Cyber Operations Designation Requirements

Mostly copied from

<https://www.nsa.gov/Resources/Students-Educators/centers-academic-excellence/cae-co-fundamental/requirements>

Contents

[Mandatory Content Knowledge Units (KUs) must teach, assess, and do hands on activities for 3](#_Toc53733328)

[M.1 Low Level Programming Languages 3](#_Toc53733329)

[M.2 Software Reverse Engineering 4](#_Toc53733330)

[M.3 Operating System Theory 5](#_Toc53733331)

[M.4 Networking (must include hands-on lab exercises) 5](#_Toc53733332)

[M.5 Cellular and Mobile Technologies 6](#_Toc53733333)

[M.6 Discrete Math and Algorithms 7](#_Toc53733334)

[M.7 Overview of Cyber Defense (must include hands-on lab exercises) 7](#_Toc53733335)

[M.8 Security Fundamental Principles (i.e., "First Principles") 8](#_Toc53733336)

[M.9 Vulnerabilities 9](#_Toc53733337)

[M.10 Legal and Ethics 10](#_Toc53733338)

[Optional Program Content: (Knowledge Units) 11](#_Toc53733339)

[O.1 Programmable Logic (must include hands-on lab exercises) 11](#_Toc53733340)

[O.2 Wireless Security 12](#_Toc53733341)

[O.3 Virtualization 13](#_Toc53733342)

[O.4 Cloud Security/Cloud Computing 14](#_Toc53733343)

[O.5 Risk Management of Information Systems 15](#_Toc53733344)

[O.6 Computer Architecture 15](#_Toc53733345)

[O.7 Microcontroller Design 16](#_Toc53733346)

[O.8 Software Security Analysis 16](#_Toc53733347)

[*O.9 Secure Software Development (Building Secure Software)* 17](#_Toc53733348)

[O.10 Embedded Systems (must include hands-on lab exercises) 18](#_Toc53733349)

[O.11 Digital Forensics (must include hands-on lab exercises) 18](#_Toc53733350)

[O.12 Systems Programming (must include hands-on lab exercises) 19](#_Toc53733351)sc

[O.13 Applied Cryptography 19](#_Toc53733352)

[O.14 Industrial Control System (ICS) 20](#_Toc53733353)

[O.15 User Experience (UX)/Human Computer Interface (HCI) Security 21](#_Toc53733354)

[O.16 Offensive Cyber Operations 21](#_Toc53733355)

[O.17 Hardware Reverse Engineering 22](#_Toc53733356)

[Schools with 4-year degree in Cyber Operations CAE Designation 23](#_Toc53733357)

[Cedarville University BS in Computer Science with Specialization in Cyber Operations 24](#_Toc53733358)

[Dakota State University Cyber Operations BS 24](#_Toc53733359)

[North Eastern University BS Computer Science with Cyber Operations Concentration 24](#_Toc53733360)

[University of Texas A&M BS in Computer Science, Minor in Cybersecurity 26](#_Toc53733361)

[Townson University BS Computer Science Cyber Operations Track 28](#_Toc53733362)

[University of Arizona BAS Cyber Operations (three separate tracks – Engineering, Law and Policy, Defense & Forensics) 29](#_Toc53733363)

[University of Nebraska Omaha BS in Cybersecurity 30](#_Toc53733364)

[University of New Haven BS in Cybersecurity and Networks 32](#_Toc53733365)

[University of Texas El Paso BS in Computer Science 34](#_Toc53733366)

[University of Texas San Antonio 36](#_Toc53733367)

[Virginia Tech Degree – Computer Engineering Cybersecurity Minor 36](#_Toc53733368)

[Course Names 37](#_Toc53733369)

# Mandatory Content Knowledge Units (KUs) must teach, assess, and do hands on activities for

## M.1 Low Level Programming Languages

(must include programming assignments to demonstrate that students are capable of the desired outcomes)

Low level programming allows programmers to construct programs that interact with a system without the layers of abstraction that are provided by many high level languages. Proficiency in low-level programming languages is required to perform key roles in the cyber operations field (e.g., forensics, malware analysis, exploit development).

Specific languages required to satisfy this knowledge unit are:

* C programming
* Assembly Language programming (for x86, ARM, MIPS or PowerPC)

Outcome: After completing the course content mapped to this knowledge unit, students will be able to develop low level programs with the required complexity and sophistication to implement exploits for discovered vulnerabilities.

**C Language programming**

Outcome: Students will be able to write complex programs such as ones that implement a simple network stack.

**Assembly Language programming**

Outcome: Students will be able to write a functional, stand-alone assembly language program, such as a simple telnet client, with no help from external libraries.

## M.2 Software Reverse Engineering

(must include hands-on lab exercises)

The discipline of reverse engineering provides the ability to deduce the design of a software component, to determine how something works (i.e., recover the software specification), discover data used by software, and to aid in the analysis of software via disassembly and/or decompilation. The ability to understand software of unknown origin or software for which source code is unavailable is a critical skill within the cyber operations field. Use cases include malware analysis and auditing of closed source software.

Specific topics to be covered in this knowledge unit include, but are not limited to:

* + Reverse engineering techniques
  + Reverse engineering for software specification recovery
  + Reverse engineering for malware analysis
  + Reverse engineering communications (to uncover communications protocols)
  + Deobfuscation of obfuscated code
  + Common tools for reverse engineering including but not limited to:
    - Disassemblers (e.g., IdaPro)
    - Debuggers (e.g., gdb, OllyDbg, WinDbg)
    - Virtualization-based sandbox environments (e.g., VMware, Xen)
    - Process and file activity monitors (e.g., ProcMon)
    - Network activity monitors (e.g., Wireshark, tcpdump, TcpView)

Outcome: Students will be able to use the tools mentioned above to safely perform static and dynamic analysis of software (or malware) of potentially unknown origin, including obfuscated malware, to fully understand the software's functionality.

In addition to course syllabi, applications must include examples of hands-on lab exercises to demonstrate that students have achieved mastery of this KU.

## M.3 Operating System Theory

Operating systems (OS) provide the platform on which running software acquires and uses computing resources. Operating systems are responsible for working with the underlying hardware to provide the baseline security capabilities of a system. Understanding the underlying theory of operating system design is critical to cyber operations as operating systems control the operation of a computer and the allocation of associated resources.

Specific topics to be covered in this knowledge unit include, but are not limited to:

* + Privileged vs. non-privileged states; and transitions between them (domain switching)
  + Concurrency and synchronization (e.g., semaphores and locks)
  + Processes and threads, process/thread management, synchronization, inter-process communications
  + Memory management, virtual memory, hierarchical memory schemes
  + Uni-processor and multi-processor interface and support
  + CPU Scheduling
  + File Systems
  + IO issues (e.g., buffering, queuing, sharing, management)
  + Distributed OS issues (client/server, message passing, remote procedure calls, clustering)

Outcome: Students will have a thorough understanding of operating systems theory and implementation. They will be able to understand operating system internals to the level that they could design and implement simple architectural changes to an existing OS.

## M.4 Networking (must include hands-on lab exercises)

Computer and communications networks are the very environment in which cyber operations are conducted. An understanding of these networks is essential to any discussion of cyber operations activities.

Specific topics to be covered in this knowledge unit include, but are not limited to:

* + Routing, network, and application protocols including:
    - TCP/IP (versions 4 and 6)
    - ARP, BGP, SSL/TLS
    - DNS
    - SMTP
    - HTTP
  + Network architectures
  + Network security
  + Wireless network technologies
  + Network traffic analysis
  + Protocol analysis (examining component-to-component communication to determine the protocol being used and what it is doing)
  + Network mapping techniques (active and passive)

Outcome: Students will have a thorough understanding of how networks work at the infrastructure, network and applications layers; how they transfer data; how network protocols work to enable communication; and how the lower-level network layers support the upper ones. They will have a thorough knowledge of the major network protocols that enable communications and data transfer.

