| 3rd Semester/Term | | |
| GLOB1-GC 2051 | Disinformation and Narrative Warfare | 3 |
| GSCC1-GC 1015 | Cyberpower & Global Security | 3 |
| Credits | | 6 |
| 4th Semester/Term | | |
| GLOB1-GC 2000 | Transnational Security | 3 |
| GLOB1-GC 3064 | Responding to Emergencies in the Global System | 3 |
| Credits | | 6 |
| 5th Semester/Term | | |
| GSCC1-GC 1005 | Cyber Law | 3 |
| GLOB1-GC 2070 | Intelligence and Counterintelligence | 3 |
| Credits | | 6 |
| 6th Semester/Term | | |
| GLOB1-GC 3900 | Graduate Thesis or Capstone Project | 3 |
| GSCC1-GC 2245 | The Economics of Cybersecurity | 3 |
| Credits | | 6 |
| Total Credits | | 36 |

Full-Time

| Course | Title | Credits |
|--------------------------|--|-----------|
| 1st Semester/Term | | |
| GSCC1-GC 2510 | Cyber: Technical, Operational & Strategic Perspectives | 3 |
| GSCC1-GC 1005 | Cyber Law | 3 |
| GSCC1-GC 1010 | National & International Cyber Organizations | 3 |
| GSCC1-GC 1020 | Infrastructure Security & Resilience | 3 |
| Credits | | 12 |
| 2nd Semester/Term | | |
| GSCC1-GC 1015 | Cyberpower & Global Security | 3 |
| GSCC1-GC 1030 | Mission Assurance or Continuity of Operations | 3 |
| GLOB1-GC 2051 | Disinformation and Narrative Warfare | 3 |

| | | |
|--------------------------|--|-----------|
| GLOB1-GC 2070 | Intelligence and Counterintelligence | 3 |
| Credits | | 12 |
| 3rd Semester/Term | | |
| GLOB1-GC 3064 | Responding to Emergencies in the Global System | 3 |
| GSCC1-GC 2245 | The Economics of Cybersecurity | 3 |
| GSCC1-GC 2500 | Special Topics | 3 |
| Credits | | 9 |
| 4th Semester/Term | | |
| GLOB1-GC 3900 | Graduate Thesis or Capstone Project | 3 |
| Credits | | 3 |
| Total Credits | | 36 |

Learning Outcomes

Upon successful completion of the program, graduates will:

1. Demonstrate understanding of different forms of cybercrime and assess the nature and extent of cybercrime.
2. Recognize and evaluate the jurisdiction issues and obstacles in policing, investigating, and prosecuting cybercrime.
3. Describe digital forensics and differentiate the processes involved in conducting public and private cybercrime investigations.
4. Discuss the role of national and international agencies in dealing with cybercrime, assess these agencies' responses to cybercrime, and recommend effective ways to deal with various cybercrimes.
5. Critically analyze and evaluate the global impact of nations' policies, laws, and measures and the ethical implications of nations' cyberoffensive and cyberdefensive tactics.
6. Conduct risk assessments of cybercrime and recognize, analyze, and synthesize information from a wide variety of sources to identify the cybersecurity threats posed to national and international critical infrastructure and the Internet of Things and the measures needed to protect them.
7. Express informed opinions about transnational security issues associated with cybercrime in oral and written communications.

Policies

NYU Policies

University-wide policies can be found on the New York University Policy pages (<https://bulletins.nyu.edu/nyu/policies/>).

School of Professional Studies Policies

Additional academic policies can be found on the School of Professional Studies academic policy pag (<https://bulletins.nyu.edu/graduate/professional-studies/academic-policies/>)e (<https://bulletins.nyu.edu/graduate/professional-studies/academic-policies/>).