Centers of Academic Excellence – Cyber Operations

Knowledge Units

v2.0

Contributors:

Seth Hamman (Lead) – Cedarville University
Bobby Birrer – United States Air Force Academy
Rajendra Boppana – University of Texas San Antonio
Kyle Cronin – Dakota State University
Jason Denno – University of Arizona
Dennis Dias – United States Naval Academy
Mike Ham – Dakota State University
Drew Hamilton – Texas A&M University
Cynthia Irvine – Naval Postgraduate School
Sidd Kaza – Towson University
Bill Mahoney – University of Nebraska Omaha
Nicholas Parry – Cedarville University
Josh Pauli – University of Arizona
Golden Richard - Louisiana State University
Salamah Salamah – University of Texas El Paso
Patrick Tague – Carnegie Mellon University
Blair Taylor – Towson University
George Trawick – Mississippi State University

Knowledge Units Criterion Description

The Knowledge Units (KU) criterion is the heart of the Cyber Operations (CO) designation. More than any other designation criteria, it paints the target for providing a rigorous cyber operations education.

The CO Student Outcomes (SOs) outline the core attributes of cyber operators. The KUs are designed to produce graduates that meet the SOs. Mandatory KUs (MKUs) form the main knowledge and skills of cyber operators. All graduates of every CO program must cover all the MKUs. A set of Optional KUs (OKUs) are chosen by schools based on their specific areas of expertise within the field of cyber operations. This division of mandatory and optional KUs helps diversify the national collection of CAE-CO designated programs.

In order to operate effectively cyber operators must have a deeply technical understanding of the underlying architectures and protocols of cyberspace. Therefore, CO programs of study (PoS) must be based on a computer science or computer engineering core. The main material required in the program core is covered in M2: Computer Science Foundations. On top of the foundational academic program schools will need to offer several specialized courses in cyber in order to meet the KU requirements for academic validation.

Mandatory Knowledge Units

The MKUs are organized logically, starting with foundational knowledge and culminating with the specialized knowledge and skills needed by cyber operators. All programs must align core courses to all 10 MKUs. No elective courses should be aligned to MKUs because all graduates of the PoS must take every course that either partially or fully covers every MKU.

Optional Knowledge Units

OKUs represent specialized areas of study connected to cyber operations. In most cases a single course similarly named is required to fully cover an OKU.

All graduates of the PoS must take courses that fully cover at least 4 OKUs. Both core and elective classes can be aligned to OKUs. If every graduate from a PoS takes courses that fully cover more than 4 OKUs, still only 4 OKUs should be aligned – it is up to the applicant to select "the best" 4. Aligning more than the minimum OKUs causes extra work for both schools and program reviewers and there are no added benefits.

Only if there are multiple elective pathways through a PoS may a program align more than 4 OKUs. In this case, every pathway that leads to graduation must cover at least 4 OKUs. If alternate pathways cover non-overlapping OKUs, it will be necessary to align more than 4 OKUs, but still only the minimum set of OKUs should be aligned.

Aligning Courses to KUs

Every KU contains learning outcomes and topics. There are no fixed requirements for the number of core hours or semester weeks needed to cover a KU, but the KU learning outcomes help to define the appropriate depth of coverage. The KU Notes provide further guidance but do not define strict requirements. While it is not required that every learning outcome be

explicitly assessed as written, applicant schools should be able to defend their coverage of the learning outcomes. All KU topics must be addressed by the aligned courses. KU topics are deliberately broad so schools can apply their discretion and expertise. More specific guidance is available if requested.

A KU may be covered by one or more courses. When multiple courses are aligned to a KU, it is assumed that all of them partially cover the KU and that together they fully cover the KU. Programs should never align multiple courses to a KU purely to show strength of coverage. There is no such thing as 110% coverage; either a KU is fully covered or it is not. If there are multiple courses that fully cover a KU, then schools should align only the minimal set or the single course with the primary coverage. 4 or more courses aligned to a single KU may be more of an indication of poor KU coverage than strong because it risks diluting the KU.