## M.5 Cellular and Mobile Technologies

As more communications are conducted via mobile and cellular technologies, these technologies have become critical (and continue to become more critical) to cyber operations. It is important for those involved in cyber operations to understand how data is processed and transmitted using these ubiquitous devices.

Specific topics to be covered in this knowledge unit include, but are not limited to:

* + Overview of smart phone technologies
  + Overview of embedded operating systems (e.g., iOS, Android)
  + Wireless technologies (mobile: GSM, WCDMA, CDMA2000, LTE; and Internet: 802.11b/g/n)
  + Infrastructure components (e.g., fiber optic network, evolved packet core, PLMN)
  + Mobile protocols (SS7, RR, MM, CC)
  + Mobile logical channel descriptions (BCCH, SDCCH, RACH, AGCH, etc.)
  + Mobile registration procedures
  + Mobile encryptions standards
  + Mobile identifiers (IMSI, IMEI, MSISDN, ESN, Global Title, E.164)
  + Mobile and Location-based Services

Outcome: Students will be able to describe user associations and routing in a cellular/mobile network, interaction of elements within the cellular/mobile core, and end-to-end delivery of a packet and/or signal and what happens with the hand-off at each step along the communications path. They will be able to explain differences in core architecture between different generations of cellular and mobile network technologies.

## M.6 Discrete Math and Algorithms

In order for cyber operators to make educated choices when provided with an array of algorithms and approaches to solving a particular problem, there are essential underlying concepts drawn from discrete mathematics, algorithms analysis, and finite automaton with which they should be familiar.

Specific topics to be covered in this knowledge unit include, but are not limited to:

* + Searching and sorting algorithms
  + Complexity theory
  + Regular expressions
  + Computability
  + Mathematical foundations for cryptography
  + Entropy

Outcome: Given an algorithm, a student will be able to determine the complexity of the algorithm and cases in which the algorithm would/would not provide a reasonable approach for solving a problem.

Outcome: Students will understand how variability affects outcomes, how to identify anomalous events, and how to identify the meaning of anomalous events.

Outcome: Students will understand how automata are used to describe computing machines and computation, and the notion that some things are computable and some are not. They will understand the connection between automata and computer languages and describe the hierarchy of language from regular expression to context free.

## M.7 Overview of Cyber Defense (must include hands-on lab exercises)

Cyber operations encompass both offensive and defensive operations. Defensive operations are essential in protecting our systems and associated digital assets. Understanding how defense compliments offense is essential in a well-rounded cyber operations program.

Specific topics to be covered in this knowledge unit include, but are not limited to:

* + Identification of reconnaissance operations
  + Anomaly/intrusion detection
  + Anomaly identification
  + Identification of command and control operations
  + Identification of data exfiltration activities
  + Identifying malicious code based on signatures, behavior and artifacts
  + Network security techniques and components (e.g., firewalls, IDS, etc.)
  + Cryptography (include PKI cryptography) and its uses in cybersecurity
  + Malicious activity detection
  + System security architectures and concepts
  + Defense in depth
  + Trust relationships
  + Distributed/Cloud
  + Virtualization

Outcome: Students will have a sound understanding of the technologies and methods utilized to defend systems and networks. They will be able to describe, evaluate, and operate a defensive network architecture employing multiple layers of protection using technologies appropriate to meet mission security goals.

In addition to course syllabi, applications must include examples of hands-on lab exercises to demonstrate that students have achieved mastery of this KU.

## M.8 Security Fundamental Principles (i.e., "First Principles")

The first fundamental security design principles are the foundation upon which security mechanisms (e.g., access control) can be reliably built. They are also the foundation upon which security policies can be reliably implemented. When followed, the first principles enable the implementation of sound security mechanisms and systems. When not completely followed, the risk that an exploitable vulnerability may exist is increased. A solid understanding of these principles is critical to successful performance in the cyber operations domain.

Specific topics to be covered in this knowledge unit include, but are not limited to:

* + General Fundamental design principles including:
    - Simplicity
    - Open Design
    - Design for Iteration
    - Least Astonishment
  + Security Design Principles including:
    - Minimize Secrets
    - Complete Mediation
    - Fail-safe Defaults
    - Least Privilege
    - Economy of Mechanism
    - Minimize Common Mechanism
    - Isolation, Separation and Encapsulation
  + Methods for Reducing Complexity including:
    - Abstraction
    - Modularity
    - Layering
    - Hierarchy

Outcome: Students will possess a thorough understanding of the fundamental principles underlying cyber security, how these principles interrelate and are typically employed to achieve assured solutions, the mechanisms that may be built from or due to these principles.

Outcome: Given a particular scenario, students will be able to identify which fundamental security design principles are in play, how they interrelate and methods in which they should be applied to develop systems worthy of trust.

Outcome: Students will understand how failures in fundamental security design principles can lead to system vulnerabilities that can be exploited as part of an offensive cyber operation.

## M.9 Vulnerabilities

Vulnerabilities are not random events, but follow a pattern. Understanding the pattern of vulnerabilities and attacks can allow one to better understand protection, risk mitigation, and identify vulnerabilities in new contexts. Vulnerability analysis and it's relation to exploit development are core skills for one involved in cyber operations.

Specific topics to be covered in this knowledge unit include, but are not limited to:

* + Vulnerability taxonomies such as CVE, CWE, OSVDB, and CAPEC
  + Buffer overflows
  + Privilege escalation attacks
  + Input validation issues
  + Password weaknesses
  + Trust relationships
  + Race conditions
  + Numeric over/underflows
  + User-space vs. kernel-space vulnerabilities
  + Local vs. remote access

Outcome: Students will possess a thorough understanding of the various types of vulnerabilities (design and/or implementation weaknesses), their underlying causes, their identifying characteristics, the ways in which they are exploited, and potential mitigation strategies. They will also know how to apply fundamental security design principles during system design, development and implementation to minimize vulnerabilities.

Outcome: Students will understand how a vulnerability in a given context may be applied to alternative contexts and to adapt vulnerabilities so that lessons from them can be applied to alternative contexts.

## M.10 Legal and Ethics

People working in cyber operations must comply with many laws, regulations, directives and policies. Cyber operations professionals should fully understand the extent and limitations of their authorities to ensure operations in cyberspace are in compliance with U.S. law. In addition, cyber operators must have knowledge of cyber ethics for both understanding and applying moral reasoning models to address current and emerging ethical dilemmas on an individual and society.

Specific topics to be covered in this knowledge unit include, but are not limited to:

* + International Law
    - Jus ad bellum
      * United Nations Charter
    - Jus in bello
      * Hague Conventions
      * Geneva Conventions
  + U.S. Laws
    - Constitution
      * Article I (Legislative Branch)
      * Article II (Presidency)
      * Article III (Judiciary)
      * Amendment 4 (Search and Seizure)
      * Article 14 (Due Process)
    - Statutory Laws
      * Title 10 (Armed Forces)
      * Title 50 (War and National Defense)
      * Title 18 (Crimes)
        + 18 USC 1030 (Computer Fraud and Abuse Act)
        + 18 USC 2510-22 Electronic Communications Privacy Act
        + 18 USC 2701-12 Stored Communications Act
        + 18 USC 1831-32 Economic Espionage Acts
  + Cyber Ethics
    - Professional Ethics and Codes of Conduct
    - Social Responsibility
    - Ethical Hacking

Outcome: Given a cyber operations scenario, students will be able to explain the authorities applicable to the scenario.

Outcome: Students will be able to provide a high-level explanation of the legal issues governing the authorized conduct of cyber operations and the use of related tools, techniques, technology, and data.

Outcome: Students will be able to evaluate the relationship between ethics and law, describe civil disobedience and its relation to ethical hacking, describe criminal penalties related to unethical hacking, and apply the notion of Grey Areas to describing situations where law has not yet caught up to technological innovation.

