Center of Academic Excellence – Cyber Operations Fundamental Program

2020 Application

Name of Institution:
United States Naval Academy

Date:
January 13, 2020

Mailing Address of Institution:
121 Blake Road
Annapolis, MD 21402

Institution's President's Name and Official Email Address:
Superintendent VADM Sean Buck,
sbuck@usna.edu

Department Submitting Application (e.g., Computer Science (CS), Electrical Computing Engineering (ECE), etc.):
Cyber Science (SCY)

Is this a new or renewal application? New

Institution's Points of Contact (POC)

***Primary* POC Name:**
Dennis P. Dias, ONR Chair, Cyber Science

Office Phone #:
(443) 418-8220

Office Email Address:
dias@usna.edu

***Alternate* POC Name:**
CAPT James Caroland, Department Chair, Cyber Science

Office Phone #:
(443) 854-5949

Office Email Address:
caroland@usna.edu

Criterion 1: Academic Content

a. **Identify the degree program(s) in which the cyber operations curriculum is based.**
NOTE: CAE-Cyber Operations programs must be based within a computer science, electrical engineering or computer engineering department, or a degree program of equivalent technical depth, or a collaboration between two or more of these departments.

Bachelor of Science in Cyber Operations

b. **Identify the program path seeking designation, including the title of the degree/specialization/track.**

NOTE: This name represents the proposed designated CAE-CO program path, will appear on the NSA.gov web page, and will be the name on the issued CAE-CO designation certificate. (e.g. Bachelor's of Science in Computer Engineering, Cyber Operations Specialization)

US Naval Academy Bachelor of Science in Cyber Operations (NSA CAE-CO approved)

c. **Using the Knowledge Unit Alignment worksheet, identify the courses that cover all 10 of the Mandatory KUs and at least 10 of the Optional Knowledge Unit requirements. List the instructors that teach the course on the worksheet.**
NOTE: This portion is completed by filling out the Knowledge Unit Alignment Worksheet. Any additional comments referencing the worksheet may be placed here.)

NOTE: For school's that had a Phase 2 on-site the previous year, explicitly identify if no/any changes have occurred for all mapped courses, including content and instructors, since the site visit.

NOTE: A single course should not be used in the curriculum mapping to satisfy too many KUs. It is unlikely the course provides the required breadth or depth of coverage to satisfy many KUs.

NOTE: Knowledge unit topics should not be spread among a large number of courses, but generally should be covered in a focused approach (e.g., a single or few courses). Spreading the material across too many courses may not present the KU in a focused enough manner for the student to thoroughly understand it.

Please see the attached document and related links to the USNA Cyber CAE-CO Project in GitHub which can be found on our public webpage at https://www.usna.edu/CyberDept/index.php

d. Identify below, or provide in a separate document, sample courses schedules, course descriptions and syllabi that contain a weekly schedule of topics. Include an example plan of study that clearly demonstrates that a student can successfully complete the requirements of a cyber operations curriculum within the degree program. If a Knowledge Unit requires hands-on labs or exercises, labs/exercises are to be included with the support documentation in a non-executable format.
NOTE: Support documentation submitted as separate files must be searchable. Support documentation should not be submitted solely as a hyperlink since links can break and there is no guarantee that reviewers will have access to the Internet.)

Please see the attached document and related links to the USNA Cyber CAE-CO Project in GitHub which can be found on our public webpage at https://www.usna.edu/CyberDept/index.php

Criterion 2: Cyber Operations Recognized via Certificate or Focus Area

Describe how students who participate in the Cyber Operations curricula will be distinguished from other (non-Cyber Operations) students:

Students who participate in the Cyber Operations curricula will have the following placed on their transcripts once they graduate:
"Completed all coursework required for CAE-CO designation".

Criterion 3: Program Accreditation

Nationally accredited? **Yes**	**Regionally accredited?** **Yes**
Name of National Accreditation Body: ABET (Accreditation Board for Engineering and Technology)	**Name of Regional Accreditation Body:** MSCHE (Middle States Commission for Higher Education)
Date of National Accreditation: 01 OCT 2015	**Date of Regional Accreditation:** Academic Year 2016 (renewable in 2025)

Criterion 4: Cyber Operations Treated as an Inter-Disciplinary Science

Describe how Cyber Operations is treated as an inter-disciplinary science at your institution:

Cyber Operations is an interdisciplinary major that covers the entire scope of cyberspace and related operations, both technical and non-technical. As such, the Cyber Operations major provides a basic foundation in computer architecture, programming, data structures, networks, internet, database systems, information assurance, cryptography, and forensics. The technical aspects of the program are balanced with additional courses and electives emphasizing applications in areas such as policy, law, ethics, and human factors/social engineering.

Criterion 5: Cyber Operations Academic Program is Robust and Active

a. Provide a brief description of your documented policy on updating course materials to remain relevant.

To support the continuous improvement of student learning and development, USNA assesses its academic programs across all divisions and departments (related policy provided in GitHub repository under Assessment). The Cyber Science Department maintains an Assessments Committee that continually assesses both our core and majors courses and our program as a whole, including updating course material to remain relevant. Cyber Operations Faculty are constantly updating course material to reflect the dynamic nature of the evolving technology in this area. Labs, case studies, lesson plans, and themes are all reviewed and updated over every semester to remain relevant and current while appreciating the historic context of the changes. In some courses (like SY401) the open source tools such as Kali Linux (which update quarterly) change several times in a semester. New Electives and core courses (such as the Honors Curriculum) are added each year as our faculty grows in size and experience. Courses in Reverse Engineering leveraging GHIDRA and other open source tools have become popular electives. We have updated our mobile communications course to best align with NSA-CAE guidelines. Our Cyber Security Team (winner of NCX in 2018) and related extra-curricular activities such as the Women in Cyber Club and Information Warfare Club provide additional professional development opportunities for Midshipman to remain current in the field. Each week dozens of Midshipmen participate in STEM support activities (which often include introductory cyber topics) in the local community and lead cyber activities in summer camps for middle and high school students at the Naval Academy Summer Seminar. The Naval Academy Cyber Lecture Series attracts world known leaders from government, industry, and the military in the cyber operations field to speak at USNA every semester. Our students and faculty can be found presenting at conferences worldwide on a myriad of topics and research areas. Faculty members are required to maintain and update course material to keep pace with the evolving field of cyber science. This is documented in annual employee performance plans. Our faculty also leverage the Naval Academy’s Instructional Development Support Center (IDSC) which is a centralized, client-oriented support facility that introduces emerging instructional technologies and helps faculty integrate appropriate technology into the teaching, learning, and assessment processes. The IDSC offers short courses in educational software programs, such as the use of Blackboard, and assists the faculty in developing course materials and the Naval Academy Foundation assists with funding where possible to support new equipment, conferences, industry relationships, and other key elements to help our program evolve.

b. **Include with this application a copy of the documented policy on updating course materials to remain relevant.**

c. **On the accompanying Knowledge Unit Alignment worksheet indicate the last time the course was taught and the last time the course was reviewed using the above policy.**

Criterion 6: Faculty Involvement in Cyber Operations-related Research

Provide a list of research topics believed to be related to the Cyber Operations Program in which faculty are currently involved.
NOTE: Evidence submitted for this application can be 1) a list of the faculty grants to include who is the grant's sponsor, the period of performance, what is the grant purpose, and the grant's funding, 2) papers published to include names, dates and an abstract, and/or 3) conference presentations including presenter names, dates and an abstract. All evidence should be related to the field of Cyber Operations (i.e., with a particular emphasis on technologies and techniques related to specialized cyber operations such as collection, exploitation, and response. These technologies and techniques are critical to intelligence, military and law enforcement organizations authorized to perform these specialized operations).

Please see the attached documention and related links to the USNA Cyber CAE-CO Project (under faculty) in GitHub which can be found on our public webpage at https://www.usna.edu/CyberDept/index.php

Criterion 7: Student Involvement in Cyber Operations Research

Provide research topics believed to be related to the Cyber Operations Program in which students are currently engaged:
NOTE: Evidence submitted for this Criterion can include 1) student participation in research grant activities (cite exactly what the student(s) did on the project), 2) student research papers are required as part of cyber operations related courses, 3) student publications related to cyber operations topics, and 4) student attendance and presentations of cyber operations related topics at conferences (must identify conference title, dates and the presentation title if the student was a briefer. All evidence should be related to the field of Cyber Operations (i.e., with a

particular emphasis on technologies and techniques related to specialized cyber operations such as collection, exploitation, and response. These technologies and techniques are critical to intelligence, military and law enforcement organizations authorized to perform these specialized operations)

Please see the attached document and related links to the USNA Cyber CAE-CO Project (under student) in GitHub which can be found on our public webpage at https://www.usna.edu/CyberDept/index.php. This includes our graduation requirement for capstone projects that all Cyber Operations midshipmen complete.