Single courses can fully and partially cover more than 1 KU. There is no limit on the number of KUs that can be aligned to a single course, but 4 or more KUs against a single course may be an indication of weak KU coverage.

Hands-on Activities

Cyber operations is an applied academic discipline not a theoretical one. Students learn the knowledge and skills they need by doing. Therefore, the heavy use of hands-on labs and programming assignments is the best practice in cyber operations education. It is expected that students graduating from CO-designated programs will be adept at operating in virtualized sandboxed environments. Coverage of every KU (with the exception of M1: Cyber Policy, Law, and Ethics) must include hands-on activities. Examples of hands-on activities include configuring and deploying cyber tools, writing and executing programs and scripts, and conducting tasks in defensive and offensive cyber operations.

Prerequisites

The KUs are not intended to define a complete Bachelor of Science program of study and do not identify all prerequisites. For example, an introductory programming course is needed to support M5: Systems Programming, but it is not specified. Additionally, not all core computer science and computer engineering content is addressed by the KUs. For example, computer science programs typically require a course in programming language theory, but there are no KUs for this topic. On the other hand, core computer science topics such as algorithms and data structures are critical for cyber operators so they are addressed in M2: Computer Science Foundations.

Graduate programs

Both graduate and undergraduate programs use the same set of KUs, but graduate programs may be held to a more in-depth standard of coverage. Graduate programs may align KUs to prerequisite courses that are required for admittance into the program but that are not taught in the graduate PoS itself.

Special Note on Definitions

The NIST Computer Security Resource Center glossary provides helpful definitions and links to primary sources for many of the technical terms used in the KUs.

Cyber Operations Student Outcomes

Graduates of cyber operation programs will be able to:

1. Operate ethically at all times, respect the rights of all citizens, and obey all applicable laws and authorities.
2. Apply logical and algorithmic thinking to navigate and produce effects in cyberspace.
3. Detail the architecture and functions of operating systems and computer networks.
4. Develop systems software using assembly and low-level languages.
5. Describe the motivations, methods, and goals of cyber threat actors.
6. Protect the confidentiality and integrity of data at rest and in transit.
7. Perform static and dynamic analysis of software to identify vulnerabilities.
8. Reverse engineer software and network protocols.
9. Secure data, computer systems, and networks from cyber attacks.
10. Plan and execute offensive cyber operations in contested environments.

Knowledge Units List

Mandatory

M1: Cyber Policy, Law, and Ethics
M2: Computer Science Foundations
M3: Operating Systems
M4: Computer Networks
M5: Systems Programming
M6: Cybersecurity Foundations
M7: Applied Cryptography
M8: Software Reverse Engineering
M9: Defensive Cyber Operations
M10: Offensive Cyber Operations

Optional

O1: Programmable Logic
O2: Computer Architecture
O3: Microcontrollers
O4: Hardware Reverse Engineering
O5: Cyber Forensics
O6: Wireless and Mobile Security
O7: Virtualization
O8: Cloud Security
O9: Critical Infrastructure Security
O10: Cyber Risk Management
O11: Game Theory

Candidate Optional Knowledge Units

Memory Forensics
Machine Learning
Artificial Intelligence
Cryptanalysis
Human Factors in Information Security
Cyber Operations Policy and Doctrine

Mandatory Knowledge Units

M1: Cyber Policy, Law, and Ethics

To comply with the many US laws, regulations, directives, and policies, it is essential that cyber operators know the extent and limitations of their authorities. In addition, cyber operators must fully grasp their societal responsibility for protecting and respecting the rights of US citizens and for acting ethically at all times.