Outcome: Students will be able to describe steps for carrying out ethical penetration testing, describe 'ethical hacking' principles and conditions, distinguish between ethical and unethical hacking, and distinguish between nuisance hacking, activist hacking, criminal hacking, and acts of war.

# Optional Program Content: (Knowledge Units)

At least 10 of the following 17 optional knowledge units must exist in the institutions curriculum and be available to all students during their required course of study. For students to qualify for recognition of completing the cyber operations program they must take courses that meet at least 4 of the institution's mapped 10+ Optional KUs.

## O.1 Programmable Logic (must include hands-on lab exercises)

In digital electronic systems, logic devices provide specific functions, including device-to-device interfacing, data communication, signal processing, data display, timing and control operations, and several other system functions. Logic devices can be fixed, or programmable using a logic language. The advantage of a programmable logic device (PLD) is the ability to use a programmable logic language to implement a design into a PLD and immediately test it in a live circuit.

Specific topics to be covered in this knowledge unit include, but are not limited to:

* + Hardware design/programming languages (e.g. VHSIC Hardware Design Language (VHDL), Verilog, OpenCL)
  + Programmable logic devices (Programmable Logic Controllers (PLC), Fully Programmable Gate Arrays (FPGA))

Outcome: Students will be able to specify digital device behavior using programmable logic language. They will be able to design, synthesize, simulate, and implement logic on an actual programmable logic device. For instance, students will be able to perform parallel computational tasks such as taking multiple cipher cores and running them in parallel to perform password cracking attacks.

## O.2 Wireless Security

(must include hands-on lab exercises)

Wireless systems are essential to enabling mobile users. However, a significant impact in security can result from the use of wireless or the improper configuration of wireless security due to the erratic nature of the wireless environment. The dynamic and inconsistent connectivity of wireless requires unique approaches to networking in everything from user identification and authentication to message integrity and cipher synchronization.

Specific topics to be covered in this knowledge unit include, but are not limited to:

* + A comparison of security implementations in different wireless technologies (e.g., 2G/3G/4G/Wi-Fi/Bluetooth/RFID)
  + Confidentiality, integrity and availability policy enforcement considerations in wireless networks
  + Enumeration issues and methods to limit exposing and identifying cellular, enterprise, device and personal wireless identifiers (e.g. WLAN and cellular beacons, System Information Reports, TMSI)
  + Security protocols used in wireless communications and how each addresses issues of authentication, integrity, and confidentiality (e.g. COMP128, UIA, TKIP, CCMP, SSP, E1)
  + Availability issues in wireless and nuances in different denial-of-service attacks (e.g. energy jamming, carrier sense exploitation, RACH flooding, access management protocol exploitation)
  + Security issues in hardware and software architectures of wireless devices
  + Common ciphers, their implementations, advantages and disadvantages for use in securing wireless networks
    - Stream ciphers (e.g. E0, RC4, A5, SNOW, ZUC)
    - Block ciphers (e.g. Kasumi, SAFER, AES)

Outcome: Students will be able to describe the unique security and operational attributes in the wireless environment and their effects on network communications. They will be able to identify the unique security implications of these effects and how to mitigate security issues associated with them.

Outcome: Students will be able to describe and demonstrate the vulnerabilities with ineffective mechanisms for securing or hiding 802.11 traffic.

Outcome: Students will be able to understand, describe, and implement a secure wireless network that uses modern encryption and enforces the proper authentication of users.

Outcome: Students will be able to compare and contrast mechanisms for association and authentication with a GSM BSC and a UMTS RNC.

## O.3 Virtualization

(must include hands-on lab exercises)

Virtualization technology has rapidly spread to become a core feature of enterprise environments, and is also deeply integrated into many server, client, and mobile platforms. It is also widely used in IT development, research, and testing environments. Virtualization is also a key technology in cyber security. As such a deep technical understanding of the capabilities and limitations of modern approaches to virtualization is critical to cyber operations.

Specific topics to be covered in this knowledge unit include, but are not limited to:

* + Type I and Type II architectures.
  + Virtualization Principles including efficiency, resource control and equivalence
  + Virtualization techniques for code execution, including trap and emulate, binary translation, paravirtualization, and hardware-supported virtualization (e.g., Intel VMX).
  + Management of memory in virtualized systems, including hardware supported memory management (e.g. EPT/SLAT), memory deduplication, and isolation of VM hypervisor and memory spaces
  + Techniques for allocating storage (e.g., hard drives) to Virtual Machines, and the associated capabilities (e.g., snapshots).
  + Techniques for associating hardware (virtual or physical) with virtual machines, including hardware-supported methods (e.g., SR-IOV) and device emulation.
  + Techniques for providing advanced virtualization capabilities, such as live-migration and live-failover.
  + Internal and External Interfaces provided by virtualized platforms for management, monitoring, and internal communication/synchronization.
  + Snapshots, migration, failover

Note: Education focused on simply using VMs or virtualization platforms/tools (such as vSphere, HyperV, or VirtualBox) for efficiency purposes (e.g. server consolidation) is not sufficient to address this KU.

Outcome: Students will understand and be able to describe the technical mechanisms by which virtualization is implemented in a variety of environments, and their implications for cyber operations.

Outcome: Students will be able to enumerate and describe the various interfaces between the hypervisors, VMs, physical and virtual hardware, management tools, networking, storage, and external environments.

## O.4 Cloud Security/Cloud Computing

Cloud resources are commonly used for a wide variety of use cases, including the provision of enterprise services, data processing and analysis, development and testing, and a wide variety of consumer focused services. As such it is important that the students have a clear understanding of the variety, complexity, and capabilities of modern cloud platforms. Cloud computing has implications for cyber operations not only as a potential target, but also as an extensive resource to bring relatively cheap computing power to solve problems (e.g. cracking passwords) which would have been more difficult pre-cloud.

Specific topics to be covered in this knowledge unit include, but are not limited to:

* + Cloud infrastructure components and the interfaces they expose. This should include public/consumer facing interfaces (such as public management APIs) and internal interfaces (such as those to provide automated backup, failover, and accounting)
  + Essential Characteristics of Cloud Platforms and an understanding of the technologies that enable these characteristics
  + Common Service models
  + Common Deployment Modes (e.g. public cloud, private cloud, hybrid cloud) and the associated tradeoffs (e.g. privacy/scalability/resilience)
  + Cloud infrastructure components and the interfaces they expose. This should include public/consumer facing interfaces (such as public management APIs), and internal interfaces (such as those to provide automated backup, failover, and accounting)
  + Techniques for deploying and scaling cloud resources (such as Puppet/Chef)
  + Security implication of cloud resources, including issues associated with shared resources and multi-tenancy, the extension of trust to include the cloud provider, and approaches to mitigating these issues
  + Developing, deploying, and managing applications on cloud resources, which should include hand-on exercises that utilize real cloud services

Recommended Resource for this KU: NIST 800-145

Outcome: Students will understand and be able to describe a variety of cloud service models and deployment modes, and select appropriate service models and delivery modes for a variety of potential workloads, including enumerating the security tradeoffs associated with their selections.

Outcome: Students will be able to develop and deploy a workload in an appropriate cloud environment, including addressing issues associated with deployment, configuration, management, scalability, and security.

## O.5 Risk Management of Information Systems

Risk Management of Information Systems is a critical topic area which forms the basis for applying information system security principles to an operational environment. Risk Management decisions are the embodiment of the organization's security culture and values as demonstrated through the willingness to commit resources to information system security capabilities.

Given the significant and growing danger of cyber security threats, it is imperative that all levels of an organization understand their responsibilities for achieving adequate information security and for managing information system-related security risks.

Specific topics to be covered in this knowledge unit include, but are not limited to:

* + Risk Models (e.g. NIST SP 800-39 Managing Information Security Risk)
  + Risk Processes (e.g. NIST SP 800-37 Risk Management Framework)

Outcome: Students will be able to identify, measure (quantitative and qualitative), and mitigate key information technology risks.