Criterion 8: Student Participation in Cyber Service-Learning Activities

Describe Cyber Security or Cyber Operations related outreach efforts in which students are currently involved (e.g., Cyber exercises, volunteers at local K-12 schools, supporting cyber camps, cyber support to local law enforcement, conference presentations, etc.):

Midshipmen are very active in a variety of activities including all of the above as well as industry and international experiences. The Cyber Science Department recently held the first ever “Hour of Code” activity in coordination with the USNA STEM Center in December 2019. The STEM Center leverages Cyber Operations students and faculty to support over 600 middle and high school students each summer at the USNA Summer Seminar. Students and faculty are regularly contacted by the STEM Center and area schools to help present, teach, and mentor students on Cyber topics. In September 2019 a USNA Midshipman from the Cyber Security Team discovered a real world cyber vulnerability in a 3D printer at the Hack The Machine Cyber Security Hackathon in Brooklyn, New York and received press coverage. Please see the attached document and related links to the USNA Cyber CAE-CO Project (under Student) in GitHub which can be found on our public webpage at https://www.usna.edu/CyberDept/index.php. This documentation provides additional details on the many related outreach efforts in which our students are currently involved.

Criterion 9: Commitment to Support the CAE-Cyber Operations Program

a. **Initial applicants must make a stated commitment to support the CAE-Cyber Operations program which is demonstrated with the official signature applied to this application. Examples of support could be in the form of student applicants to the CAE-Cyber Operations Summer Internship Program, comprehensive faculty participation in**

Knowledge Unit review and changes, mentorship of another institution applying for the CAE-Cyber Operations designation, and/or faculty support in the form of briefing or teaching during the CAE-Cyber Operations Summer Intern Program.

b. **For renewal applications to the CAE-Cyber Operations Program, describe below how your institution has supported the CAE-Cyber Operations Program which also must include support with, at a minimum, eight students and three faculty members, over the course of the five-year designation window.**

The USNA is fully on board with supporting the CAE-CO Program and considers the program a hallmark of this new major. Specifically, the USNA has taken part and wants to continue to participate in the CAE-Cyber Operations Summer Internship Program (one of the largest contributors of interns) as well continuous evaluation of our program and course content. A majority of Cyber Operations faculty have been involved in Knowledge Unit Review, and the Naval Academy is fully vested in supporting other universities applying for CAE-CO designation by placing our program material in GitHub https://www.usna.edu/CyberDept/index.php which can provide ready access for other institutions. We have coordinated with several universities and colleges – especially institutions that are near military facilities nationwide. Each summer USNA Cyber Faculty help train Navy ROTC instructors using our curriculum. Last Summer a faculty member went TDY to Naval Station Great Lakes to brief all 1,000 new Navy ROTC Midshipman on cyber strategy and best practices for college students. We have also shared course information with the Naval Postgraduate School.

Criterion 10: Number of Faculty Involved in Cyber Operations Education and Research Activities

a. **Identify the names and number of faculty who teach active Cyber Operations related program courses. At least 2 full- time equivalents must be listed. Any instructors identified on the Knowledge worksheet must be listed here.**
NOTE: For the purposes of meeting this criterion, full time is considered to be teaching 3 courses associated with the required KUs per semester. Faculty with significant active research clearly and directly associated with cyber operations, or who are advising multiple students at the Master's or Doctoral level on clearly cyber operations research topics, may request that credit for such be allowed for one or two of the required courses.

Please see the attached documention and related links to the USNA Cyber CAE-CO Project (under Faculty) in GitHub which can be found on our public webpage at https://www.usna.edu/CyberDept/index.php

b. For each of the above listed faculty, include with this Application a curriculum vitae or biography.

Continuation and Additional Comments:

Our application package reflects our qualifications to be designated a National Center of Excellence in Cyber Operations. Review of these documents will make it clear to the reviewing board that our Bachelor of Science in Cyber Operations reflects the breadth, demanding coursework and rigor to prepare our students to be successful in the cyber operations field. The cyber domain touches every one of our graduates wherever they serve. Our program is supported by World Class Faculty with experience found in few other institutions and success is demonstrated by our students in the program, the success of our Cyber Security Team, and the substantial research by faculty and students. Each year we also send highly qualified students to graduate education programs at prestigious institutions around the globe. Our unique location near the center of gravity for cyber operations (NSA/USCC) makes our program the beneficiary of new talent and opportunities for our program as we seek to educate and train the future leaders that will serve and protect our nation.

Our Institution understands and believes that our program meets the criteria defined for the CAE-Cyber Operations program and has active courses that cover all 10 of the mandatory knowledge units and at least 10 of the optional knowledge units to meet the academic content requirements. Our Institution agrees, as part of the application process, that its program will participate in an in-person curricula review of courses satisfying the mandatory and optional knowledge units as part of the application review and selection process. If designated as a CAE-Cyber Operations program our Institution agrees to support the CAE-Cyber Operations program *(See Criteria 9)* and to submit annual reports that describe current program activities and program changes.

	17 JANUARY 2020
Signature	**Date**
CAPT James Caroland, US NAVY	**Department Chair, Cyber Science**
Type/Print Name	**Position**

MANDATORY KNOWLEDGE UNITS **Note:** To qualify for designation as a CAE in Cyber Operations, the institution/program must demonstrate that their curriculum satisfactorily **covers all 10** Mandatory KUs to the desired breadth and depth. For students to qualify for recognition of completing the Cyber Operations program they must take all courses the institution maps to the 10 Mandatory KUs. **Note:** A course description and syllabus containing a weekly schedule of topics must be included in the application package for all courses identified in this KU Alignment Worksheet. **Note:** The Outcomes listed in each KU description are examples of the level of depth cyber operations students must demonstrate to meet the requirement.	**Course # and Course Title**	**Instructor(s)**	**Date Last Taught**	**Date Last Reviewed**
M.1 Low Level Programming Languages	**Course # and Course Title**	**Instructor(s)**	**Date Last Taught**	**Date Last Reviewed**
Must include programming assignments. 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	**SY204 (Systems Programming and OS Fundamentals)** **Topic: C Programming. See a complete list of related course documents including labs in the GitHub repo at** https://github.com/USNA-CyberScience/CAE-CO-Application **SY303 (Applied Cyber Systems Architecture)** **Topic: Assembly Language Programming (for x86, ARM, MIPS or PowerPC).** **See course documents at** https://www.usna.edu/CyberDept/index.php	**SY204: LCDR Chris Hoffmeister** **SY303: Dr Dane Brown**	SY204: Spring CY2020 SY303: Fall	SY204: Spring CY2020 SY303: Fall CY2019

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** • **Assembly Language (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. ***Outcome***: Students will be able to write complex programs such as ones that implement a simple network stack. ***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.			CY2019	
M.2 Software Reverse Engineering	**Course # and Course Title**	**Instructor(s)**	**Date Last Taught**	**Date Last Reviewed**
Must include examples of 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	**SY485J (SY416) Reverse Engineering: course materials referenced can be found at the NSA CAE link the left side of the page at:** https://www.usna.edu/CyberDept/index.php	**SY485J: Mr Mark Debels, NSA Visiting Professor**	SY485J: Fall CY2019	SY485J: Fall CY2019

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 software 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 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.	Reverse engineering techniques	• Link to SY485J syllabus • Lab 4, 5, 7, and 8 are the examples provided. • Static and dynamic analysis techniques and tools are the backbone for this course.			
	Reverse engineering for software specification recovery	• This is the entire intent of the course. All Labs require students to do this. Labs 4 & 5 are the examples provided.			
	Reverse engineering for malware analysis	• The last 4 weeks of the course are primarily devoted to malware reverse engineering and the specific characteristics seen in malware software. • Labs 9 & 10 require students to perform malware analysis.			
	Reverse engineering communications (to uncover communications protocols)	• Part of the discussion in reversing malware is detecting whether the malware is communicating with another entity and how this is done. Demos are performed in class of how to detect malware using Wireshark. There is also a lesson on specific secure communication protocols to include IKE for IPsec and TLS. Lab 10 requires the students to use Wireshark to detect malware exfiltrating data. • See following document in course folder: Secure_Communication_Protocols.pdf			
	Deobfuscation of obfuscated code	• Deobfuscating obfuscated code is discussed in detail in Lesson 15 - see following document in course folder: Anti_Reversing_Techniques.pdf			

