THE CITADEL
CYBER AND COMPUTER SCIENCES

Bachelor of Science in Cyber Operations

Program Contact Information

Dr. Shankar Banik, 843 953-5039, baniks1@citadel.edu
Professor and Head of Department of Cyber and Computer Sciences

Program Mission

The mission of Bachelor of Science program in Cyber Operations is to develop the next generation of cyber leaders who can analyze the security of cyber systems, protect and defend cyber systems, investigate different types of attacks and incidents in cyber systems in the industry, government or military environment. **The Citadel has been designated as National Center of Academic Excellence in Cyber Defense Education (CAE-CDE) by National Security Agency and Department of Homeland Security in 2016.** The Citadel currently offers B.S. in Computer Science and a minor in Cybersecurity which is the academic path for CAE-CDE. **The B.S. in Cyber Operations that will start in Fall 2020**, will be a standalone major that will meet the academic standards of Center of Excellence in Cyber Operations program set by National Security Agency. This major is deeply technical and inter-disciplinary program grounded in computer science, computer engineering, and/or electrical engineering disciplines, with extensive opportunities for hands-on applications via labs and exercises. The major is housed in the newly created Department of Cyber and Computer Sciences.

Program Objectives

Graduates of Bachelor of Science in Cyber Operations will be able to:

1. Apply security principles and practices to the design and implementation of the physical, software, and human component of the cyber systems,
2. Analyze and evaluate cyber systems with respect to security,
3. Identify, analyze, and mitigate threats in the cyber systems.

Employment Opportunities

The United States Bureau of Labor and Statistics estimates a 32% increase in the number of cyber-related positions over the next eight years, with a median salary of $98,350 [1]. Possible career paths include:

- Cybersecurity Analyst
- Penetration Tester
- Digital Forensic Analyst
- Malware Analyst
- Incident Responder
- Threat Analyst

[1] https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

THE CITADEL

CYBER AND COMPUTER SCIENCES

Curriculum

		Fall				Spring	
	Course No.	**Course Title**	**Credit Hours**		**Course No.**	**Course Title**	**Credit Hours**
Freshman	CSCI 201	Introduction to Computer Science I	3		FSEM 101	Freshman Seminar	3
	CSCI 211	Introduction to Computer Science I Lab	1		FSWI 101	Freshman Linked Writing Intensive	3
		Modern Language	3		CSCI 202	Introduction to Computer Science II	3
	MATH 131	Analytical Geometry and Calculus I	4			Modern Language	3
	RPED 260	Physical Fitness, Resiliency, and Wellness	3		MATH 132	Analytical Geometry and Calculus II	4
	LDRS 101	First Year Experience	1			1st Year Basic ROTC	1
		1st Year Basic ROTC	1				
	CSCI 227	Principles and Practices of Cybersecurity	3				
Sophomore	ENGL XXX	Strand English	3		CSCI 317	Computer Networks and Internet	3
	CSCI 305	Computer Organizations and Programming	3		CSCI 223	Data Structures and Algorithms	3
		Science	4		CSCI 320	Database Design	3
	MATH 206	Discrete Structures	3			Science (satisfies Strand Science requirement)	3
		Strand Elective	3		STAT 261	Introduction to Probability and Statistics	3

THE CITADEL

CYBER AND COMPUTER SCIENCES

	LDRS 201	Sophomore Seminar in Principled Leadership	1		RPED	Required Physical Education	0
		2nd Year Basic ROTC			LDRS 211	Sophomore Seminar Service Learning Lab	0
						2nd Year Basic ROTC	
Junior	CSCI 327	Computer Security	3		CSCI 409	Malware Analysis	3
	CSCI 405	Operating Systems	3		CSCI 427	Advanced Cybersecurity	3
	CSCI 408	Software Security	3		MATH 302	Applied Cryptography	3
		Strand Social Science	3		HIST 30X	Strand History	3
		General Elective	3		LDRS 371	Leadership in Organizations	3
	LDRS 311	Junior Ethics Enrichment Experience	0			1st Year Advanced ROTC	
		1st Year Advanced ROTC					
	RPED	Required Physical Education					
Senior	CSCI 410	Offensive Cyber Operations	3		CSCI 499	Senior Research Project	3
	CRMJ 401	Cyber Ethics and Policy	3		CSCI 411	Cyber Forensics	3
	ELEC 311	Digital Logic and Circuits	3		CSCI 410	Software Security	3
	CSCI 411	Cyber Forensics	3		ELEC 330	Digital Systems Engineering	3
		General Elective	3			*Approved Cyber Elective	3
		2nd Year Advanced ROTC				2nd Year Advanced ROTC	

	LDRS 411	Senior Leadership Integration Seminar	0		COMM 260	Technical Writing and Communications	3

***Approved Cyber Electives:**

CRMJ 392 Cyber Crime

CRMJ 331 Cyber Investigations

CSCI 490 Special Topics: Cyber Warfare

INTL 465 Special Topics: Cyber Intelligence

Course Descriptions

CSCI 227: Principles and Practices of Cybersecurity

This course will provide an introduction to concepts related to cybersecurity. Students will learn safe practices which can be deployed to secure computer systems. Students will gain an understanding of different tools which can be used to defend attacks on computer systems. Special emphasis will be given to systems and applications that cyber users will likely to encounter in daily life. In addition to lecture classes, security lab exercises will be conducted to perform hands-on experiments on safe security practices.