Outcome: Students will also be able to describe each of the tasks associated with risk framing, assessment, response and monitoring.

## O.6 Computer Architecture

(includes Logic Design)

This knowledge unit ensures students understand the components that comprise a computing system and possess the ability to assess processor design and organization alternatives as they impact functionality and performance of a system.

Specific topics to be covered in this knowledge unit include, but are not limited to:

* + Organization of computer and processor architectures
  + Instruction set design alternatives
  + Processor implementation
  + Memory system hierarchy
  + Buses
  + I/O systems
  + Factors affecting performance

Outcome: Students will be able to define devices of electronic digital circuits and describe how these components are interconnected. They will be able to integrate individual components into a more complex digital system and understand the data path through a CPU.

## O.7 Microcontroller Design

(must include hands-on lab exercises)

A microcontroller (or MCU, short for microcontroller unit) is a small, simple computer on a single integrated circuit containing a processor core, limited memory, and programmable input/output peripherals and sensors. Microcontrollers are typically inexpensive and have little or no interface for human interaction. They are typically programmed for a fixed function with little or no change over their lifecycle.

Specific topics to be covered in this knowledge unit include, but are not limited to:

* + Typical instruction sets and architectures
  + Common programming environments for microcontrollers
  + How the real-time requirements and simple architecture of the typical microcontroller require special programming considerations
  + Cyber considerations and issues related to microcontrollers and the larger systems they are typically integrated into

Outcome: Students are knowledgeable of the concepts, methods, techniques, technologies, requirements, and development tools commonly used in the design and implementation of microcontroller applications. They will be able to develop or make a substantial modification to a simple microcontroller-based system and identify the cyber concerns associated with such a system.

## O.8 Software Security Analysis

(must include hands-on lab exercises)

This knowledge unit ensures that students will possess the ability to analyze software for the presence of weaknesses that may lead to exploitable vulnerabilities in operational systems.

Specific topics to be covered in this knowledge unit include, but are not limited to:

* + Source code analysis
  + Binary code analysis
  + Static code analysis techniques
  + Dynamic code analysis techniques
  + Testing methodologies (Black Box/White Box/Fuzz)

Outcome: Students will be able to perform analysis of existing source code for functional correctness. Through the application of testing methodologies, students should be able to build test cases that demonstrate the existence of vulnerabilities. For example, students could apply industry standard tools that analyze software for security vulnerabilities.

#### O.9 Secure Software Development (Building Secure Software)

(must include hands-on lab exercises)

This knowledge unit ensures that students know how to write robust, secure software. These methods taught in this class should lead to software that maintains the Confidentiality, Integrity and Availability of the software and data.

Specific topics to be covered in this knowledge unit include, but are not limited to:

* + Secure programming principles and practices
  + Constructive techniques (What process might provide for "good code.")

Outcome: Students should be able to demonstrate that they understand the techniques specifying program behavior, the classes of well-known defects, and how they manifest themselves in various languages.

Outcome: Students will understand how poor coding affects security and can identify common coding errors. Students will demonstrate that they are capable of authoring programs that are free from defects and can document their code with clear and succinct explanations, so other people can enhance and maintain the developed code.

## O.10 Embedded Systems (must include hands-on lab exercises)

An embedded system is a computer system with a dedicated function within a larger mechanical or electrical system, often with real-time computing constraints. It includes a microprocessor, memory, and peripherals either packaged as an SOC or as separate components within the device. It is embedded as part of a complete device often including hardware and mechanical parts. It typically has more robust user interaction than a microcontroller. The embedded system's function typically changes very little, if at all, over the lifecycle of an instance of the system. Examples of embedded systems would include a wireless router or military weapons systems.

Specific topics to be covered in this knowledge unit include, but are not limited to:

* + Typical instruction sets and architectures
  + Common operating systems and programming environments for embedded systems
  + How the real-time requirements typical of embedded systems require differences in the OS & applications
  + Cyber considerations and issues related to embedded systems

Outcome: Students are knowledgeable of the concepts, methods, techniques, technologies, requirements, and development tools commonly used in the design and implementation of embedded systems. They will be able to develop or make a substantial modification to a simple embedded system and identify the cyber concerns associated with such an embedded system.

## O.11 Digital Forensics (must include hands-on lab exercises)

Digital forensics is the recovery and investigation of material found in various cyber environments (e.g. networks, memory, operating systems, etc.). The focus of this KU is on the digital forensics process and technology (tools and techniques) not the legal aspect (such as chain of custody or preparing evidence for court).

Broad coverage of all the below topics and in-depth coverage, including hands-on-experience, of at least one of the below topics must be covered:

* + Operating system forensics
  + Device/Media forensics
  + Network forensics
  + Memory forensics

Outcome: Students will be able to understand a user's activity, determine the manner in which an operating system or application has been subverted, recover "deleted" and/or intentionally hidden information from various types of media, and demonstrate proficiency with handling a large number of different kinds of devices.

Outcome: Students will be able to understand how to identify forensic artifacts left by attacks.

Outcome: Students will be able to understand how to acquire a forensically sound image.

## O.12 Systems Programming (must include hands-on lab exercises)

This knowledge unit ensures that students will be proficient in programming systems software (i.e., software that interacts with the system hardware and/or other low-level system components that interact with the hardware). Systems programming usually uses a low-level programming language (e.g., C, assembly) that allows efficient use of core resources. Systems programming is sufficiently different from applications programming such that programmers tend to specialize in one or the other.

Specific topics to be covered in this knowledge unit include, but are not limited to:

* + Kernel modules
  + Device drivers
  + Multi-threading
  + Use of alternate processors (e.g., graphics card processors)

Outcome: Students will be able to build and integrate kernel modules, understand the system call mechanism and how malicious software subverts system calls. They should demonstrate sufficient knowledge of the networking stack to be able to construct network filter components. They will also be able to discuss strengths and weaknesses of alternative processors and demonstrate familiarity of tool sets for making use of alternative processors (e.g., GPUs).

## O.13 Applied Cryptography

In cyber operations it is critical to understand the role of keys, cryptographic algorithms, and protocols as they relate to security (attacks and defenses) in complex real-life systems.

Specific topics to be included in this knowledge unit include, but are not limited to:

* + Cryptographic primitives (e.g. randomization)
  + Symmetric and asymmetric cryptography, hash functions and data integrity, public-key encryption and digital signatures, key establishment and key management
  + The appropriate application of different types of cryptography to Internet security, computer security and communications security

Outcome: Students will be able to identify the appropriate uses of symmetric and asymmetric encryption. They will be able to assign some measure of strength to cryptographic algorithms and the associated keys.

Outcome: Students will understand the common pitfalls or shortcomings associated with the implementation of cryptography, and will understand the challenges and limitations of current key management systems.

Outcome: Given an enterprise architecture scenario consisting of different components (e.g. servers, clients, databases) with information that has various temporal and distribution constraints, networks, multiple sites, and trusted and untrusted clients, students will describe the appropriate cryptographic tools/algorithms/protocols that can be applied at various locations throughout that architecture in order to achieve a variety of goals, and the management challenges/tradeoffs associated with their choices.

## O.14 Industrial Control System (ICS)

ICSs are crucial to the operations of U.S. critical infrastructures that are often widely deployed, interconnected and mutually dependent systems. ICSs can include Supervisory Control and Data Acquisition (SCADA) systems and Distributed Control Systems (DCS), and other control system configurations. Several infrastructures that use ICSs have critical national security impact including electric, water and wastewater, oil and natural gas, transportation, chemical, and aerospace. Cyber operators should have knowledge of the attack and defense of ICSs.