KU Learning Outcomes (supports SO1)

Students will be able to:

1. Identify the main US governmental organizations responsible for cybersecurity.
2. Identify the authorities applicable to various cyber operations scenarios.
3. Explain US cyber operations doctrine.
4. Describe how the rights guaranteed in the US Constitution apply in cyberspace.
5. Identify the major US cyberspace-related laws.
6. Describe how international law impacts US cyber operations.
7. Describe the societal responsibility of cyber operators to act legally and ethically at all times.
8. Perform reasoned ethical analyses of cyberspace-related ethical gray areas.

Topics

1. US governmental organization for cybersecurity and cyber operations
2. US governing authorities for conducting cyber operations
3. US cyber operations doctrine
4. US constitutional rights and their application to cyberspace
5. US cybersecurity legislation
6. International humanitarian law and cyber operations
7. Societal responsibility
8. Ethical frameworks
9. Ethical hacking-related codes of conduct

Notes

This KU may be covered by a course devoted to cyber law and ethics or by a module in an introductory cyber course or capstone cyber course or both. In addition, it is assumed that the legality and ethics of cyber operation activities will be reinforced across the curriculum as they apply in various contexts. Ideally, schools will have students sign a statement of ethical conduct.

M2: Computer Science Foundations

A deeply technical understanding of the infrastructure and functioning of cyberspace is essential for cyber operators. They must understand the basic building blocks of cyberspace including digital logic, data encoding, and data structures. Additionally, they must be skilled in logical and algorithmic thinking.

KU Learning Outcomes (supports SO2)

Students will be able to:

1. Design logic circuits that perform basic computational tasks.
2. Encode and decode data to and from binary format.
3. Define fundamental data structures and their appropriate uses.
4. Apply the principles of abstraction and modularity in the design of software.
5. Characterize the complexity of algorithms.
6. Identify when heuristics are needed for finding practical solutions to algorithmic problems.

Topics

1. Discrete math
2. Digital logic
3. Data encoding
4. Data structures
5. Abstraction
6. Modularity
7. Algorithmic analysis
8. Computational tractability

Notes

In undergraduate programs this KU will likely be covered by multiple program core courses such as digital logic design, discrete math, data structures, and algorithms. For graduate programs, this KU may be covered by prerequisite admission requirements. This KU includes prerequisite material for M3 through M10.

M3: Operating Systems

Malware subverts operating systems to undermine system security and evade detection. As the software foundation of computer systems, it is vital that cyber operators understand operating system structures and functions. Operating systems implement access control, process isolation, logging, and many other fundamental cybersecurity properties. They are also a major source of critical cybersecurity vulnerabilities, including software bugs and configuration mistakes.

KU Learning Outcomes (supports SO3)

Students will be able to:

1. Detail the main components of an operating system and their functions.
2. Describe how operating systems manage privileged and non-privileged access.
3. Describe how operating systems implement security.

Topics

1. User space and kernel space
2. Processes and threads
3. Memory management
4. CPU scheduling, including multiprocessor architectures
5. Storage management, including I/O systems
6. File systems and permissions
7. Virtual machines
8. Operating system security

Notes

This KU is best covered by an operating systems concepts course. This KU includes prerequisite material for M8 through M10.

M4: Computer Networks

Computer networks are the infrastructure of cyberspace and the primary domain where cyber operations are conducted. An in-depth understanding of computer networking protocols and the ability to write networked applications is essential for conducting cyber operations.

KU Learning Outcomes (supports SO3)

Students will be able to:

1. Detail the layered architecture of the Internet.
2. Describe the function and operation of the main Internet protocols.
3. Explain how security is implemented at each Internet layer.
4. Capture and analyze network packets.
5. Write computer network applications that employ standard and custom protocols.
6. Describe the operation of wireless and mobile networks.

Topics

1. Internet layers and protocols
2. Network security at each layer
3. Network utilities
4. Packet sniffing
5. Socket programming
6. Wireless network basics
7. Mobile network basics

Notes

This KU may be covered by multiple computer networks courses or by an advanced computer networks course that includes a module in wireless and mobile networking. This KU includes prerequisite material for M8 through M10.

