**Principles of Cyber Law & Policy Syllabus**

**Course Developers/Creators:** This course was developed by **James W. Houck**, Vice Admiral, Judge Advocate General’s Corps, U.S. Navy (Ret.), Penn State Law and Penn State Center for Security Research and Education; **Anne Toomey McKenna**, Penn State Dickinson Law and Institute for CyberScience; and Dr. **Scott S. Gartner**, Penn State School of International Affairs. Biographies and contact information for Admiral Houck and Professors McKenna and Gartner are on the last page of this Syllabus.

**Prerequisites:** Upper division undergraduate, graduate, and professional students should have an understanding of the functioning roles of the three branches of U.S. Government and an awareness of basic U.S. Constitutional concepts. This course’s four Modules are designed to be taught in sequential order and build upon each other. However, as noted below in the Module Prerequisites section, specified Modules and Lessons may be taught as stand-alone content.

**Length of Completion:** This Syllabus is laid out as a 15-week semester with two 75-minute classes/week (2x per week) = 37.5 hours. Instructors may teach certain Modules and specific Lessons as stand-alone Modules and Lessons, and this Syllabus identifies what Modules and Lessons are standalone, what Modules link together for learning purposes, and what Modules require another Module as a prerequisite (see Module Prerequisites and Learning Outcomes section below). The Course Developers assume that your faculty and instructors will modify this Syllabus to meet their own content needs and schedules as well as to keep abreast of changes in law that occur after this Course was created (July 2018).

**Level of Instruction:** Upper division undergraduate / graduate / professional.

**Learning Setting:** In-class / face-to-face instruction.

***Course Description***

Cyber activities and cyber operations are subject to a diverse array of U.S. federal laws, state laws, constitutional law, and regulatory policies, as well as international laws that together comprise a framework of law called *Cyberlaw*. Individuals, businesses, and governments involved in any aspect of cyber operations (“cyber actors”) must have a clear understanding of cyber technology platforms (cyberspace) and the legal and policy background (cyberlaw) to ensure that cyber activities and operations (“cyber actions”) are conducted within, but not beyond, the maximum limits of legal authority.

Students from all educational disciplines and professional backgrounds will learn fundamental concepts designed to help ensure that the cyber operations in which they participate are consistent with the laws and values of the society they serve.

Please note that laws, policies and organizations can change at any time and that the course is up-to-date as of July 2018.

***Module Prerequisites and Learning Outcomes***

**MODULE I. Overview of Cyberspace and Its Intersection with Law and Policy**

**Prerequisites:** Module I is the introductory Module and may be taught as a standalone module independent of other Modules. Module I’s Lesson 4 may be taught as a standalone lesson.

**Learning Outcomes:** Upon completion of this Module, students will understand:

* What the term “cyberspace” means by learning the functional and technical workings of cyber systems, i.e., modern communication (Internet, cellular, GPS), business, government, and security platforms
* How cyber systems and operations function by reviewing internet technology, and electronic device and data advances, such as Internet of Things, Autonomous Vehicles, Sensor Technologies (environmental, biometric, wearable, smart devices), GPS Tracking, Biometrics, Thermal Imaging, Big Data concepts, Predictive Analytics, and the proliferation of Unmanned Aerial Vehicles (UAVs)
* How data and information is created, collected, aggregated, bought, sold, manipulated, and hacked (Cyber Actions) by private and state actors across cyber platforms
* The distinction between Private Actors and State Actors in Cyberspace

**MODULE II. Cyber Governance: Three Branches of Government**

**Prerequisites:** Module II is the second Module in a course designed primarily as a Four Module Course. Module II, however, also may function as a standalone Module for instructors wishing to teach basic U.S. government structure, the structure of U.S. court systems, constitutional concepts of jurisdiction – including in cyberspace, and U.S. federal agencies actively involved in cyber investigations, operations and policy.

The Introductory Lesson in Module 1 (*Learning How to Learn Law*) is highly recommended before this Module.

Module II’s Lessons 6 and 12 each may be taught as standalone lessons. Lessons 7-8 may be taught together as a two-lesson, standalone content course; the same is likewise for Lessons 9-10. Lesson 11, however, requires Module II’s Lessons 3-10 as prerequisites because the content is Lesson 11 is based upon and assumes knowledge of this prior lessons.