	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)	- Students get first hand experience with GDB, Objdump, and Ghidra as well as learn about IdaPro - Students perform reversing inside of a VM - Labs 4, 5, 7, 8, 9, and 10 all use reverse engineering tools - Lab 10 - students use Wireshark to view traffic as it travels across a network.			
M.3 Operating System Theory	**Course # and Course Title**		**Instructor(s)**	**Date Last Taught**	**Date Last Reviewed**

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

<b><i>Outcome</i></b>: Students will have a thorough understanding of operating systems theory and implementation. They will be able to understand</td>
<td><b>IC411: Operating Systems</b>
<b>SY204: Systems Programming and Operating Systems</b>
<table>
<tr><th><u>Topic</u></th><th><u>Assessment</u></th></tr>
<tr><td>Privileged vs. non-privileged states; and transitions between them (domain switching)</td><td>Fully covered in IC411
SY204: supports (system calls)</td></tr>
<tr><td>Concurrency and synchronization (e.g., semaphores and locks)</td><td>Fully covered in IC411</td></tr>
<tr><td>Processes and threads, process/thread management, synchronization, inter-process communications</td><td>Fully covered in IC411
IPC: SY204, current (file I/O, desc I/O, signals, pipes, sockets)</td></tr>
<tr><td>Memory management, virtual memory, hierarchical memory schemes</td><td>Fully covered in IC411</td></tr>
<tr><td>Uni-processor and multi-processor interface and support</td><td>Fully covered in IC411</td></tr>
<tr><td>CPU Scheduling</td><td>Fully covered in IC411</td></tr>
<tr><td>File Systems</td><td>Fully covered in IC411
SY204: supports (file I/O, stat, Hiding from ls)</td></tr>
<tr><td>IO issues (e.g., buffering, queuing, sharing, management)</td><td>Fully covered in IC411</td></tr>
<tr><td>Distributed OS issues (client/server, message passing, remote procedure calls, clustering)</td><td>Not fully covered in IC411 prior to 2019, but we added a lecture (pulled from our Distributed Systems course –SI486E) and an in-class exercise to address these specific topics.</td></tr>
</table>
</td>
<td><b>IC411: Professor Rick Schlichting, RADM Frank Leighton USNA 1909/Class of 1948 Distinguished Visiting Professor of Information Technology</b>

<b>SY204: LCDR Chris Hoffmeister</b></td>
<td>IC411: Fall CY2019

SY204: Spring CY2020</td>
<td>IC411: Fall CY2019

SY204: Spring CY2020</td>
</tr>
</table>

<table>
<tr><td>operating system internals to the level that they could design and implement simple architectural changes to an existing OS.</td><td></td><td></td><td></td><td></td></tr>
<tr><th>M.4 Networking</th><th>Course # and Course Title</th><th>Instructor(s)</th><th>Date Last Taught</th><th>Date Last Reviewed</th></tr>
<tr><td><b>Must include hands-on lab exercises.</b>

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:<ul><li><b>Routing, network and application protocols including TCP/IP (versions 4 and 6), ARP, BGP, SSL/TLS, DNS, SMTP, HTTP</b></li><li><b>Network architectures</b></li><li><b>Network security</b></li><li><b>Wireless network technologies</b></li><li><b>Network traffic analysis</b></li><li><b>Protocol analysis (examining component-to-component communication to determine the protocol being used and what it is doing)</b></li><li><b>Network mapping techniques (active and passive)</b></li></ul></td><td><b>SY283N (SY205): Networking: Operations and Analysis</b>
<b>SY308: Security Fundamental Principles</b><table><tr><td>Routing, network, and application protocols including:<ul><li>TCP/IP (versions 4 and 6)</li><li>ARP, BGP, SSL/TLS</li><li>DNS</li><li>SMTP</li><li>HTTP</li></ul></td><td>IPv4: SY205, current.
IPv6: SY205, planned CY2020 Fall.
ARP: SY205, current.
BGP: SY205, planned CY2020 Fall.
SSL/TLS: SY308, current.
DNS: SY205, planned CY2020 Fall.
SMTP: SY205, planned CY2020 Fall.
HTTP: SY205, planned CY2020 Fall.
SY301: Djikstra’s Algo.</td></tr><tr><td>Network architectures</td><td>SY205: current partial, expansion planned CY2020 Fall.</td></tr><tr><td>Network security</td><td>SY205: current partial, expansion planned CY2020 Fall.</td></tr></table></td><td><b>SY283N (SY205): LCDR Chris Hoffmeister</b>

<b>SY308: Dr Travis Mayberry, Dr Ellis Fenske</b></td><td><b>SY283N (SY205): Fall CY2019</b>

<b>SY308: Spring CY2020</b></td><td><b>SY283N (SY205): Fall CY2019</b>

<b>SY308: Spring CY2020</b></td></tr>
</table>

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.		SY308: TLS, certificates, PKI, symmetric and asymmetric ciphers, MACs			
	Wireless network technologies	SY312 (SY488A): planned CY2020 Spring.			
	Network traffic analysis	SY205: current.			
	Protocol analysis (examining component-to-component communication to determine the protocol being used and what it is doing)	SY205: current, expansion planned CY2020 Fall.			
	Network mapping techniques (active and passive)	SY205: planned CY2020 Fall (traceroute, nmap, p0f, DNS Zone transfer, Banner grabbing, and studying traffic analysis [HTTP, SMTP]). SY401: nmap used extensively for passive and active recon in Labs.			
M.5 Cellular and Mobile Technologies	**Course # and Course Title**		**Instructor(s)**	**Date Last Taught**	**Date Last Reviewed**
As more communications are conducted via mobile and cellular technologies, these technologies have become critical (and continue	**SY488A (SY312): Digital and Mobile Communications**		**SY488A (SY312): LCDR**	**SY488A (SY312)**	**SY488A (SY312):**

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.	Overview of smart phone technologies	Covered in one class period. This entire course (SY312/SY488A) was designed based on feedback from the NSA-CAE application in 2018.	**James Shey**	**: Spring CY2020**	**Spring CY2020**
	Overview of embedded operating systems (e.g., iOS, Android)	While not explicitly covered in SY312/SY488A, students will meet the outcome noted below. SY401 does discuss exploitation of these OSs as part of the Kali Linux toolkit.			
	Wireless technologies (mobile: GSM, WCDMA, CDMA2000, LTE; and Internet: 802.11b/g/n)	GSM 4 class periods, LTE 3 class periods, WiFi 2 class periods.			
	Infrastructure components (e.g., fiber optic network, evolved packet core, PLMN)	Topics covered: fiber optics, Ethernet, coaxial transmissions to include signal loss over a distance, bandwidth and applicable tables and equations (2 classes). Evolved packet core and PLMN covered by white papers and in class discussions (2 classes).			
	Mobile protocols (SS7, RR, MM, CC)	Covered by whitepapers and in class discussions (1 class period). TDMA, CDMA, FDMA covered in 1 class period. Signal encoding covered 2 class periods.			
	Mobile logical channel descriptions (BCCH, SDCCH, RACH, AGCH, etc.)	Covered by whitepapers and in class discussions (1 class).			

Mobile registration procedures	Covered by whitepapers and in class discussions (1 class).
Mobile encryptions standards	In SY308 - discussion of A5/1 in GSM and how it was broken in the early 2000s, leading to the many security and privacy issues with cellular phones along with discussion of the replacement cipher used in 4G and 5G called SNOW.
Mobile identifiers (IMSI, IMEI, MSISDN, ESN, Global Title, E.164)	Covered by whitepapers and in class discussions (1 class).
Mobile and Location-based Services	Covered by whitepapers and in class discussions (1 class).