Specific topics to be included in this knowledge unit include, but are not limited to:

* + SCADA
  + DCS
  + Vulnerabilities, countermeasures and attacks of ICS ecosystems

Outcome: Students will have an overall comprehension of key U.S. infrastructures controlled by ICS including the associated vulnerabilities associated with each infrastructure.

Outcome: Students will be able to describe how embedded systems are employed in industrial infrastructures and control systems. They will be able to identify means for capturing instrument telemetry and identifying feedback controls. They should be able to describe methods for managing distributed nodes and identify potential security vulnerabilities associated with the use of such systems and means for mitigating these vulnerabilities.

Outcome: Students will be able to demonstrate the ability to discover and understand an ICS environment and identify the attack surface.

## O.15 User Experience (UX)/Human Computer Interface (HCI) Security

HCI is the practice and study of human interaction with machines. This includes usability, machine interaction design, and psychological reactions to the interface. UX deals with the entirety of the user experience relative to a product (not just the user interface). UX includes HCI but also encompasses the emotional, physical, and behavioral perception of a product or service. Cyber security professionals must acknowledge that while they need to give utmost precedence to system security, they cannot overlook user experience, and vice versa.

Specific topics to be included in this knowledge unit include, but are not limited to:

* + Authentication interfaces and passwords
  + Implicit and explicit policies in systems
  + Policies that users control and hidden policies controlled by the system
  + The role of social engineering and how it continues to be the primary attack vector
  + How implementing security affects the user experience.

Outcome: Students will understand user interface issues that will affect the implementation of and perception of security mechanisms and the behavioral impacts of various security "policies."

Outcome: Students will understand the tension between user security and convenience which results in user behavior that undermines system security. Students will learn how to develop approaches which have the right balance.

## O.16 Offensive Cyber Operations

Offensive cyber operations is everything related to reconnaissance and exploitation in the cyber space offensive mission. This knowledge unit provides a high-level overview of the different phases of cyber operations including target identification, reconnaissance, fingerprinting, development of operational plans, decision authorities/authorization, execution, and assessment.

Specific topics to be included in this knowledge unit include, but are not limited to:

* + Cyber attacks are restricted to military members of DoD, as restricted by international law. Authorities are derived from U.S. Code Title 10.
  + Cyber kill chain
  + Mission planning and execution process
  + Define mission objectives and desired effects from the overall mission standpoint
  + The different phases of cyber operations

Outcome: Students will understand the phases of a cyber operation, what each phase entails, who has authorities to conduct each phase, and how operations are assessed after completion.

## O.17 Hardware Reverse Engineering

(must include hands-on lab exercises)

Hardware Reverse Engineering is the study of hardware hacking and reverse engineering approaches that are routinely used against electronic devices and embedded systems. This knowledge unit provides students with an introduction to the basic procedures necessary to perform reverse engineering of hardware components to determine their functionality, inputs, outputs, and stored data.

Specific topics to be included in this knowledge unit include, but are not limited to:

* + Hardware reverse engineering methodology
  + The use of tools and test measurement equipment
  + Circuit board analysis and modification
  + Embedded security
  + Common hardware attack vectors

Outcome: Students will understand basic fundamental procedures such as probing, measuring, and data collection to identify functionality and to affect modifications to the hardware functionality.

Outcome: Students will understand the proper use of evaluation tools and common hardware attack vectors.

# Schools with 4-year degree in Cyber Operations CAE Designation

Copied from <https://www.nsa.gov/resources/students-educators/centers-academic-excellence/cae-co-centers/>

* **Cedarville University (Ohio)**
* **Dakota State University (South Dakota)**
* **Northeastern University (Massachusetts)**
* **Old Dominion University (Virginia)**
* **Texas A&M University (Texas)**
* **Towson University (Maryland)**
* **United States Air Force Academy (Colorado)**
* **University of Arizona (Arizona)**
* **University of Nebraska Omaha (Nebraska)**
* **University of New Haven (Connecticut)**
* **University of Texas at El Paso (Texas)**
* **University of Texas at San Antonio (Texas)**
* **Virginia Polytechnic Institute and State University (Virginia)**

Total of 13 listed in alphabetical order. Closest one is Dakota State or University of Arizona other than Airforce Academy.

## Cedarville University BS in Computer Science with Specialization in Cyber Operations

Copied from <https://www.cedarville.edu/Academic-Programs/Cyber-Operations.aspx> but still looking for courses.

## Dakota State University Cyber Operations BS

System-wide General Education Requirement (30 Credits)

Majors who test directly into MATH 201 will not need to complete MATH 114, but must take 3 credits of general electives.

**Required Courses (78 Credits)**

[CIS 275 - Web Application Programming I](https://catalog.dsu.edu/preview_program.php?catoid=29&poid=2108&returnto=1397) 3 credits

[CIS 375 - Web Application Programming II](https://catalog.dsu.edu/preview_program.php?catoid=29&poid=2108&returnto=1397) 3 credits

[CSC 105 - Introduction to Computers](https://catalog.dsu.edu/preview_program.php?catoid=29&poid=2108&returnto=1397) 3 credits

[CSC 134 - Introduction to Cyber Operations](https://catalog.dsu.edu/preview_program.php?catoid=29&poid=2108&returnto=1397) 3 credits

[CSC 150 - Computer Science I](https://catalog.dsu.edu/preview_program.php?catoid=29&poid=2108&returnto=1397) 3 credits

[CSC 234 - Software Security](https://catalog.dsu.edu/preview_program.php?catoid=29&poid=2108&returnto=1397) 3 credits

[CSC 250 - Computer Science II](https://catalog.dsu.edu/preview_program.php?catoid=29&poid=2108&returnto=1397) 3 credits

[CSC 300 - Data Structures](https://catalog.dsu.edu/preview_program.php?catoid=29&poid=2108&returnto=1397) 3 credits

[CSC 314 - Assembly Language](https://catalog.dsu.edu/preview_program.php?catoid=29&poid=2108&returnto=1397) 3 credits

[CSC 321 - Information Security Management](https://catalog.dsu.edu/preview_program.php?catoid=29&poid=2108&returnto=1397) 3 credits

[CSC 328 - Operating Environments](https://catalog.dsu.edu/preview_program.php?catoid=29&poid=2108&returnto=1397) 3 credits

[CSC 163 - Hardware, Virtualization, and Data Communication](https://catalog.dsu.edu/preview_program.php?catoid=29&poid=2108&returnto=1397) 3 credits

[CSC 285 - Networking I](https://catalog.dsu.edu/preview_program.php?catoid=29&poid=2108&returnto=1397) 3 credits

[CSC 385 - Networking II](https://catalog.dsu.edu/preview_program.php?catoid=29&poid=2108&returnto=1397) 3 credits

[CSC 404 - Foundation of Computation](https://catalog.dsu.edu/preview_program.php?catoid=29&poid=2108&returnto=1397) 3 credits

[CSC 420 - Cellular and Mobile Communications](https://catalog.dsu.edu/preview_program.php?catoid=29&poid=2108&returnto=1397) 3 credits

[CSC 428 - Reverse Engineering](https://catalog.dsu.edu/preview_program.php?catoid=29&poid=2108&returnto=1397) 3 credits

[CSC 432 - Malware Analysis](https://catalog.dsu.edu/preview_program.php?catoid=29&poid=2108&returnto=1397) 3 credits

[CSC 436 - Offensive Network Security](https://catalog.dsu.edu/preview_program.php?catoid=29&poid=2108&returnto=1397) 3 credits

[CSC 437 - Survey of Enterprise Systems](https://catalog.dsu.edu/preview_program.php?catoid=29&poid=2108&returnto=1397) 3 credits

[CSC 438 - Defensive Network Security](https://catalog.dsu.edu/preview_program.php?catoid=29&poid=2108&returnto=1397) 3 credits

[CSC 456 - Operating Systems](https://catalog.dsu.edu/preview_program.php?catoid=29&poid=2108&returnto=1397) 3 credits

[MATH 201 - Introduction to Discrete Mathematics](https://catalog.dsu.edu/preview_program.php?catoid=29&poid=2108&returnto=1397) 3 credits

CIS/CSC 300/400 or MATH 123 and above, except CIS 350. (9 credits)

**Electives (12 Credits)**

**Copied from** <https://dsu.edu/programs/cyber-operations-bs.html>

## North Eastern University BS Computer Science with Cyber Operations Concentration

Not sure if this degree is still valid? Can’t find specific stuff on this program. They have a cybersecurity degree, but no program requirements.