**Learning Outcomes:** Upon completion of this Module, students will understand:

* The roles of the Congress, President, U.S. Courts, and U.S. State governments in formulating cyber policy and cyberlaw, and executing cyber operations that address the conduct of Private and State Actors engaging in Cyber Actions
* The structure, function, and jurisdictional authority of U.S. federal and state court systems
* The concept of subject jurisdiction and personal jurisdiction and how jurisdictional authority functions in cyber operations
* The structure and roles of pertinent U.S. federal and U.S. state agencies who investigate and defend against cyber threats, engage in cyber operations, and prosecute cyber actors engaged in actions that constitute cybercrimes as well as the relation between U.S. federal and state agencies
* The import of *Presidential Policy Directive on United States Cyber Incident Coordination – 41* (PPD 41)
* The federal government’s threat response framework
* How agencies handle foreign private and public attacks
* Federal Offensive Cyber Operations
* What a “Cyber Threat Indicator” (CTI) is under the Cybersecurity Information Sharing Act of 2015 (CISA); what constitutes a Defensive Measure (DM) under CISA, and other CISA statutory definitions
* How Automated Indicator Sharing (AIS) functions and other means of sharing Classified and Non-Classified CTIs and DMs across all levels of government and between government and private sector
* The relationship between federal and state governments as well as federal and private actors in cyber threat responses

**MODULE III. Legal Foundations of Modern Cyber Law & Policy**

**Prerequisites:** Module III is the third Module in a course designed primarily as a Four Module Course. Module III, however, also may function as a standalone Module for instructors wishing to teach the historical evolution of privacy as a right in the U.S., U.S. Constitutional concepts of privacy, Fourth Amendment doctrines, warrants, First Amendment speech concepts, and the Fifth, Sixth, and Fourteenth Amendments and the potential applicability of all of these amendments to cyber operations. In addition, this Module reviews U.S. federal and state statutes that form part of the framework of modern cyberlaw as well as international law and common law concepts that impact cyber operations.

The Introductory Lesson in Module 1 (*Learning How to Learn Law*) is highly recommended before this Module if this Module is taught by itself.

Module III’s Lessons 13 and 21 each may be taught as standalone content.

**Learning Outcomes:** Upon completion of this Module, students will understand:

* The historical evolution of the right to privacy in U.S. Law
* How the U.S. Constitution regulates government actors versus private actors
* The U.S. Constitution and the Fourth Amendment (search and seizure), including the concepts of a reasonable expectation of privacy and the third party doctrine, and warrants
* The U.S Constitution and the First Amendment (freedom of speech and association) including anonymous speech and unmasking the identity of anonymous online speakers, and speech content/time/place/manner restrictions
* The U.S. Constitution’s Fifth, Sixth and Fourteenth Amendments and how these amendments may impact cyber operations
* The Constitutional requirement of “standing" to bring lawsuits
* The framework of existing federal and state statutes and regulatory laws that function as part of the framework of domestic U.S. federal and state cyberlaw
* How courts apply the U.S. Constitution to government electronic surveillance and cyber operations
* U.S. Common Law (invasion of privacy, contracts, copyright, electronic evidence) and how it applies in cyberspace
* Understanding international law and its role in cyber operations

**MODULE IV. Cyber Operations**

**Prerequisites:** Module IV is the fourth Module in a course designed primarily as a Four Module Course. Module IV is not intended to be taught as a standalone module. Its required prerequisites are Modules II and III.

If only teaching Modules II and III as a prerequisite to Module IV, the Introductory Lesson in Module 1 (*Learning How to Learn Law*) is highly recommended before this Module.

\*It is critical that Module I’s Lesson 6 be taught prior to teaching Module IV’s Lesson 24 as it contains material that assumes knowledge of material taught in Module I’s Lesson 6.

\*It is critical that Module III’s Lesson 21 be taught prior to teaching Module IV’s Lessons 25-29 as those lessons contain material that assumes knowledge of material taught in Module III’s Lesson 21.