M5: Systems Programming

Systems programming uses low-level programming languages such as C and assembly language to interface with the operating system and computer hardware. Systems programmers must be familiar with system calls, memory management, and registers. Systems programming is a foundational skill for software reverse engineering, vulnerability discovery, and exploit development.

KU Learning Outcomes (supports SO4)

Students will be able to:

1. Write systems programs in C that leverage assembly language and operating system calls.

Topics

1. C programming
2. Assembly language programming
3. Operating system calls
4. Kernel modules
5. Device drivers

Notes

This KU is best covered by an advanced programming course. This KU includes prerequisite material for M8 and M10.

M6: Cybersecurity Foundations

Cyber operators must be able to describe the current cybersecurity threat landscape, including the various motivations, objectives, and methods of cyber threat actors. This knowledge reinforces adversarial thinking and the need for cybersecurity. Cyber operators must also be able to describe the goals of cybersecurity, how risk management informs the approach to cybersecurity, and the principles and best practices of cybersecurity.

KU Learning Outcomes (supports SO5)

Students will be able to:

1. Discuss current events in cybersecurity.
2. Describe different categories of threat actors and their motivations.
3. Describe different objectives of cyber attackers.
4. Describe different types of cyber attacks.
5. Describe different types of malware.
6. Describe different types of common cyber vulnerabilities.
7. Research known vulnerabilities and rate their severity.
8. Describe the goals of cybersecurity.
9. Describe how cyber risk management leads to the efficient allocation of resources.
10. Define the fundamental principles of cybersecurity.
11. Describe the components of access control and how they are implemented.

Topics

1. Current events in cybersecurity
2. Adversarial thinking
3. Cyber threat actors
4. Cyber attack methods including social engineering
5. Types of malware
6. Cyber vulnerabilities
7. Vulnerability taxonomies, databases, and scores
8. CIA Triad
9. Cyber risk management
10. Cybersecurity principles
11. Cybersecurity best practices
12. Access control (AAA)

Notes

In undergraduate programs this KU will likely be covered by an introductory cybersecurity course. Examples of hands-on activities include guided labs where students conduct point-and-click attacks and complete basic cybersecurity tasks. For graduate programs, this KU may be covered in the introductory portion of a more advanced cyber course. This KU includes prerequisite material for M8, M9 and M10.

M7: Applied Cryptography

Cyber operators must be able to apply cryptography to protect the confidentiality and integrity of information. They must also understand the risks and limitations of cryptography.

KU Learning Outcomes (supports SO6)

Students will be able to:

1. Explain the process and methods of encrypting and decrypting data.
2. Use symmetric key and public key algorithms to encrypt and decrypt data.
3. Explain the benefits and weaknesses of the public key infrastructure.
4. Describe the properties and uses of hash functions.
5. Use hash functions to protect and verify the integrity of data.
6. Write software that performs cryptographic operations using standard libraries.
7. Describe methods for attacking cryptography.
8. Describe the risks and limitations of cryptography.

Topics

1. Mathematical foundations for cryptography
2. Symmetric key cryptography
3. Stream ciphers
4. Block ciphers and modes
5. The key distribution problem
6. Public key cryptography
7. The key binding problem
8. Public key infrastructure (PKI)
9. Digital signatures
10. Hash functions
11. Key stretching
12. Kerckhoff's principle
13. Attacks on cryptography
14. Quantum computing risks to cryptography

Notes

This KU is best covered by a single course devoted to cryptography but also could be covered as a significant portion of a cyber defense course. It is assumed that cryptography will also be covered throughout the curriculum as it applies in various contexts. This KU includes prerequisite material for M9 and M10.

M8: Software Reverse Engineering

The ability to understand 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.