M.6 Discrete Math and Algorithms	Course # and Course Title	Instructor(s)	Date Last Taught	Date Last Reviewed
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**	**SM242: Discrete Math** **SY301: Data Structures** **SY308: Security Fundamental Principles**	**SM242: Dr Carolyn Chun** **SY301: Dean Peter Nardi** **SY301: Dr April Edwards** **SY301: Dr Travis Mayberry**	**SM242: Fall CY2019** **SY301: Fall CY2019** **SY308: Fall CY2019**	**SM242: Fall CY2019** **SY301: Fall CY2019** **SY308: Fall CY2019**

Searching and sorting algorithms	SY301
Complexity theory	SY301

<table>
<tr>
<td>• <b>Complexity theory</b>
• <b>Regular expressions</b>
• <b>Computability</b>
• <b>Mathematical foundations for cryptography</b>
• <b>Entropy</b>

<b><i>Outcome</i>:</b> 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.
<b><i>Outcome</i>:</b> Students will understand how variability affects outcomes, how to identify anomalous events, and how to identify the meaning of anomalous events.
<b><i>Outcome</i>:</b> 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.</td>
<td>
<table>
<tr><td>Regular expressions</td><td>SY205 - Shell/Command Line operations
SY402 - use GREP & Python scripting to sort files/logs</td></tr>
<tr><td>Computability</td><td>SY301, SY308</td></tr>
<tr><td>Mathematical foundations for cryptography</td><td>SY308</td></tr>
<tr><td>Entropy</td><td>SY308</td></tr>
</table>
</td>
<td><b>SY308: Dr. Travis Mayberry</b></td>
<td></td>
<td></td>
</tr>
<tr>
<th>M.7 Overview of Cyber Defense</th>
<th>Course # and Course Title</th>
<th>Instructor(s)</th>
<th>Date Last Taught</th>
<th>Date Last Reviewed</th>
</tr>
<tr>
<td><b>Must include hands-on lab exercises.</b>

Cyber operations encompass both offensive and defensive operations. Defensive operations are essential in protecting our systems and associated digital assets. Understanding how</td>
<td><b>SY304: Human Factors in Cyber Operations</b>
<b>SY308: Security Fundamental Principles</b>
<b>SY401: Cyber Operations Capstone I (Offensive Operations)</b>
<b>SY402: Cyber Operations Capstone II (Defensive Operations)</b></td>
<td><b>SY304: LCDR Joseph Hatfield</b></td>
<td><b>SY304: Spring CY2020</b></td>
<td><b>SY304: Spring CY2020</b></td>
</tr>
</table>

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.	Identification of reconnaissance operations	These techniques are demonstrated in labs and lectures in SY401 as both passive and active reconnaissance using open source tools such as NMAP.	**SY308: Dr Travis Mayberry** **SY401/402: Mr. Dennis Dias**	**SY308: Spring CY2020** **SY401: Fall CY2019** **SY402: Spring CY2020**	**SY308: Spring CY2020** **SY401: Fall CY2019** **SY402: Spring CY2020**
	Anomaly/intrusion detection	These techniques are demonstrated in labs and lectures in SY402 using student built rules in python and using SNORT.			
	Anomaly identification	These are demonstrated in SY402 labs using SPLUNK and SNORT using rules and behavior based labs.			
	Identification of command and control operations	These are discussed and demonstrated in SY401 (offensive operations) and SY402 (defensive operations). The development of C&C infrastructure using VMs is also discussed and demonstrated in labs/lectures using Metasploit, Armitage, and ToR.			
	Identification of data exfiltration activities	These are demonstrated in labs and lectures in SY401/402. We discuss COVCOM and use of ToR for hiding traffic as well as use of exploits that take advantage of routine services and ports to exfil traffic from a host or network. See SY401 course material			
	Identifying malicious code based on signatures, behavior and artifacts	These are demonstrated in labs and lectures in SY401/402. We discuss the use of VirusTotal for identifying hashes and SHAs as well as how AV leverages			

		cloud based and behavioral characteristics			
	Network security techniques and components (e.g., firewalls, IDS, etc.)	These are demonstrated in labs and lectures in SY401/402 using open source tools such as SNORT and packet sniffers Firewalls: SY205, planned CY2020 Fall.			
	Cryptography (include PKI cryptography) and its uses in cybersecurity	SY308 discusses this area and this is re-enforces in SY401 and 402.			
	Malicious activity detection	These are discussed and demonstrated in labs and lectures in SY401/402 using open source monitoring tools such as SNORT and SPLUNK Agents			
	System security architectures and concepts	Gen Sys Sec: SY204 supports these concepts such as Hiding from ls, Untouchables.			
	Defense in depth	These are demonstrated in labs and lectures in SY401/402. This is analogous to US Navy defense in depth leveraged in Naval Operations by Carrier Battlegroups. There is no single cybersecurity tool that can protect a network - and all elements of the problems are discussed - from human faults, HW/SW faults to physical vulnerabilities.			

Trust relationships	Exploiting trust is demonstrated inn SY401 using the Social Engineering Toolkit in Metasploit. Use of the Veil framework demonstrates in labs how to defeat AV products in offensive operations.
Distributed/Cloud	This is covered in SY401/402 with a special lecture from NSA CAPS representative on large software development.
Virtualization	These are demonstrated in labs and lectures in SY401/402. Virtual Machines are created and used in a variety of lab applications as well as a hypervisor in the USNA cyber.moboard environment.

M.8 Security Fundamental Principles (i.e., "First Principles")	**Course # and Course Title**	**Instructor(s)**	**Date Last Taught**	**Date Last Reviewed**
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	**SY201: Cyber Fundamentals I** **SY202: Cyber Systems Engineering** **SY204: Systems Programing and Operating Systems Fundamentals** **SY205: Networking: Operations and Analysis** **SY303: Cyber Systems Architecture** **SY308: Security Fundamental Principles**	**SY201: LT Timmy Galvin** **SY202: CDR Paul Frontera** **SY204/205: LCDR Chris Hoffmeister**	**SY201: Fall CY2019** **SY202: Spring CY2020** **SY204: Spring CY2020**	**SY201: Fall CY2019** **SY202: Spring CY2020** **SY204: Spring CY2020**

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	General Fundamental design principles including: • Simplicity • Open Design • Design for Iteration • Least Astonishment	Simplicity: SY201, SY301, SY308 Open Design: SY205, current (RFCs), SY308 Design Iteration: SY201, SY204, SY308 Least Astonishment: SY308	**SY303: Dr Dane Brown** **SY308: Dr Travis Mayberry**	**SY205: Fall CY2019** **SY303: Fall CY2019** **SY308: Spring CY2020**	**SY205: Fall CY2019** **SY303: Fall CY2019** **SY308: Spring CY2020**
	Security Design Principles including: • Minimize Secrets • Complete Mediation • Fail-safe Defaults • Least Privilege • Economy of Mechanism • Minimize Common Mechanism • Isolation, Separation and Encapsulation	Gen Sec Prin: SY204, current. Least Priv: SY201, SY204, current. All: SY308			
	Methods for Reducing Complexity including: • Abstraction • Modularity • Layering • Hierarchy	Abstraction: SY204, current; SY205, current; SY301 Modularity: SY204, current; SY301 Layering: SY205, current. Hierarchy: SY205, current; SY301			

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	**Course # and Course Title**	**Instructor(s)**	**Date Last Taught**	**Date Last Reviewed**
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**	**IC411: Operating Systems** **SY304: Human Factors in Cyber Operations** **SY306: Web and Databases for Cyber Operations** **SY308: Security Fundamental Principles** **SY401: Cyber Operations I Capstone (Offensive Operations)** **SY402: Cyber Operations II Capstone (Defensive Operations)**	**IC411: Prof Rick Schlichting** **SY304: LCDR Joseph Hatfield** **SY306: Dr Kirsten Richards** **SY401/402: Mr Dennis Dias**	**IC411: Fall CY2019** **SY304: Spring CY2020** **SY306: Spring CY20220** **SY401: Fall CY2019** **SY402: Spring CY2020**	**IC411: Fall CY2019** **SY304: Spring CY2020** **SY306: Spring CY20220** **SY401: Fall CY2019** **SY402: Spring CY2020**

Outcome: Students will possess a thorough understanding of the various types of vulnerabilities, 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	**Course # and Course Title**	**Instructor(s)**	**Date Last Taught**	**Date Last Reviewed**
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**	**SY304: Human Factors in Cyber Operations** **SY406: Cyber Policy and Law** **SY401: Cyber Operations I Capstone (Offensive Operations)** **SY402: Cyber Operations II Capstone (Defensive Operations)**	**SY304: Mr Chris Inglis, former NSA Deputy Director** **SY304: LCDR Joseph Hatfield** **SY406: Professor Jeff Kosseff** **SY401/402: Mr Dennis Dias**	**SY304: Spring CY2020** **SY406: Spring CY2020** **SY401: Fall CY2019** **SY402: Spring CY2020**	**SY304: Spring CY2020** **SY406: Spring CY2020** **SY401: Fall CY2019** **SY402: Spring CY2020**