List of cyber classes here <http://catalog.northeastern.edu/undergraduate/computer-information-science/cybersecurity/#coursestext>

List of computer science classes here <http://catalog.northeastern.edu/undergraduate/computer-information-science/computer-science/#coursestext>

Old Dominion University BS in Interdisciplinary Studies, Cyber Operations Major

They have both CAE-CDE and CAE-CO designations. They have maps for both in their cybersecurity program <https://www.odu.edu/ccser>

Program requirements for Cyber Operations <http://catalog.odu.edu/undergraduate/collegeofartsletters/interdisciplinarystudies/bs-ids---cybersecurity/>

Lower-Division General Education

Written Communication \* 6

Oral Communication 3

Mathematics (MATH 211 and MATH 212 required) 8

Language and Culture 0-6

Information Literacy and Research 3

Human Creativity 3

Interpreting the Past 3

Literature 3

Philosophy and Ethics (met in the major by PHIL 355E)

The Nature of Science 8

Impact of Technology (met in the major by CYSE 200T)

Human Behavior (CRJS 215S or SOC 201S required) 3

Prerequisites 22

CS 150 Problem Solving and Programming I

CS 170 Introduction to Computer Architecture I

CS 250 Problem Solving and Programming II

CS 252 Introduction to Unix for Programmers

CS 270 Introduction to Computer Architecture II

ECE 241 Fundamentals of Computer Engineering

ECE 304 Probability, Statistics, and Reliability

Core Courses 12

CYSE 200T Cybersecurity, Technology, and Society

CYSE 301 Cybersecurity Techniques and Operations

CYSE 425W Cybersecurity Strategy and Policy

CYSE/CRJS 406 Cyber Law

Major Coursework 39

CS 361 Data Structures and Algorithms

CS 390 Introduction to Theoretical Computer Science

CS 466 Principles and Practice of Cyber Defense

CS 467 Introduction to Reverse Software Engineering

CS 471 Operating Systems

CYSE 368 Cybersecurity Internship

or IDS 493 IDS Electronic Portfolio Project

ECE 346 Microcontrollers

ECE 355 Introduction to Networks and Data Communications

ECE 416 Cyber Defense Fundamentals

ECE 419 Cyber Physical System Security

ECE 455 Network Engineering and Design

MSIM 470 Foundations of Cyber Security

PHIL 355E Cybersecurity Ethics

Approved Program Electives (Choose two) 6

CS 476 Systems Programming

CYSE 407 Digital Forensics

ECE 483 Embedded Systems

IT 417 Management of Information Security

Elective Credit as Needed for the Required 120 Credit Hours 1

Total Hours 120-126

Copied from

<http://catalog.odu.edu/undergraduate/collegeofartsletters/interdisciplinarystudies/cyberoperations/>

Website has link to catalog for course descriptions for most courses.

## University of Texas A&M BS in Computer Science, Minor in Cybersecurity

<https://catalog.tamu.edu/undergraduate/engineering/computer-science/bs/#programrequirementstext>

First Year

Fall Semester Credit Hours

CHEM 107 General Chemistry for Engineering Students 1,4 3

CHEM 117 General Chemistry for Engineering Students Laboratory 1,4 1

ENGL 103

or ENGL 104

Introduction to Rhetoric and Composition 1

or Composition and Rhetoric 3

ENGR 102 Engineering Lab I - Computation 1 2

MATH 151 Engineering Mathematics I 1,2 4

University Core Curriculum 3 3

Semester Credit Hours 16

Spring

CHEM 120 Fundamentals of Chemistry II 1,4 4

ENGR 216/PHYS 216 Experimental Physics and Engineering Lab II - Mechanics 1 2

MATH 152 Engineering Mathematics II 1 4

PHYS 206 Newtonian Mechanics for Engineering and Science 1 3

University Core Curriculum 3,5 3-6

Semester Credit Hours 15-16

Total Semester Credit Hours 31-32

Second Year

Fall Semester Credit Hours

CSCE 121 Introduction to Program Design and Concepts 1 4

CSCE 181 Introduction to Computing 1 1

CSCE 222/ECEN 222 Discrete Structures for Computing 1 3

MATH 304 Linear Algebra 1 3

General elective 6 1

Science elective 6,7 4

Semester Credit Hours 16

Spring

CSCE 221 Data Structures and Algorithms 1 4

CSCE 312 Computer Organization 1 4

CSCE 314 Programming Languages 1 3

Select one from: 3

COMM 203 Public Speaking

COMM 205 Communication for Technical Professions

ENGL 210 Technical and Business Writing

Concentration area elective 8 3

Semester Credit Hours 17

Third Year

Fall

CSCE 313 Introduction to Computer Systems 1 4

CSCE 315 Programming Studio 1 3

CSCE 481 Seminar 1 1

STAT 211 Principles of Statistics I 3

University Core Curriculum 3 3

Concentration area elective 8 3

Semester Credit Hours 17

Spring

CSCE 411 Design and Analysis of Algorithms 3

Select one from: 1 3

MATH 251 Engineering Mathematics III

MATH 302 Discrete Mathematics

MATH 308 Differential Equations

High Impact Experience 10 0

CSCE 399 High-Impact Experience

Science elective 7 3

Computer science elective 9 6

Semester Credit Hours 15

Fourth Year

Fall

University Core Curriculum 3 3

Computer science elective 9 9

Concentration area elective 8 3

Semester Credit Hours 15

Spring

CSCE 482 Senior Capstone Design 1 3

University Core Curriculum 3 6

Computer science elective 9 3

Concentration area elective 8 3

Semester Credit Hours 15

Total Semester Credit Hours 95

## Townson University BS Computer Science Cyber Operations Track

Required Computer Science Courses

CIS 377 INFORMATION SYSTEMS SECURITY 3

COSC 236 INTRODUCTION TO COMPUTER SCIENCE I 1 4

COSC 237 INTRODUCTION TO COMPUTER SCIENCE II 4

COSC 290 PRINCIPLES OF COMPUTER ORGANIZATION 4

COSC 336 DATA STRUCTURES AND ALGORITHM ANALYSIS 4

COSC 350 DATA COMMUNICATIONS AND NETWORKING 3

COSC 412 SOFTWARE ENGINEERING 3

COSC 439 OPERATING SYSTEMS 3

COSC 455 PROGRAMMING LANGUAGES: DESIGN & IMPLEMENTATION 3

COSC 457 DATABASE MANAGEMENT SYSTEMS 3

Required Math Courses

MATH 263 DISCRETE MATHEMATICS 3-4

or MATH 267 INTRODUCTION TO ABSTRACT MATHEMATICS

MATH 273 CALCULUS I 4

MATH 274 CALCULUS II 4

MATH 314 INTRODUCTION TO CRYPTOGRAPHY 3

MATH 330 INTRODUCTION TO STATISTICAL METHODS 4

Required Cyber Operations Track Courses

COSC 310 SPECIAL TOPICS: ADVANCED PROGRAMMING 3

COSC 440 OPERATING SYSTEMS SECURITY 3

COSC 450 NETWORK SECURITY 3

COSC 458 APPLICATION SOFTWARE SECURITY 3

COSC 481 CASE STUDIES IN COMPUTER SECURITY 3

COSC 485 REVERSE ENGINEERING AND MALWARE ANALYSIS 3

Science Requirement

Select two lab science courses from the following (the courses do not need to form a sequence): 8

ASTR 161 THE SKY AND THE SOLAR SYSTEM

ASTR 181 STARS, GALAXIES, AND THE EARLY UNIVERSE

BIOL 200 & 200L INTRODUCTION TO CELLULAR BIOLOGY AND GENETICS [LECTURE]

and INTRODUCTION TO CELLULAR BIOLOGY AND GENETICS [LAB]

BIOL 202 INTRODUCTION TO ECOLOGY AND EVOLUTION

CHEM 131 & 131L GENERAL CHEMISTRY I LECTURE and GENERAL CHEMISTRY I LABORATORY

CHEM 132 & 132L GENERAL CHEMISTRY II LECTURE and GENERAL CHEMISTRY II LABORATORY

GEOL 121 PHYSICAL GEOLOGY

PHYS 241 GENERAL PHYSICS I CALCULUS-BASED

PHYS 242 GENERAL PHYSICS II CALCULUS-BASED

Other Requirements

Must be completed with a grade equivalent of 2.00 or higher.