KU Learning Outcomes (supports SO7 and SO8)

Students will be able to:

1. Safely reverse engineer and document software of unknown origin and malware.
2. Safely and directly patch software to modify its functionality.
3. Recognize common C programming constructs in assembly language.
4. Reverse engineer network traffic to document custom communication protocols.
5. Identify vulnerabilities in software using fuzzing and static and dynamic analysis.

Topics

1. Reverse engineering techniques
2. Reverse engineering tools
3. Reverse engineering for software specification recovery
4. Reverse engineering for malware analysis
5. Patching software
6. Deobfuscation of obfuscated code
7. Protocol reverse engineering
8. Software analysis

Notes

This KU is best covered by a single course in software reverse engineering. This KU includes prerequisite material for M9 and M10.

M9: Defensive Cyber Operations

Cyber operations encompass both offensive and defensive operations. Defensive operations are needed to protect computer systems and networks from attack. Also, it is essential that cyber operators understand how defense compliments offense.

KU Learning Outcomes (supports SO9)

Students will be able to:

1. Apply adversarial thinking to anticipate the strategic actions of adversaries
2. Identify common programming errors that lead to vulnerabilities.
3. Develop secure software following best practices.
4. Create and implement firewall rules given high-level objectives.
5. Perform system administration tasks on the command-line and using scripts in Windows and Unix-based environments.
6. Scan networks and computer systems to discover vulnerabilities.
7. Secure computer systems and data from tampering and unauthorized access.
8. Patch vulnerabilities in operating systems and software.
9. Detect and remove malware from computer systems.
10. Detect malicious activity in computer systems and networks.

Topics

1. Software security vulnerabilities
2. Secure software development practices
3. Software security testing
4. Firewalls
5. Operating system hardening
6. Scripting
7. Vulnerability scanners
8. Patching
9. Malware detection
10. Indicators of compromise (IOCs)
11. Log analysis
12. Process and file activity monitors
13. Network activity monitors

Notes

This KU is best covered by an advanced cyber defense course where students complete labs in virtualized sandbox environments. This KU complements M10.

M10: Offensive Cyber Operations

Offensive cyber operations are carefully planned military and intelligence operations that are executed in and through cyberspace to achieve actions on objectives. Real life cyber operations are restricted to those explicitly authorized by various US government authorities.

KU Learning Outcomes (supports S10)

Students will be able to:

1. Perform open-source intelligence on organizations and individuals.
2. Conduct enumeration and scanning of target networks.
3. Conduct various types of cyber attacks using tools, custom software, and scripts.
4. Identify vulnerabilities in target organizations, systems, and networks.
5. Write malware to exploit vulnerabilities.
6. Gain unauthorized access to computer systems.
7. Define and achieve actions on objectives in target systems.
8. Employ techniques for evading detection including covert communications.

Topics

1. Mission planning and execution
2. Cyber attack frameworks
3. Open-source intelligence (OSINT)
4. Cyber attack tools
5. Privilege escalation
6. Shellcode
7. Packet crafting
8. Command and control (C2)
9. Data exfiltration
10. Actions on objectives
11. Techniques for evading detection
12. Covert communication and steganography

Notes

This KU is best covered by a capstone cyber operations course where students complete attack labs in virtualized sandbox environments. Ideally, students would also engage one another in cyber exercises to gain experience operating in contested environments. This KU complements M9.

Optional Knowledge Units

O1: Programmable Logic

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.

KU Learning Outcomes

Students will be able to:

1. Specify digital device behavior using programmable logic language.
2. Design, synthesize, simulate, and implement logic on an actual programmable logic device.

Topics

1. Hardware design and programming languages
2. Programmable logic devices

O2: Computer Architecture

Computer architecture provides an organized computing framework to allow firmware and software to leverage computing capabilities and various system resources.

KU Learning Outcomes

Students will be able to:

1. Describe how various computing components and system resources are interconnected within a processor.
2. Assess the functionality and performance impact of processor design alternatives.

