Cybersecurity Operations (MS)

This program is offered by the George Herbert Walker School of Business and Technology and is offered online via asynchronous modality and at select U.S. and international campuses. Please see the Campus Locations and Offerings section of this catalog for a list of campuses.

Program Description

Education at the graduate level is an expansion of the knowledge attained from undergraduate studies. Graduate education encourages the development of advanced skills, theoretical knowledge and critical thinking skills to practice the art and science of cybersecurity management.

Students entering the cybersecurity program should have knowledge of computer systems, digital networks**,** familiarity with internet and wireless applications, and possess good (high school algebra and exposure to trigonometry) mathematical as well as written and oral communication skills.

The master of science (MS) in cybersecurity operations prepares individuals for demanding positions in public and private sectors overseeing, operating, or protecting critical computer systems, information, networks, infrastructures and communications networks.

Students will be well-versed to apply their knowledge and critical thinking related to domestic and international legal systems, private and public policies, and ethics, as they apply cybersecurity to information protection, terrorism, fraud, theft, intelligence/counterintelligence, digital forensics, pre-emptive and strategic force operation application situations.

Students may not apply for dual majors because of the technical nature of this MS degree program. Students may apply for sequential degrees as long as they do not duplicate core courses.

Webster University is designated as a National Center of Academic Excellence in Cyber Defense Education (CAE-CDE).

Learning Outcomes

- Graduates will be capable of explaining important principles and theories used throughout the field of cybersecurity.
- Graduates will be capable of applying knowledge in the field of cybersecurity to analyze real world problems.
- Graduates will be capable of effectively integrating knowledge in the field of cybersecurity to propose solutions to real world problems.

Program Curriculum

The 36 credit hours required for the MS in cybersecurity operations must include the required core courses.

Core Courses (24 hours)

- CSSS 5000 Introduction to Cybersecurity (3 hours)
- CSSS 5110 Cybersecurity Communications (3 hours)
- CSSS 5120 Cybersecurity Infrastructures (3 hours)
- CSSS 5130 Cybersecurity Intelligence/Counter Intelligence (3 hours)
- CSSS 5140 Cybersecurity Strategic Operations (3 hours)
- CSSS 5160 Encryption Methods and Techniques (3 hours)
- CSSS 5180 Social Engineering (3 hours)
- CSSS 6000 Practical Research in Cybersecurity (3 hours)

Elective Courses (12 hours)

Three elective courses (9 hours) chosen from the following:

- CSSS 5210 Cybersecurity Law and Policy (3 hours)
- CSSS 5220 Cybersecurity Threat Detection (3 hours)
- CSSS 5230 Cybersecurity Forensics (3 hours)
- CSSS 5250 Use and Protection of Space Assets (3 hours)
- CSSS 5265 Foundations of Software Development (3 hours)
- CSSS 5270 Cybersecurity in Cloud Computing (3 hours)
- CSSS 5290 Cybersecurity Risk Management Framework (3 hours)
- CSSS 5990 Advanced Topics in Cybersecurity** (3 hours)
- CSSS 6500 Cybersecurity Internship (3 hours)

***A maximum of one CSSS 5990 Advanced Topics in Cybersecurity courses may be counted toward the 36 required credit hours.*

One additional elective course (3 hours):

The student must select one additional elective from CSSS or other Webster elective credit courses that may be offered at the location where the student is completing their MS requirements.

All students in this curriculum must complete the CSSS 6000 Practical Research in Cybersecurity (3 hours) capstone course as a practical research paper or an individual or team project for a total of 3 credit hours and 36 contact hours.

Webster reserves the right to restrict access to some courses that **may** require specific clearances to address specific classified topics related to advanced course content in cybersecurity. Professors must advise the Site Director, Faculty Advisor or Site Manager of the potential of including any classified content in the course and clearly identify the need for security clearances, the level, agency issued by, and methods employed for the protection of information with applicable security policies and procedures at the location where the course is to be taught. Counselors must understand specific clearance requirements of these courses and the specific clearances of students attempting to enroll in these courses. This restriction will only apply to those programs offered at national laboratories; intelligence agencies or specified military sites which request this level of security.

Dual Degree Option: MA in National Security Studies/MS in Cybersecurity Operations

This program is only available at select U.S. locations.

54 Credit Hours

Upon completion of the 54 credits, two separate diplomas are issued at the same time. The two degrees cannot be awarded separately or sequentially under this arrangement.