▪ 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 KNOWLEDGE UNITS	**Course # and Course Title**	**Instructor(s)**	**Date Last Taught**	**Date Last Updated**

<table>
<tr><td><b>Note:</b> To qualify for designation as a CAE in Cyber Operations, the institution/program must demonstrate that their curriculum satisfactorily <b>covers minimally <u>10 of the 17</u></b> Optional KUs to the desired breadth and depth. 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.
<b>Note:</b> A course description and syllabus containing a weekly schedule of topics must be included in the application package for all courses identified in this KU Alignment Worksheet</td><td></td><td></td><td></td><td></td></tr>
<tr><td><b>O.1 Programmable Logic</b></td><td><b>Course # and Course Title</b></td><td><b>Instructor(s)</b></td><td><b>Date Last Taught</b></td><td><b>Date Last Updated</b></td></tr>
<tr><td><b>Must include hands-on lab exercises.</b>
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:<ul><li><b>Hardware design/programming languages (e.g. VHSIC Hardware Design Language (VHDL), Verilog, OpenCL)</b></li><li><b>Programmable logic devices (Programmable Logic Controllers (PLC), Fully Programmable Gate Arrays (FPGA))</b></li></ul></td><td><b>SY202: Cyber Systems Engineering
SY303: Cyber Systems Architecture</b><table><tr><td><b><u>Topic</u></b></td><td><b><u>Assessment</u></b></td></tr><tr><td><b>Hardware design/programming languages (e.g. VHSIC Hardware Design Language (VHDL), Verilog, OpenCL)</b></td><td><b>Covered in SY202 and SY303</b></td></tr><tr><td><b>Programmable logic devices (Programmable Logic Controllers (PLC), Fully Programmable Gate Arrays (FPGA))</b></td><td><b>SY303 covers design and implementation of a simple yet functional computer using NAND gates and D Flip-Flops</b></td></tr></table></td><td><b>SY202: CDR Paul Frontera
SY303: Dr. Dane Brown</b></td><td><b>SY202: Spring CY2020
SY303: Fall CY2019</b></td><td><b>SY202: Spring CY2020
SY303: Fall CY2019</b></td></tr>
</table>

<table>
<tr>
<td><b><i>Outcome</i></b>: 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.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<th>O.2 Wireless Security</th>
<th>Course # and Course Title</th>
<th>Instructor(s)</th>
<th>Date Last Taught</th>
<th>Date Last Updated</th>
</tr>
<tr>
<td><b>Must include hands-on lab exercises.</b>

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:
• <b>A comparison of security implementations in different wireless technologies (e.g., 2G/3G/4G/Wi-Fi/Bluetooth/RFID)</b>
• <b>Confidentiality, integrity and availability policy enforcement considerations in wireless networks</b>
• <b>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)</b>
• <b>Security protocols used in wireless communications and how each addresses issues of authentication, integrity,</b></td>
<td><b>SY488A (SY312): Digital and Mobile Communications</b>
<table>
<tr><th><u>Topic</u></th><th><u>Assessment</u></th></tr>
<tr><td><b>A comparison of security implementations in different wireless technologies (e.g., 2G/3G/4G/Wi-Fi/Bluetooth/RFID)</b></td><td><b>Covered in SY488A</b></td></tr>
<tr><td><b>Confidentiality, integrity and availability policy enforcement considerations in wireless networks</b></td><td><b>Covered in SY488A</b></td></tr>
<tr><td><b>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)</b></td><td><b>Mobile protocols, identifiers covered in SY488A</b></td></tr>
<tr><td><b>Security protocols used in wireless communications and how each addresses issues of authentication, integrity, and confidentiality (e.g. COMP128, UIA, TKIP, CCMP, SSP, E1)</b></td><td><b>Mobile protocols, identifiers covered in SY488A</b></td></tr>
</table>
</td>
<td><b>SY488A (SY312): LCDR James Shey</b></td>
<td><b>SY488A (SY312): Spring 2020</b></td>
<td><b>SY488A (SY312): Spring 2020</b></td>
</tr>
</table>

<table>
<tr>
<td>

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.

</td>
<td>
<table>
<tr><td><b>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)</b></td><td><b>Vulnerabilities covered in SY488A</b></td></tr>
<tr><td><b>Security issues in hardware and software architectures of wireless devices</b></td><td><b>Covered in SY488A</b></td></tr>
<tr><td><b>Common ciphers, their implementations, advantages and disadvantages for use in securing wireless networks</b>
• <b>Stream ciphers (e.g. E0, RC4, A5, SNOW, ZUC)</b>
• <b>Block ciphers (e.g. Kasumi, SAFER, AES)</b></td><td><b>Covered in SY488A</b></td></tr>
</table>
</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><b>O.3 Virtualization</b></td>
<td><b>Course # and Course Title</b></td>
<td><b>Instructor(s)</b></td>
<td><b>Date Last Taught</b></td>
<td><b>Date Last Updated</b></td>
</tr>
<tr>
<td><b>Must include hands-on lab exercises.</b>

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</td>
<td><b>SY401: Cyber Operations I</b>
<b>SY402: Cyber Operations II</b>
<table>
<tr><th><b><u>Topic</u></b></th><th><b><u>Assessment</u></b></th></tr>
</table>
</td>
<td><b>SY401/402: Mr. Dennis Dias</b></td>
<td><b>SY401: Fall CY2019</b></td>
<td><b>SY401: Fall CY2019</b></td>
</tr>
</table>

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	**Type I and Type II architectures**	**DIscussed in SY401 and SY402 - extensive use of VMs for weekly labs. We use Type I (via VMWare ESXI) and discuss the use Type II. Students have extensive experience creating, leveraging, and attacking VMs in both classes.**		**SY402: Spring CY2020**	**SY402: Spring CY2020**
	Virtualization Principles including efficiency, resource control and equivalence	**These topics are discussed in classroom lectures and applied in weekly labs in both SY401 and SY402.**			
	Virtualization techniques for code execution, including trap and emulate, binary translation, paravirtualization, and hardware-supported virtualization (e.g., Intel VMX)	**CST, SY401**			
	Management of memory in virtualized systems, including hardware supported memory management (e.g. EPT/SLAT), memory deduplication, and	**SY303 and SY401**			

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.	**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)	**These techniques are discussed and applied using VMWare in SY401 and 402 labs**			
	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	**SY401/402 supported by a faculty member and in CST**			
O.4 Cloud Security/Cloud Computing	**Course # and Course Title**		**Instructor(s)**	**Date Last Taught**	**Date Last Updated**

<table>
<tr>
<td>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:
<ul>
<li><b>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)</b></li>
<li><b>Essential Characteristics of Cloud Platforms and an understanding of the technologies that enable these characteristics</b></li>
<li><b>Common Service models</b></li>
<li><b>Common Deployment Modes (e.g. public cloud, private cloud, hybrid cloud) and the associated tradeoffs (e.g. privacy/scalability/resilience)</b></li>
<li><b>Cloud infrastructure components, and the interfaces the 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)</b></li>
<li><b>Techniques for deploying and scaling cloud resources (such as Puppet/Chef)</b></li>
<li><b>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</b></li>
</ul></td>
<td><b>SY486C: Cloud Security and Cryptography</b>
<table>
<tr><th><u>Topic</u></th><th><u>Assessment</u></th></tr>
<tr><td><b>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)</b></td><td><b>Covered in SY486C</b></td></tr>
<tr><td><b>Essential Characteristics of Cloud Platforms and an understanding of the technologies that enable these characteristics</b></td><td></td></tr>
<tr><td><b>Common Service models</b></td><td></td></tr>
<tr><td><b>Common Deployment Modes (e.g. public cloud, private cloud, hybrid cloud) and the associated tradeoffs (e.g. privacy/scalability/resilience)</b></td><td></td></tr>
<tr><td><b>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)</b></td><td><b>Covered in SY486C</b></td></tr>
<tr><td><b>Techniques for deploying and scaling cloud resources (such as Puppet/Chef)</b></td><td></td></tr>
<tr><td><b>Security implication of cloud resources, including issues associated with shared resources and multi-tenancy, the extension of trust to include the cloud</b></td><td></td></tr>
</table></td>
<td><b>SY486C: Dr. Travis Mayberry</b></td>
<td><b>SY486C: Spring CY2018</b></td>
<td><b>SY486C: Spring CY2018</b></td>
</tr>
</table>

<table>
<tr>
<td>

- **Developing, deploying, and managing applications on cloud resources, which should include hand-on exercises that utilize real cloud services**

