



BACHELOR OF SCIENCE IN CYBERSECURITY CYBER OPERATIONS TRACK

Would you like to help secure our nation’s information technology (IT) infrastructure? If so, the study of Cybersecurity will prepare you for a challenging and rewarding career. Today more than ever there’s a strong need for professionals interested in finding ways to make our information technology safer.

The National Security Agency’s (NSA) National Centers of Academic Excellence in Cyber Operations (CAE-CO) program supports the President’s “National Initiative for Cybersecurity Education (NICE): Building a Digital Nation” and furthers the goal of broadening the pool of skilled workers capable of supporting a cyber-secure nation. The University of Nebraska at Omaha Cybersecurity undergraduate degree program is one of the few NSA-certified CAE-CO universities in the nation and the only one in the state of Nebraska (<https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-operations/centers.shtml>). As a result, UNO’s College of Information Science and Technology is able to offer undergraduate students majoring in Cybersecurity the option to pursue a specialized Cyber Operations (CO) track and complete the requirements set out by the NSA’s CAE-CO program. Successfully completing the CO track opens up a variety of new opportunities that are only available to students with this specialization.

Students who successfully complete the Cyber Operations track will have the designation recorded on their transcript and will also receive a certificate in addition to receiving their regular Bachelor of Science in Cybersecurity diploma.

The CAE-CO program is intended to be a highly technical, interdisciplinary, higher education program firmly grounded in computer science (CS), computer engineering (CE), and technical cybersecurity, with extensive opportunities for hands-on applications via labs/exercises. The track provides a particular emphasis on technologies and techniques related to specialized cyber operations (e.g. collection, exploitation, and response) to enhance the national security posture of our nation. These technologies and techniques are critical to intelligence, military, and law enforcement organizations authorized to perform these specialized operations.

Each student in the Cyber Operations track must complete ten required knowledge units (KUs) and four out of eleven additional elective KUs that UNO offers. Some graduate level courses (marked with * on the table below) are required for successful completion of the Cyber Operations track.

National Security Agency (NSA) Summer Internship Program

Students who are eligible for security clearances enrolled in the Cyber Operations track must apply to **the** NSA summer intern program specially designed for Cyber Operations students.

If you are selected and join, NSA pays interns a bi-weekly salary for the 12-week ~~intern~~ **internship**. Housing will be paid by you out of the salary. However, the agency does arrange for reduced price 3-4 bedroom apartments for interns which you may wish to use.

The College of IS&T offers both a Bachelor of Science and a minor in Cybersecurity. Please visit www.unomaha.edu/college-of-information-science-and-technology/academics/cybersecurity.php for more information.

Students already enrolled in BS Cybersecurity degree program have very few additional requirements to meet in order to complete the Cyber Operations track.

REQUIRED KNOWLEDGE UNITS (KU)

UNO courses that cover all the required KUs

CSCI 2030 – Mathematical Foundations of CS
CYBR 2250 – Low-Level Programming

CSCI 3320 – Data Structures
CSCI 3550 – Communications Networks
CYBR 3570 – Cryptography
CSCI 3660 – Theory of Computation

CYBR 4360 – Foundations of Information Assurance
CYBR 4450 – Host-Based Vulnerability Discovery
CYBR 4460 – Network-Based Vulnerability Discovery
CSCI 4500 – Operating Systems
PSCI 4250 – Intelligence and National Security
PSCI 4260 – International Law

CYBR 8410 – Distributed Systems and Network Security *
CYBR 8420 – Software Assurance *
CSCI 8620 – Mobile Computing and Wireless Networking *
CYBR 8480 – Secure Mobile and Internet of Things
(IOT) Development *

* Graduate level courses required for Cyber Operations track. Can be taken with special permission.

ELECTIVE KNOWLEDGE UNITS (KU)

Must choose any 4 out of 11. Courses that must be taken to fulfill corresponding elective knowledge units

Programmable Logic

CYBR 8460 – Security of Embedded Systems

Risk Management of Information Systems

CYBR 3600 – Info Security, Policy, and Awareness

Computer Architecture (includes Logic Design)

CSCI 3710 – Intro to Digital Design and
Computer Organization
CSCI 4350 – Computer Architecture

Microcontroller Design

CYBR 8460 – Security of Embedded Systems

Embedded Systems

CYBR 8460 – Security of Embedded Systems

Digital Forensics

CYBR 4380 – Computer and Network Forensics

Applied Cryptography

CYBR 8450 – Applied Cryptography

Industrial Control System (ICS)

CYBR 4440 – Industrial Control System Security

No additional courses required for following elective KUs:

- **Offensive Cyber Operations**
- **Software Security Analysis**
- **Secure Software Development**

For further information, please contact

Undergraduate Advising
Office: PKI 170
Phone: 402-554-3819