Required Courses

- CSSS 5000 Introduction to Cybersecurity (3 hours)
- CSSS 5110 Cybersecurity Communications (3 hours)
- CSSS 5120 Cybersecurity Infrastructures (3 hours)
- CSSS 5130 Cybersecurity Intelligence/Counter-Intelligence (3 hours)
- CSSS 5140 Cybersecurity Strategic Operations (3 hours)
- CSSS 5160 Encryption Methods and Techniques (3 hours)
- CSSS 5180 Social Engineering (3 hours)
- CSSS 6000 Practical Research in Cybersecurity (3 hours)
- NTSC 5000 Introduction to National Security Studies (3 hours)
- INTL 5590 International Security (3 hours)
- NTSC 5100 Research Methods in National Security Studies (3 hours)

Cybersecurity Operations (MS)

- NTSC 6000 Capstone in National Security Studies (3 hours) **or** NTSC 6250 Thesis in National Security Studies* (6 hours) **and** INTL 6900 University Thesis Requirement* (0 hours)

*Students taking NTSC 6250 Thesis in National Security Studies (6 hours) must also register for INTL 6900 University Thesis Requirement (0 hours). INTL 6900 acknowledges successful completion of all thesis requirements including conforming to university and departmental guidelines, as well as depositing the thesis in the University library. The 6 credit hours for NTSC 6250 are drawn from the 3 credit hours reserved for the NTSC 6000 capstone and 3 elective credit hours in the program.

Electives

- 2 elective courses chosen from the MS in cybersecurity operations
- 4 electives chosen from the International Regional and National Security Track of the MA in national security studies

Sequential MS in Cybersecurity Operations

A student who holds an MA, MS or an equivalent graduate degree from Webster University or another regionally accredited college or university (or its international equivalent) may earn a sequential MS in cybersecurity operations from Webster University.

Transfer credit may not be applied toward the sequential MS.

These conditions apply to the student seeking the sequential MS in cybersecurity operations:

- The student must take a minimum of 27 credit hours to earn the sequential MS in cybersecurity operations. This includes the 24-hour degree core, as well as one elective. The elective must be selected from the following list:
  - CSSS 5210 Cybersecurity Law and Policy (3 hours)
  - CSSS 5220 Cybersecurity Threat Detection (3 hours)
  - CSSS 5230 Cybersecurity Forensics (3 hours)
  - CSSS 5250 Use and Protection of Space Assets (3 hours)
  - CSSS 5265 Foundations of Software Development (3 hours)
  - CSSS 5270 Cybersecurity in Cloud Computing (3 hours)
  - CSSS 5290 Cybersecurity Risk Management Framework (3 hours)
  - CSSS 5990 Advanced Topics in Cybersecurity (3 hours)
  - CSSS 6500 Internship in Cybersecurity (3 hours)
- The student must meet the core course requirements of the MS in cybersecurity operations. If the student enrolled in any of the core courses as electives in his or her MA, MS or an equivalent degree program, those courses must be replaced with applicable CSSS electives (see list above).
- Advancement to Candidacy for sequential MS in cybersecurity operations:
  - Sequential MS in cybersecurity operations students who received the MA, MBA or MS from Webster University will be advanced to candidacy with initial registration.
  - A student who received the master's degree from another regionally accredited institution will be advanced to candidacy upon approval of the master's degree transcript.

Admission

See the Admission section of this catalog for general admission requirements. Students interested in applying must submit their application online at www.webster.edu/apply. Transcripts should be sent from your institution electronically to transcripts@webster.edu. If this service is not available, send transcripts to:

Office of Admission
Webster University
470 E. Lockwood Ave.
St. Louis, MO 63119

Special Requirements

- Students entering the cybersecurity program should have knowledge of computer systems, digital networks, familiarity with internet and wireless applications, and possess good (high school algebra and exposure to trigonometry) mathematical as well as written and oral communication skills.
- Applicants to the MS Cybersecurity Operations who have an active Certified Information Systems Security Professional (CISSP) certification at the point of admission, will be exempt from two core courses (CSSS 5000 and CSSS 5140), reducing the number of required courses to 30 credit hours.

Advancement to Candidacy

Students are admitted to their graduate program upon completion of all admission requirements. Students are advanced to candidacy status after successfully completing 12 credit hours with a cumulative GPA of 3.0 or higher. In specialized programs, courses required as prerequisites to the program do not count toward the 12 credit hours required for advancement.