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.
</td>
<td>
<table>
<tr><td><b>provider, and approaches to mitigating these issues</b></td><td></td></tr>
<tr><td><b>Developing, deploying, and managing applications on cloud resources, which should include hand-on exercises that utilize real cloud services</b></td><td></td></tr>
</table>
</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<th>O.5 Risk Management of Information Systems</th>
<th>Course # and Course Title</th>
<th>Instructor(s)</th>
<th>Date Last Taught</th>
<th>Date Last Updated</th>
</tr>
<tr>
<td>

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)**
</td>
<td>
<b>SY402: Cyber Operations II</b>
<table>
<tr><td><b><u>Topic</u></b></td><td><b><u>Assessment</u></b></td></tr>
<tr><td><b>Risk Models (e.g. NIST SP 800-39 Managing Information Security Risk)</b></td><td><b>SY402 has several lectures on the NIST frameworks and Risk models and processes</b></td></tr>
<tr><td><b>Risk Processes (e.g. NIST SP 800-37 Risk Management Framework)</b></td><td><b>SY402 has several lectures on the NIST frameworks and Risk models and processes</b></td></tr>
</table>
</td>
<td><b>SY402: Mr. Dennis Dias</b></td>
<td><b>SY402: Spring CY2020</b></td>
<td><b>SY402: Spring CY2020</b></td>
</tr>
</table>

<table>
<tr>
<td>• <b>Risk Processes (e.g. NIST SP 800-37 Risk Management Framework)</b>

<b><i>Outcome</i></b>: Students will be able to identify, measure (quantitative and qualitative), and mitigate key information technology risks.
<b><i>Outcome</i></b>: Students will also be able to describe each of the tasks associated with risk framing, assessment, response and monitoring.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<th>O.6 Computer Architecture (includes Logic Design)</th>
<th>Course # and Course Title</th>
<th>Instructor(s)</th>
<th>Date Last Taught</th>
<th>Date Last Updated</th>
</tr>
<tr>
<td>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:
• <b>Organization of computer and processor architectures</b>
• <b>Instruction set design alternatives</b>
• <b>Processor implementation</b>
• <b>Memory system hierarchy</b>
• <b>Buses</b>
• <b>I/O systems</b>
• <b>Factors affecting performance</b>

<b><i>Outcome</i></b>: 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.</td>
<td><b>SY303: Cyber Systems Architecture</b>
<b>SY485J: Reverse Engineering</b>
<table>
<tr><th><u>Topic</u></th><th><u>Assessment</u></th></tr>
<tr><td>Organization of computer and processor architectures</td><td>Covered in SY303 and SY485J</td></tr>
<tr><td>Instruction set design alternatives</td><td>MBED and ARM in SY303</td></tr>
<tr><td>Processor implementation</td><td>Covered in SY303</td></tr>
<tr><td>Memory system hierarchy</td><td>Covered in SY303</td></tr>
<tr><td>Buses</td><td>Covered in SY303</td></tr>
<tr><td>I/O systems</td><td>Covered in SY303</td></tr>
</table>
</td>
<td><b>SY303: Dr. Dane Brown</b>

<b>SY485J: Mr. Mark Debels</b></td>
<td><b>SY303: Fall CY2019</b>

<b>SY485J: Fall CY2019</b></td>
<td><b>SY303: Fall CY2019</b>

<b>SY485J: Fall CY2019</b></td>
</tr>
</table>

<table>
<tr><td></td><td><table><tr><td>Factors affecting performance</td><td>Covered in SY303</td></tr></table></td><td></td><td></td><td></td></tr>
<tr><th>O.7 Microcontroller Design</th><th>Course # and Course Title</th><th>Instructor(s)</th><th>Date Last Taught</th><th>Date Last Updated</th></tr>
<tr><td><b>Must include hands-on lab exercises.</b>

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:<ul><li><b>Typical instruction sets and architectures</b></li><li><b>Common programming environments for microcontrollers</b></li><li><b>How the real-time requirements and simple architecture of the typical microcontroller require special programming considerations</b></li><li><b>Cyber considerations and issues related to microcontrollers and the larger systems they are typically integrated into</b></li></ul><i><b>Outcome</b></i>: 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.</td><td>SY202: Cyber Systems Engineering
SY303: Cyber Systems Architecture<table><tr><td><u>Topic</u></td><td><u>Assessment</u></td></tr><tr><td>Typical instruction sets and architectures</td><td>Covered in SY303</td></tr><tr><td>Common programming environments for microcontrollers</td><td>MATLAB, MS VS Code platform IO in SY202</td></tr><tr><td>How the real-time requirements and simple architecture of the typical microcontroller require special programming considerations</td><td>Covered in SY202 through application and SY303 through discussion</td></tr><tr><td>Cyber considerations and issues related to microcontrollers and the larger systems they are typically integrated into</td><td>Covered in SY202 and SY303 through discussion</td></tr></table></td><td>SY202: CDR Paul Frontera

SY303: Dr. Dane Brown</td><td>SY202: Spring CY2020

SY303: Fall CY2019</td><td>SY202: Spring CY2020

SY303: Fall CY2019</td></tr>
</table>

<table>
<tr><th>O.8 Software Security Analysis</th><th>Course # and Course Title</th><th>Instructor(s)</th><th>Date Last Taught</th><th>Date Last Updated</th></tr>
<tr>
<td><b>Must include hands-on lab exercises.</b>
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:
• <b>Source code analysis</b>
• <b>Binary code analysis</b>
• <b>Static code analysis techniques</b>
• <b>Dynamic code analysis techniques</b>
• <b>Testing methodologies (Black Box/White Box/Fuzz)</b>
<b><i>Outcome</i></b>: 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.</td>
<td><b>SY485J: Reverse Engineering</b>
<table>
<tr><th><u>Topic</u></th><th><u>Assessment</u></th></tr>
<tr><td>Source code analysis</td><td>SY485J covers this
Lab 1 covers C Source code analysis and other labs require Ghidra use and analysis for source code analysis</td></tr>
<tr><td>Binary code analysis</td><td>All labs in this class except for Lab 1, require binary analysis</td></tr>
<tr><td>Static code analysis techniques</td><td>Static analysis is the backbone for SY485J - Objdump and Ghidra are used for this.</td></tr>
<tr><td>Dynamic code analysis techniques</td><td>Dynamic analysis must be used in half the labs in SY485J. gdb is the the primary tool used.</td></tr>
<tr><td>Testing methodologies (Black Box/White Box/Fuzz)</td><td>Fuzzing is a method that is discussed and demoed in class as a way to test software before reversing - testing extreme input/output possibilities to observe behavior of software. SY485J stresses the importance of all kinds of testing of software, not just reverse engineering, to build a complete picture of what the software is doing.</td></tr>
</table>
</td>
<td><b>SY485J: Mr. Mark Debels</b></td>
<td><b>SY485J: Fall CY2019</b></td>
<td><b>SY485J: Fall CY2019</b></td>
</tr>
</table>

<table>
<tr><th>O.9 Secure Software Development (Building Secure Software)</th><th>Course # and Course Title</th><th>Instructor(s)</th><th>Date Last Taught</th><th>Date Last Updated</th></tr>
<tr><td><b>Must include hands-on lab exercises.</b>

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:
• <b>Secure programming principles and practices</b>
• <b>Constructive techniques (What process might provide for “good code.”)</b>

<b><i>Outcome</i></b>: 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.
<b><i>Outcome</i></b>: 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.</td><td><b>SY201: Cyber Fundamentals I</b>
<b>SY204: Systems Programming & OS Fundamentals</b>
<b>SY308: Security Fundamental Principles</b><table><tr><th><u>Topic</u></th><th><u>Assessment</u></th></tr><tr><td><b>Secure programming principles and practices</b></td><td><b>SY201: user input validation, safe exception handling, trust relationship with compiler/interpreter</b>
<b>SY308: Using memory-safe functions, format string vulnerabilities and prevention</b></td></tr><tr><td><b>Constructive techniques (What process might provide for "good code.")</b></td><td><b>SY201: concept of least privilege</b>
<b>SY308: Fundamental security principles, economy of mechanism, failsafe default</b></td></tr></table></td><td><b>SY201: LT Timothy Galvin</b>