COMM 131 PUBLIC SPEAKING (Core 5) 3

COSC 418 ETHICAL AND SOCIETAL CONCERNS OF COMPUTER SCIENTISTS (Core 14) 3

ENGL 317 WRITING FOR BUSINESS AND INDUSTRY (Core 9) 3

Total Units 87-88 (doesn’t include general education)

Copied from <https://catalog.towson.edu/undergraduate/fisher-science-mathematics/computer-information-sciences/computer-science-cyber-operations/>

Individual courses have links to catalog information at that page.

US Airforce Academy BS Computer Science

|  |  |  |  |
| --- | --- | --- | --- |
| 4th CLASS YEAR (FRESHMAN) | 3RD CLASS YEAR (SOPHOMORE) | 2ND CLASS YEAR (JUNIOR) | 1ST CLASS YEAR (SENIOR) |
| For Lang 1  Beh Sci 110  History 100  Math 141  *Comp Sci 110*  For Lang 2  Chem 100  English 111  Math 142  Physics 110  Leadership 100 | *Comp Sci 210*  MSS 251  ECE 315  Physics 215  English 211  *Comp Sci 220*  ECE 281  Math 340  Law 220  P / C / B Option 2  Mech Engr 220  Leadership 200 | Cyber Sci 333  *Comp Sci 467*  ECE 382  Pol Sci 211  History 300  Econ 201  Cyber Sci 334  Cyber Sci  Elective 1  *Comp Sci 483*  Philos 310  Math 356  Adv Open Option  Leadership 300 | Cyber Sci 435  Cyber Sci 438  *Comp Sci 431*  Aero Engr 315  Soc Sci 311  Cyber Sci 439  ECE 348  Cyber Sci Elective 2  Astro Engr 310  Adv SocioCultural Op  Leadership 400 |

Copied from <https://www.usafa.edu/academic/cyber-science/>

Bottom of that page has a link to their catalog

## University of Arizona BAS Cyber Operations (three separate tracks – Engineering, Law and Policy, Defense & Forensics)

Access all three tracks here <http://cyber-operations.uas.arizona.edu/>.

Year Three

FIFTH SEMESTER

Courses Units

BASV 314 Mathematics for Applied Sciences 3

CYBV 385 Introduction to Cyber Operations 3

BASV 326 Introductory Methods of Network Analysis 3

INFV 320 Computational Thinking & Doing 3

Tier II General Education 3

Total 15

SIXTH SEMESTER

Courses Units

ENGV 308 Technical Writing 3

CYBV 388 Cyber Investigations & Forensics 3

CYBV 400 Active Cyber Defense 3

Tier II General Education 3

Total 12

Year Four

SEVENTH SEMESTER

Courses Units

BASV 329 Cyber Law, Ethics & Policy 3

CYBV 435 Cyber Threat Intelligence 3

CYBV 477 Advanced Cyber Forensics\*

\*Student can choose to focus by taking CYBV 436, 473, 477, or 481 3

Tier II General Education 3

Total 12

EIGHTH SEMESTER

Courses Units

CYBV 454 Malware Threats & Analysis 3

CYBV 480 Cyber Warfare 3

CYBV 498 Cyber Operations Senior Capstone 3

Tier II General Education 3

Total 12

There is a reference to the first two years as an AAS. Couldn’t find that link easily.

<http://cyber-operations.uas.arizona.edu/content/defense-and-forensics-schedule>

## University of Nebraska Omaha BS in Cybersecurity

|  |  |
| --- | --- |
| Required Knowledge Units (KU) | UNO courses that cover all the required KUs |
| * Low-Level Programming Languages * Software Reverse Engineering * Operating System Theory * Networking * Cellular and Mobile Technologies * Discrete Math and Algorithms * Overview of Cyber Defense * Security Fundamental Principles (i.e. “First Principles”) * Vulnerabilities * Legal | 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 |
| Software Security Analysis | No additional courses required |
| Secure Software Development (Building Secure Software) | No additional courses required |
| 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 |
| Offensive Cyber Operations | No additional courses required |

Copied from <https://www.unomaha.edu/college-of-information-science-and-technology/school-of-interdisciplinary-informatics/cybersecurity/bs-cyber-operations.php>

## University of New Haven BS in Cybersecurity and Networks

University Core Curriculum

Core Tier 1

CC 1.1: ENGL 1112 or ENGL 1113

CC 2.1: COMM 1130

CC 3.1: MATH 1115

CC 4.1: PHYS 1103 or PHYS 1150

CC 5.1: UNIV 1141

CC 6.1: any approved course from competency 6

CC 7.1: CSCI 3316

CC 8.1: any approved course from competency 8

CC 9.1: any approved course from competency 9

Core Tier 2

CC 5.2: CSCI 1110

CC 5.2 or 7.2: ECON 1133 or ECON 1134

Six additional credits from any Tier 2 course

Required Major Courses

ELEC 1155 - Digital Systems I

CSCI 1166 - Discrete Mathematics for Computing

CSCI 2210 - Java Programming

CSCI 2215 - Databases and SQL

CSCI 3320 - Operating Systems

ELEC 3330 - Computer Architecture

CSCI 3331 - Computer Organization Lab

CSCI 3347 - Network Essentials and Technologies

CSCI 3351 - Script Programming/Python

CSCI 3398 - Computer Science Internship

CSCI 4445 - Unix Network Administration

CSCI 4482 - Wireless Networks

CSCI 4497 - Capstone Software Project I

CSCI 4498 - Capstone Software Project II

CSCI Programming Elective

CSCI elective 3000 level or higher

CSCI elective 4000 level or higher

Other Requirements

EASC 1107 - Introduction to Engineering

MATH 1117 - Calculus I or laboratory science restricted elective

MATH 2228 - Elementary Statistics

Business restricted elective (see definition below)

Three restricted electives (see definition below)

Free elective (CC W if not taken elsewhere)

Free elective

Definitions of elective categories and restrictions:

Programming elective: CSCI 2212, 2226, or any higher-level CSCI course that emphasizes programming

Laboratory Science elective: CHEM 1115/1117 or BIOL 1121 or BIOL 2253 or ENVS 1101/1102

Business restricted elective: EASC 2232, ECON 1133, ECON 1134, BUSL 1101, ACCT 1101, or MGMT 2210

Restricted elective: any course approved by the advisor that supports the student’s academic focus

Free elective: any college course that is beyond the level that is considered as remedial in this program, and does not duplicate material of another required or elective course. Remedial courses are those below the level of ENGL 1105, MATH 1115, CHEM 1115, PHYS 1100, and BIOL 1121

National Security Agency Accredited Designation

The National Security Agency has designated the University of New Haven as a National Center of Academic Excellence (CAE) in Cyber Operations Fundamentals in the following two programs:

Bachelor of Science in Computer Science, NSA Cyber Operations Fundamentals Focus Area

Bachelor of Science in Cybersecurity and Networks, NSA Cyber Operations Fundamentals Focus Area

You can earn your degree with the National Security Agency accredited designation of NSA Cyber Operations Fundamentals Focus Area by completing one of these two named degree programs. Doing so will complete the NSA Cyber Operations Focus Area Mandatory Knowledge Units plus these five Optional Knowledge Units: Computer Architecture with Logic Design, Software Security Analysis, Secure Software Development, Digital Forensics and Systems Programming.