Topics

1. Organization of computer and processor architectures
2. Instruction set design alternatives
3. Processor implementation
4. Memory system hierarchy
5. Buses
6. I/O systems
7. Factors affecting performance

O3: Microcontrollers

Microcontrollers represent a special class of computing systems that are typically small and simple computers with a processor core, limited memory, programmable input/output peripherals, and sensors. Microcontrollers are typically inexpensive, have little or no interface for human interaction, and have a fixed (often special-purpose) function with little to no change over their lifecycle.

KU Learning Outcomes

Students will be able to:

1. Design and build a basic microcontroller application.
2. Assess the limitations of a given microcontroller design.

Topics

1. Instruction sets and architectures
2. Microcontroller programming environments
3. Special considerations for architecture limitations and real-time requirements
4. Integrating microcontrollers into larger systems
5. Security considerations

O4: Hardware Reverse Engineering

Hardware reverse engineering is the study of hardware hacking and dissecting electronic devices and embedded systems. Hardware reverse engineers probe hardware components to determine their functionality, inputs, outputs, and stored data.

KU Learning Outcomes

Students will be able to:

1. Safely document hardware functionality using procedures such as probing, measuring, and data collection.
2. Safely and directly modify hardware functionality.
3. Describe common hardware attack vectors.

Topics

1. Hardware reverse engineering methodology
2. The use of tools and test measurement equipment
3. Circuit board analysis and modification
4. Embedded security
5. Common hardware attack vectors

O5: Cyber Forensics

Cyber forensics focuses on the recovery and investigation of artifacts in networks, memory, and operating systems.

KU Learning Outcomes

Students will be able to:

1. Determine the manner in which an operating system or application has been subverted.
2. Recover deleted and intentionally hidden information from various types of media.
3. Demonstrate proficiency with handling a large number of different kinds of devices.
4. Identify forensic artifacts left by cyber attackers.
5. Acquire a forensically sound image for investigation.

Topics

1. Operating system forensics
2. Device / media forensics
3. Network forensics
4. Memory forensics

Notes

This KU focuses specifically on cyber forensic processes and technology (i.e., tools and techniques), not legal aspects (e.g., chain of custody, preparation of evidence for legal proceedings).

O6: Wireless and Mobile Security

Wireless and mobile systems have become ubiquitous, and they can have significant impacts on system security and operation, especially due to the relative openness and 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.

KU Learning Outcomes

Students will be able to:

1. Describe unique security and operational attributes in the wireless environment and their effects on network communication guarantees and protections.
2. Demonstrate knowledge of common vulnerabilities and use of available tools.
3. Describe effective (and ineffective) mechanisms for protecting commonly deployed wireless and mobile networks and corresponding protocols that are employed in these systems, including wireless link and infrastructure components.

Topics

1. Stream and block ciphers and security protocols commonly used in wireless networks, what properties each one provides, and known limitations / vulnerabilities
2. Security implementations in different wireless systems (e.g., GSM, LTE, WiFi, Bluetooth, RFID)
3. Mobile identifiers and registration, device / user tracking, and protection of identifiers for anti-tracking
4. Availability issues in wireless networks

O7: Virtualization

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.

KU Learning Outcomes

Students will be able to:

1. Describe the technical mechanisms by which virtualization is implemented in a variety of environments, and their implications for cyber operations.
2. Enumerate and describe the various interfaces between the hypervisors, VMs, physical and virtual hardware, management tools, networking, storage, and external environments.

Topics

1. Type I and Type II architectures
2. Virtualization Principles including efficiency, resource control and equivalence
3. Virtualization techniques for code execution, including trap and emulate, binary translation, paravirtualization, and hardware-supported virtualization (e.g., Intel VMX).
4. 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
5. Techniques for allocating storage (e.g., hard drives) to Virtual Machines, and the associated capabilities (e.g., snapshots)
6. Techniques for associating hardware (virtual or physical) with virtual machines, including hardware-supported methods (e.g., SR-IOV) and device emulation
7. Techniques for providing advanced virtualization capabilities, such as live-migration and live failover
8. Internal and External Interfaces provided by virtualized platforms for management, monitoring, and internal communication/synchronization
9. Snapshots, migration, failover

Notes

Education focused on simply using VMs or virtualization platforms such as vSphere, HyperV, or VirtualBox is not sufficient to address this KU.