<b>SY204: LCDR Chris Hoffmeister</b>

<b>SY308: Dr. Travis Mayberry</b></td><td><b>SY201: Fall CY2019</b>

<b>SY204: Spring CY2020</b>

<b>SY308: Spring CY2020</b></td><td><b>SY201: Fall CY2019</b>

<b>SY204: Spring CY2020</b>

<b>SY308: Spring CY2020</b></td></tr>
<tr><th>O.10 Embedded Systems</th><th>Course # and Course Title</th><th>Instructor(s)</th><th>Date Last Taught</th><th>Date Last Updated</th></tr>
<tr><td><b>Must include hands-on lab exercises.</b>

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</td><td><b>SY202: Cyber Systems Engineering</b>
<b>SY303: Cyber Systems Architecture</b></td><td><b>SY202: CDR Paul Frontera</b>

<b>SY303: Dr. Dane Brown</b></td><td><b>SY202: Spring CY2020</b></td><td><b>SY202: Spring CY2020</b></td></tr>
</table>

<table>
<tr>
<td>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:<ul><li><b>Typical instruction sets and architectures</b></li><li><b>Common operating systems and programming environments for embedded systems</b></li><li><b>How the real-time requirements typical of embedded systems require differences in the OS & applications</b></li><li><b>Cyber considerations and issues related to embedded systems</b></li></ul><b><i>Outcome</i></b>: 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.</td>
<td><table>
<tr><th><u>Topic</u></th><th><u>Assessment</u></th></tr>
<tr><td><b>Typical instruction sets and architectures</b></td><td><b>Covered in SY303</b></td></tr>
<tr><td><b>Common operating systems and programming environments for embedded systems</b></td><td><b>Covered in SY303</b></td></tr>
<tr><td><b>How the real-time requirements typical of embedded systems require differences in the OS & applications</b></td><td><b>Covered in SY303</b></td></tr>
<tr><td><b>Cyber considerations and issues related to embedded systems</b></td><td><b>Discussed in SY202 and SY303</b></td></tr>
</table></td>
<td></td>
<td><b>SY303: Fall CY2019</b></td>
<td><b>SY303: Fall CY2019</b></td>
</tr>
<tr>
<th>O.11 Digital Forensics</th>
<th>Course # and Course Title</th>
<th>Instructor(s)</th>
<th>Date Last Taught</th>
<th>Date Last Updated</th>
</tr>
<tr>
<td><b>Must include hands-on lab exercises.</b>

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</td>
<td><b>SY485: Cyber Crime Investigations</b><table>
<tr><th>Topic</th><th>Assessment</th></tr>
<tr><td><b>Operating system forensics</b></td><td><b>File system forensics, Memory Forensics, Registry Analysis lectures and Imaging drives and</b></td></tr>
</table></td>
<td><b>SY485: Dr. Tony Melaragno</b></td>
<td><b>SY485: Fall CY2018</b></td>
<td><b>SY485: Fall CY2018</b></td>
</tr>
</table>

<table>
<tr>
<td>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:<ul><li><b>Operating system forensics</b></li><li><b>Device/Media forensics</b></li><li><b>Network forensics</b></li><li><b>Memory forensics</b></li></ul><b><i>Outcome</i></b>: 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.
<b><i>Outcome</i></b>: Students will be able to understand how to identify forensic artifacts left by attacks.
<b><i>Outcome</i></b>: Students will be able to understand how to acquire a forensically sound image.</td>
<td><table>
<tr><td></td><td><b>operating systems, File system Forensics and NTFS labs.</b></td></tr>
<tr><td><b>Device/Media Forensics</b></td><td><b>Memory Forensics, Mobile Forensics lectures and Forensics Tools, Volatility, Autopsy, Imaging Drives and Operating Systems, Graphics Files lab.</b></td></tr>
<tr><td><b>Network Forensics</b></td><td><b>Email investigations lecture and Mobile Forensics labs.</b></td></tr>
<tr><td><b>Memory forensics</b></td><td><b>Memory Forensics lecture and Volatility lab.</b></td></tr>
</table></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<th>O.12 Systems Programming</th>
<th>Course # and Course Title</th>
<th>Instructor(s)</th>
<th>Date Last Taught</th>
<th>Date Last Updated</th>
</tr>
<tr>
<td><b>Must include hands-on lab exercises.</b>

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.</td>
<td><b>EC404: Operating Systems
EC462: Superscalar Process Design
EC463: Microcomputer Interfacing</b><table>
<tr><td><b><u>Topic</u></b></td><td><b><u>Assessment</u></b></td></tr>
<tr><td><b>Kernel modules</b></td><td><b>EC404 (Dr Delozier)</b></td></tr>
</table></td>
<td><b>EC404: Dr. Christian Delozier

EC462: Dr. Rakvic

EC463: Dr. Ngo</b></td>
<td><b>EC404: Spring CY2020

EC462: Spring CY2020

EC463: Fall CY2019</b></td>
<td><b>EC404: Spring CY2020

EC462: Spring CY2020

EC463: Fall CY2019</b></td>
</tr>
</table>

<table>
<tr>
<td>Specific topics to be covered in this knowledge unit include, but are not limited to:<ul><li><b>Kernel modules</b></li><li><b>Device drivers</b></li><li><b>Multi-threading</b></li><li><b>Use of alternate processors (e.g., graphics card processors)</b></li></ul>
<b><i>Outcome</i></b>: 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 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).</td>
<td><table>
<tr><td><b>Device drivers</b></td><td><b>EC463 (Controllers and Drivers) Dr Ngo</b></td></tr>
<tr><td><b>Multi-threading</b></td><td><b>EC404 (Operating Systems) Dr Delozier</b></td></tr>
<tr><td><b>Use of alternate processors (e.g., graphics card processors)</b></td><td><b>EC462 (Dr Rakvic)</b></td></tr>
</table></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><b>O.13 Applied Cryptography</b></td>
<td><b>Course # and Course Title</b></td>
<td><b>Instructor(s)</b></td>
<td><b>Date Last Taught</b></td>
<td><b>Date Last Updated</b></td>
</tr>
<tr>
<td>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:<ul><li><b>Cryptographic primitives (e.g. randomization)</b></li><li><b>Symmetric and asymmetric cryptography, hash functions and data integrity, public-key encryption and digital signatures, key establishment and key management</b></li><li><b>The appropriate application of different types of cryptography to Internet security, computer security and communications security</b></li></ul></td>
<td><b>SY308: Security Fundamental Principles</b>
<b>SY486C (CY2018): Cloud Security and Cryptography</b>
<b>SY486C (CY2020): Anonymous Communication</b>
<table>
<tr><td><b><u>Topic</u></b></td><td><b><u>Assessment</u></b></td></tr>
<tr><td><b>Cryptographic primitives (e.g. randomization)</b></td><td><b>SY308: Pseudorandom number generators</b></td></tr>
<tr><td><b>Symmetric and asymmetric cryptography, hash functions and data integrity, public-key encryption and digital signatures, key</b></td><td><b>SY308: Block ciphers, stream ciphers, RSA, Diffie Hellman, ElGamal, hash functions, MACs, PKI, certificates</b></td></tr>
</table></td>
<td><b>SY308: Dr. Travis Mayberry</b>

<b>SY486C (CY2018): Dr. Travis Mayberry</b>

<b>SY486C (CY2020): Dr. Ellis Fenske</b></td>
<td><b>SY308: Spring CY2020</b>

<b>SY486C (CY2018): Spring CY2018</b>

<b>SY486C (CY2020): Spring CY2020</b></td>
<td><b>SY308: Spring CY2020</b>

<b>SY486C (CY2018): Spring CY2018</b>

<b>SY486C (CY2020): Spring CY2020</b></td>
</tr>
</table>

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.	**establishment and key management**	**SY486C: Homomorphic encryption**			
	The appropriate application of different types of cryptography to Internet security, computer security and communications security	**SY308: SSL/TLS** **SY486C (CY2020): Tor, blockchains, end-to-end cryptographic voting, searchable encryption, oblivious RAM, private information retrieval**			

O.14 Industrial Control System (ICS)	**Course # and Course Title**		**Instructor(s)**	**Date Last Taught**	**Date Last Updated**
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**	**SY202: Cyber Systems Engineering** **SY401: Cyber Operations I** **IT432: Advanced Computer Networks and Security**		**SY202: CDR Paul Frontera** **SY401: Mr. Dennis Dias** **IT432: Dr. Michael Oehler**	**SY202: Spring CY2020** **SY401: Fall CY2019** **IT432: Fall CY2019**	**SY202: Spring CY2020** **SY401: Fall CY2019** **IT432: Fall CY2019**
	Topic	**Assessment**			
	SCADA	**SY401 dedicates a full lesson to reviewing the Stuxnet case as detailed in the Symantec report on the malware as well as documented in the book Countdown to Zero Day.**			
	DCS	**Covered by guest speakers in SY202**			