To fulfill the Bachelor of Science in Cybersecurity and Networks, NSA Cyber Operations Fundamentals Focus Area, in addition to completing the University’s core curriculum, and the courses required by Bachelor of Science in Cybersecurity and Networks, the following courses are required. These courses are used to fulfil the program’s Tier 2 electives, CSCI electives, restricted electives, and electives. This program and focus area require a total of 122 credits.

CSCI 2226 Data Structures and Algorithms 3

CSCI 3326 Algorithm Design and Analysis 3

CSCI 4434 Assembly Language Programming 3

CSCI 4438 Small Scale Digital Forensic Science 3

CSCI 4448 Reverse Engineering 3

CSCI 4449 Ethical Hacking 3

CSCI 4526 Advanced C++/OOPP 3

CSCI 4536 Structure of Programming Languages 3

CSCI 4538 Memory Forensics 3

CSCI 4547 Systems Programming 3

These math courses are needed to complete the above courses:

MATH 1118 Calculus II (requires MATH 1117 Calculus I for one University Core Tier 2 requirement 4

MATH 3311 Linear Algebra – preferred 4

<http://catalog.newhaven.edu/preview_program.php?catoid=20&poid=4099>

<https://www.newhaven.edu/engineering/undergraduate-programs/cybersecurity-networks/>

## University of Texas El Paso BS in Computer Science

Required Credits: 120

University Core Curriculum

Complete the University Core Curriculum requirements. 42

Computer Science Designated Core (All courses require a grade of C or better.)

Required Courses:

PHYS 2420 Introductory Mechanics 4

MATH 1411 Calculus I 4

Select one of the following lecture/lab combinations: 4

BIOL 1305 & BIOL 1107 General Biology and Topics in Study of Life I

BIOL 1306 & BIOL 1108 Organismal Biology and Organismal Biology Laboratory

ASTR 1307 & ASTR 1107 Elem Astronomy-Solar System and Astronomy Lab I

CHEM 1305 & CHEM 1105 General Chemistry and Laboratory for CHEM 1305

CHEM 1306 & CHEM 1106 General Chemistry and Laboratory for CHEM 1306

GEOL 1313 & GEOL 1103 Intro to Physical Geology and Lab for GEOL 1313

GEOL 1314 & GEOL 1104 Intro to Historical Geol and Lab for GEOL 1314

PHYS 2421 Introductory Electromagnetism

Computer Science Core (All courses require a grade of C or better.)

Required Courses:

CS 1301 & CS 1101 Intro to Computer Science and Intro to Computer Science Lab 4

CS 2302 Data Structures 3

CS 2401 Elem. Data Struct./Algorithms 4

EE 2169 Laboratory for EE 2369 1

EE 2369 Digital Systems Design I 3

MATH 1312 Calculus II 3

MATH 2300 Discrete Mathematics 3

Computer Science Major

Required Courses:

CS 3195 Junior Professionl Orientation 1

CS 3331 Adv. Object-Oriented Programng C 3

CS 3350 Automata/Computabi/Formal Lang 3

CS 3360 Design/Implementation Prog Lan 3

CS 3432 Comp Arch I: Comp Org/Design C 4

CS 4310 Software Eng: Requirements Eng C 3

CS 4311 Software Eng: Design & Implmnt 3

CS 4342 Data Base Management 3

CS 4375 Theory of Operating Systems 3

MATH 3323 Matrix Algebra 3

Statistics:

Select one of the following: 3

EE 3384 Probabilistic Methods-Engr/Sci

STAT 3320 Probability and Statistics

STAT 3330 Probability Additional Mathematics or Science Option:

Option A: Mathematics (Select one course from the following):

MATH 2313 Calculus III

MATH 2325 Intro. to Higher Mathematics

MATH 2326 Differential Equations

MATH 3320 Actuarial Mathematics

MATH 3325 Principles of Mathematics

MATH 4329 Numerical Analysis

STAT 3381 Nonparametric Statistics

STAT 4380 Statistics I

STAT 4385 Applied Regression Analysis

Option B: An additional 3 credit lecture course from the list of science courses above

Technical Electives:

Select 15 hours from the following: 1 15

CS 1190 Special Topics in Computing 1

CS 1290 Special Topics in Computing 2

CS 3000 or 4000 level course

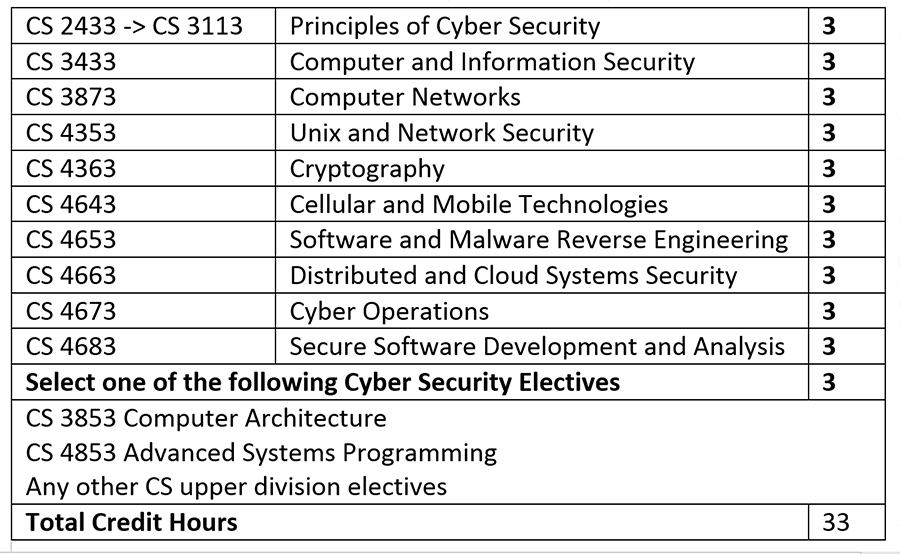
Free Electives:

Complete four additional hours of free electives 2 4

Total Hours 120

<http://catalog.utep.edu/undergrad/college-of-engineering/computer-science/computer-science-bs/>

## University of Texas San Antonio



Flow chart diagram of the courses for the full degree available in a PDF here

<https://cs.utsa.edu/sites/default/files/2019-01/cs-bs-courseSequenceGraph-CYBERSECURITY-181207.pdf>

## Virginia Tech Degree – Computer Engineering Cybersecurity Minor

<https://www.cyber.vt.edu/edu-ugrad.html>

Requirements

One of the following networks courses:

ECE 4564: Network Application Design

CS 4254: Computer Network Arch and Programming

CS 4244 Internet Software Development

ECE 4614: Telecommunication Networks

One of the following computer systems courses:

CS 3214: Computer Systems

CS/ECE 4504: Computer Organization

ECE 3574: Applied Software Engineering

Two core security courses:

ECE 4560: Network Security Fundamentals

CS 4264: Principles of Computer Security

One of the following interdisciplinary courses:

ACIS 4684: Information Systems Security and Assurance

FIN 4014: Internet, Electronic, and Online Law

MATH 4175: Cryptography I

MATH 4176: Cryptography II

This is a minor to computer engineering degree, not computer science.

Here is a link to a horrible PDF that identifies what courses to take for that degree. I couldn’t find anything easier to read. <https://www.registrar.vt.edu/content/dam/registrar_vt_edu/documents/Updates/coe/2020/coe_cpe_20.pdf>

# Course Names