O8: Cloud Security

Cloud resources are commonly used for a wide variety of use cases, including the provisioning of enterprise services, data processing and analysis, development and testing, and a wide variety of consumer-focused services. 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 were previously too difficult.

KU Learning Outcomes

Students will be able to:

1. Describe cloud service models and deployment modes and their suitability for various service tasks, including understanding security tradeoffs.
2. Develop and deploy a task in an appropriate cloud environment, including addressing issues associated with deployment, configuration, management, scalability, and security.

Topics

1. Essential characteristics of cloud platforms and the underlying technologies that enable them
2. Common service, deployment, and management models and their associated tradeoffs
3. Cloud infrastructure components and the interfaces they expose to internal and external processes
4. Security implications of cloud computing, including issues associated with shared resources and multi-tenancy, extension of trust to include the cloud provider, and approaches to mitigating these issues
5. Developing, deploying, and managing applications on deployed cloud infrastructure

O9: Critical Infrastructure Security

Industrial Control Systems (ICSs) and Supervisory Control and Data Acquisition (SCADA) systems are at the core of many critical infrastructure sectors in the United States. These systems use common components and are frequently interconnected; vulnerabilities can cause significant problems to their owner operators. Many ICSs have critical national security impacts, such as the electrical power grid as well as dams and water treatment facilities. Cyber operators should have knowledge of the attack and defense of ICSs.

KU Learning Outcomes

Students will be able to:

1. Describe the components of ICS systems and how they are programmed.
2. Describe the different network protocols used in the operation of ICS and SCADA systems and their security vulnerabilities.
3. Use industry standard software such as the DHS CSET tool to aid in analysis of ICS systems at a compliance level

Topics

1. Programmable logic controllers (PLCs)
2. Supervisory Control and Data Acquisition (SCADA) systems
3. Distributed Control System (DCS)
4. ICS communication protocols
5. US Critical Infrastructure sectors and regulations by sector

O10: Cyber Risk Management

Risk management forms the basis for applying information system security principles to an operational environment, including an organization's security culture and values.

KU Learning Outcomes

Students will be able to:

1. Describe the methods used to identify, measure, and mitigate key information technology risks.
2. Describe tasks associated with risk framing, assessment, response, and monitoring.

Topics

1. Risk models (e.g., NIST SP 800-39)
2. Risk processes (e.g., NIST SP 800-37)

O11: Game Theory

Cybersecurity is predicated on the existence of human adversaries. Therefore, adversarial thinking underlies both defensive and offensive cyber operations. Game theory is the study of strategic reasoning and is useful for anticipating the strategic actions of adversaries.

KU Learning Outcomes

Students will be able to:

1. Define canonical game theoretical games.
2. Describe the differences between traditional and behavioral game theory.
3. Determine scenarios where behavioral game theory renders more accurate predictions than traditional game theory.
4. Define the necessary conditions for a game theoretical scenario.
5. Draw a normal form representation of a real-life strategic scenario.
6. Identify the Nash equilibrium for basic normal form games.
7. Apply best response analysis to solve game theoretical games.
8. Define level-k strategies for games.

Topics

1. Canonical game theoretical games
2. Types of games
3. Traditional game theory
4. Behavioral game theory
5. Utility preferences
6. Normal form games
7. Nash equilibrium
8. Level-k reasoning

Candidate Optional Knowledge Units

Memory Forensics

Machine Learning

Artificial Intelligence

Cryptanalysis

Human Factors in Information Security

Cyber Operations Policy and Doctrine