<table>
<tr>
<td>

- **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.
</td>
<td>
<table>
<tr><td><b>Vulnerabilities, countermeasures and attacks of ICS ecosystems</b></td><td><b>Covered in IT432 lessons</b></td></tr>
</table>
</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<th>O.15 User Experience (UX)/Human Computer Interface (HCI) Security</th>
<th>Course # and Course Title</th>
<th>Instructor(s)</th>
<th>Date Last Taught</th>
<th>Date Last Updated</th>
</tr>
<tr>
<td>

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:

- **The Authentication interfaces and passwords**
- **Implicit and explicit policies in systems**
</td>
<td>
<b>SY304: Human Factors in Cyber Operations</b>
<table>
<tr><th><u>Topic</u></th><th><u>Assessment</u></th></tr>
<tr><td><b>Authentication interfaces and passwords</b></td><td><b>Authentication interfaces are discussed in SY304 as primary topics in four lessons, while they are touched upon in six additional lessons as a secondary focus. One lesson has passwords and the psychology of password management as its central topic, while passwords in general are used as examples and secondary topics in four additional</b></td></tr>
</table>
</td>
<td><b>SY304: LCDR Joseph Hatfield</b></td>
<td><b>SY304: Spring CY2020</b></td>
<td><b>SY304: Spring CY2020</b></td>
</tr>
</table>

• **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.		**lessons. Students are asked to design an authentication GUI that humans can actually understand and consider the impact that user interfaces have on the security of networks.**			
	Implicit and explicit policies in systems	**Implicit and explicit policies are discussed throughout the SY304 course, specifically in the password periodicity discussion during the psychology of password management lesson. Implicit and explicit policies with regard to physical access is discussed as a primary topic in three lessons: tailgating and piggybacking, shoulder surfing, dumpster diving. During the lockpicking lab students are also asked to consider access control policies and the risks associated with ease of access.**			
	Policies that users control and hidden policies controlled by the system	**Controlled and hidden policies are discussed throughout SY304 but are not the sole subject of any particular lesson. Nevertheless, in six lessons controlled policies are discussed explicitly while policies that are hidden are discussed in three of these lessons. The "Tiger Team" pen-testing case study lesson includes a deep discussion of both user-controlled policies and hidden policies both in terms of the vulnerabilities found by the pen-testing team and in the**			

		improvements required to mitigate these vulnerabilities. Both controlled and hidden policies are also discussed as primary topics in the lesson on secure data deletion.			
	The role of social engineering and how it continues to be the primary attack vector	SY304 has this topic as its main focus and theme, with eight full lessons and three hands-on labs specifically dedicated to this topic. For the remaining lessons, this theme forms the background of the discussions. Specifically dedicated lessons include psychological explanations of social engineering and pretexting, the history and theory of social engineering, automated social engineering (ASE), reverse social engineering, all types of phishing (e.g. vishing, pharming, spearphishing, etc.), impersonation attacks and other in-person social attacks, tailgating and piggybacking, shoulder surfing, dumpster diving, and a number of other topics. The labs include a lockpicking lab, a phishing e-mail lab (using Kali Linux), a browser exploitation lab (using BeEF), and a credential harvesting lab (using Kali Linux).			
	How implementing security affects	SY304 includes five lessons that have as one of their primary topics how the implementation of security measures affects the user			

<table>
<tr><td></td><td><table><tr><td>the user experience.</td><td>experience. For example, during the psychology of password management lesson, students are asked to consider a shoulder-surfing resistant password scheme that is so complex that the user experience would be completely ruined. During the firewall lesson, students learn how draconian firewall restrictions so restrict data availability that humans will often simply turn off the firewall, thereby rendering their system less secure.</td></tr></table></td><td></td><td></td><td></td></tr>
<tr><th>O.16 Offensive Cyber Operations</th><th>Course # and Course Title</th><th>Instructor(s)</th><th>Date Last Taught</th><th>Date Last Updated</th></tr>
<tr><td>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:
• <b>Cyber attacks are restricted to military members of DoD, as restricted by international law. Authorities are derived from U.S. Code Title 10.</b>
• <b>Cyber kill chain</b>
• <b>Mission planning and execution process</b>
• <b>Define mission objectives and desired effects from the overall mission standpoint</b>
• <b>The different phases of cyber operations</b></td><td><b>SY401: Cyber Operations I
SY402: Cyber Operations II</b><table><tr><th><u>Topic</u></th><th><u>Assessment</u></th></tr><tr><td>Cyber attacks are restricted to military members of DoD, as restricted by international law. Authorities are derived from U.S. Code Title 10.</td><td>SY403 discusses the specific authorities granted to the DoD and spends two lessons distinguishing them from the authorities of intelligence agencies, federal agencies (especially DHS and DOJ/FBI) and the private sector. Four SY403 in-class exercises are devoted to exploring DoD authorities in various scenarios (two of these exercises require students to assume roles as the principals representing DHS, DOJ, DoD, and the IC in strategy</td></tr></table></td><td><b>SY401/402: Mr. Dennis Dias</b></td><td><b>SY401: Fall CY2019

SY402: Spring CY2020</b></td><td><b>SY401: Fall CY2019

SY402: Spring CY2020</b></td></tr>
</table>

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.		**deliberations at the National Security Council; other exercises are centered on tactical and strategic military levels). SY403 covers US national cyber strategy, DoD cyber strategy, relevant US law (e.g., NDAA19 which modified DoD cyber authorities), and JP3-12 (DoD guidance on cyber operations tactics and integration into traditional military campaigns) in detail.**			
	Cyber kill chain	**The Mitre attack framework is covered by SY403 in detail in a lesson devoted to Cyber operational tactics. SY403 guest speakers from NSA provide additional context to the operational context of both offensive and defensive cyber operations (Fall 2019 hosted two currently serving NSA subject matter experts). Defensive tactics are also covered in SY403, largely through the lens of the NIST framework.**			
	Mission planning and execution process	**SY401 discusses the phases as an outline for the semester schedule - labs and lecture re-enforce these steps (see course materials in GitHub)**			
	Define mission objectives and desired effects from the overall	**SY401 demonstrates this for host based attacks using open source tools in weekly labs. SY403 devotes one lesson each to US**			

	mission standpoint	military cyber tactics (centered on DoD JP3-12) and US military cyber strategy (centered on USCYBERCOM doctrine, DoD cyber strategy, and enabling law and US national security strategy)			
	The different phases of cyber operations	SY401 discusses the phases as an outline for the semester schedule - labs and lecture re-enforce these steps. SY403 covers cyber operations campaigns in both classroom lectures (separate lessons on tactical employment and overall strategy) and through exercises. The final course exercise is built around competition and conflict between the US and the PRC over events originating in contested waters of the South China Sea. in preparation for the SY403 final exercise, students must research and provide written recommendations bearing on US strategy and tactics for a state-to-state cyber engagement involving US military forces.			

O.17 Hardware Reverse Engineering	Course # and Course Title		Instructor(s)	Date Last Taught	Date Last Updated
Must include hands-on lab exercises. Hardware Reverse Engineering is the study of hardware hacking and reverse engineering approaches that are routinely used	<u>Topic</u>	<u>Assessment</u>	Click here to enter text.	Click here to enter text.	Click here to enter text.

<table>
<tr>
<td>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:<ul><li><b>Hardware reverse engineering methodology</b></li><li><b>The use of tools and test measurement equipment</b></li><li><b>Circuit board analysis and modification</b></li><li><b>Embedded security</b></li><li><b>Common hardware attack vectors</b></li></ul><b><i>Outcome</i>:</b> Students will understand basic fundamental procedures such as probing, measuring and data collection to identify functionality and to affect modifications to the hardware functionality.
<b><i>Outcome</i>:</b> Students will understand the proper use evaluation tools and common hardware attack vectors.</td>
<td><table>
<tr><td><b>Hardware reverse engineering methodology</b></td><td></td></tr>
<tr><td><b>The use of tools and test measurement equipment</b></td><td></td></tr>
<tr><td><b>Circuit board analysis and modification</b></td><td></td></tr>
<tr><td><b>Embedded security</b></td><td></td></tr>
<tr><td><b>Common hardware attack vectors</b></td><td></td></tr>
</table></td>
<td></td>
<td></td>
<td></td>
</tr>
</table>