CSCI 201: Introduction to Computer Science I

An introduction to problem solving and algorithm development using Java. Topics include computer organization, operating systems, structured programming, and program modularization. Assignments involve designing, coding, debugging, and documenting computer programs.

CSCI 202: Introduction to Computer Science II

A continuation of the material covered in CSCI 201. This course emphasizes object-oriented programming and a disciplined approach to program development. Topics include data abstraction, recursion, inheritance, polymorphism, linked data structures, stacks, and queues.

CSCI 223: Data Structures and Algorithms

Formal specification and implementation of abstract data types and analysis of algorithms. Topics include list and set representation methods, sorting, trees and graphs. Data structures used include stacks, queues, binary trees, hash tables, priority queues, and search trees.

CSCI 305: Computer Organizations and Programming

THE CITADEL

CYBER AND COMPUTER SCIENCES

An introduction to computer architecture and assembly language programming. Relationship of the conventional machine level of a modern computer system with its other levels. Topics are chosen from addressing; machine instructions; I/O; subroutines; parameters; recursion; stacks; interrupts; number systems and arithmetic; and the physical, digital, and the microprogramming levels.

CSCI 317: Computer Networks and Internet

An introduction to data communications and computer networking. Topics include LAN technologies, packet switching networks, internetworking of heterogeneous network technologies, internetworking protocol suites (with emphasis on TCP/IP), the client/server paradigm, the BSD Socket interface, network security, and important network applications.

CSCI 320: Database Design

An introduction to the logical and physical structures of computer database systems. Topics include data models, query languages, relational database de-sign, and database constraints. Students will be required to complete a project involving database design and implementation.

CSCI 327: Computer Security

A survey of the principles and practices related to computer security emphasizing the problems of security associated with computer networks. Topics include cryptography, privacy, authentication, access control and authorization, security policies, and legal and ethical issues. A significant component of the course is the investigation of attacks commonly used by computer criminals and strategies that can be used to thwart the attacks.

CSCI 408: Software Security

An introduction to secure software development methodologies, reverse engineering, and software exploitation. Topics include secure programming principles and practices, source code auditing, fuzzing, binary code analysis, reverse engineering, and exploitation. A heavy emphasis will be placed on hands-on lab activities to enforce concepts.

CSCI 409: Malware Analysis

An introduction to malware analysis. Topics include detection, obfuscation, and static and dynamic analysis techniques. Students will be introduced to a variety of different malware types, including, but not limited to, interpreted languages, macros, and compiled executables. A heavy emphasis will be placed on the use of hands-on lab activities to enforce concepts.

CSCI 410: Offensive Cyber Operations

An overview of the phases involved in an offensive cyber operation. Special attention will be paid to decision authority/authorization, the cyber kill chain, mission planning, execution, and assessment. Hands-on labs will be used to demonstrate and enforce concepts.

CSCI 411: Cyber Forensics

An introduction to digital forensics on Windows-based Operating Systems. Topics include the incident response lifecycle, collecting forensically sound evidence, analyzing memory and filesystems, and report writing. Hands-on lab assignments will be used extensively to apply concepts.

CSCI 427: Advanced Cybersecurity

This course will cover the techniques used to secure cyber systems. Topics covered will include security policies, computer security management and risk assessment, secured network protocols, software security issues, ethical and legal aspects of security, and disaster recovery. Special emphasis will be given to designing, deploying, and managing complete secured cyber systems.

MATH 302: Applied Cryptography

In this course the students will learn about the common cryptographic use, for example: security functions (data protection, data integrity, authentication, non-repudiation). The students will learn about symmetric cryptography, public key cryptography (Diffie-Hellman, RSA, El Gamal), the strength and weaknesses of various cryptography models. Finally, the students will learn about cryptographic failures including types of attacks (brute force, chosen plaintext, known plaintext, differential and linear cryptanalysis, etc.) and implementation failures.

CRMJ 401: Cyber Ethics and Policy

This course explore the ethics, policies, and legal responses that affect behavior in cyber space with an emphasis on nefarious behavior. Students will explore these topics both from a computer scientist perspective, with an emphasis on computers and networks, as well as a social science perspective, with an emphasis on human behavior in cyberspace.

CRMJ 331: Cyber Investigations

This course will introduce the student to the best practices for seizing and securing digital evidence and the complicated legal issues surrounding digital evidence within the area of Cyber-Crime Investigation to include Cyber-Terrorism. The course will cover evidence and issues relative to file Meta-data for various types of electronic devices such as computer networks, cell phones, and electronic storage. Searches justified by exigent circumstances, search incident to arrest, and search warrant issues will also be covered. This course provides students interested in improving their investigative knowledge with an understanding of identifying, quantifying/qualifying, seizing, and protecting electronic information. The investigative process is studied from basic theoretical concepts to the application of the basic

elements for prosecution of criminal cases. Included are several studies of electronic crime scene investigation, white collar crime, organized crime, and cyber-terrorism. While this class focuses on cyber investigative practices and procedures in the United States, it offers a global perspective and will incorporate examples from different parts of the world.

CRMJ 392: Cyber Crime

An exploration of the current state of computer crime in the United States. The course traces the history of technological crime and identifies areas ripe for exploitation from technology savvy deviants. It also evaluates forensic practices and software in light of government legislation together with an analysis of emerging case law. The course also addresses guidelines for the development of computer forensic laboratories, the creation of computer crime task forces, and the search and seizure of electronic equipment.