**Learning Outcomes:** Upon completion of this Module, students will understand:

* The current threat-response framework for cyber operations, including investigation of CTIs and the Cyber Action, use of DMs to counteract CTIs, identification of the Cyber Actor, and permissible offensive operations
* Legal distinctions in the threat-response framework as applied to Cyber Actions conducted by Private Actors and State Actors
* What the law permits with respect to cyber operations involving Private Actors
* How the Congress and President share responsibility for national security operations and how these responsibilities are embodied in the War Powers Resolution and covert action statutes
* The international law governing a nation-state’s conduct of cyber operations against other nation-states and non-state actors

***Outcomes***

***Suggested Materials and Grading***

**Suggested Books and Materials:**

1. Geoffrey Corn et al., *National Security Law: Principles and Policy* (2015).
2. P.W. Singer & Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (2014).
3. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Michael N. Schmitt & Liis Vihul, eds., 2d ed. 2017).
4. Lisa J. Sotto, *Privacy and Cybersecurity Law Deskbook*, 2018 Ed., Wolters Kluwer (2018).
5. Clifford S. Fishman & Anne T. McKenna, *Wiretapping & Eavesdropping: Surveillance in the Internet Age, 3rd Ed.*, Thomson Reuters (2007-).
6. References to specific Law Review Articles, which are available via open public access online, as well as academic treatises, all of which are available on Westlaw for educators and students at accredited institutions, are incorporated throughout the lesson content. The Course Developers expect faculty and students to access the referenced materials in accordance with copyright laws.

**Grading:**

Every Lesson contained within the Modules I-IV includes Assessment Slides with questions followed by slides with the answers. These Assessment Slides may be used as quizzes. For grading purposes, more complete and comprehensive examination and testing may be drawn from the included Assessment questions if an instructor so chooses. Given the nature of the Course (with certain Modules and Lessons able to be taught as standalone content), the Course Developers have purposely left grading structure open to the determination of the individual faculty or instructor based upon how the instructor is using the content.

***Module and Lesson Contents; Course Schedule***

|  |  |
| --- | --- |
| **Week** | **Lesson Number and Title** |
| **MODULE I. OVERVIEW OF CYBERSPACE AND ITS INTERSECTION WITH LAW AND POLICY** | |
| **1** | * **Introduction to Legal Learning:** Learning How to Learn Law * **Lesson 1:** Course Overview | Understanding Technology and “Cyberspace” * **Lesson 2:** Understanding Cyber Systems and Operations | Cyberspace and Internet Technology Advances (Internet of Things, Autonomous Vehicles, Sensors, GPS, Big Data, Predictive Analysis) |
| **2** | * **Lesson 3:** Cellular Technology and Cellular Tracking | Enhanced Visual Surveillance and Other Cyber Tracking (Biometrics) * **Lesson 4:** Unmanned Aerial Vehicles (Drones); Autonomous Vehicles |
| **3** | * **Lesson 5:** Understanding Data and Information Sharing across Cyber Platforms |
| **MODULE II. CYBER GOVERNANCE IN THE U.S.** | |
| **3** | * **Lesson 6:** Cyber Governance: Three Branches of Government – President, Congress |
| **4** | * **Lesson 7:** Cyber Governance: Three Branches of Government Continued - Courts * **Lesson 8:** Cyber Governance: Three Branches of Government - Courts; Cyberspace and Jurisdiction; Foreign Intelligence Surveillance Courts |
| **5** | * **Lesson 9:** Cyber Governance: Federal Agencies Overseeing Cyber Operations * **Lesson 10:** Presidential Policy Directive – 41; Cyber Governance: Federal Agencies Threat Response Framework; U.S. Offensive Cyber Operations |
| **6** | * **Lesson 11:** Cyber Governance: Federal and State Roles in Cyber Crime Investigation and Prosecution * **Lesson 12:** Cyber Governance: Cybersecurity Information Sharing Act of 2015 (CISA) |
| **MODULE III. LEGAL FOUNDATIONS OF MODERN CYBER LAW & POLICY** | |
| **7** | * **Lesson 13:** U.S. Constitution: the Right to Privacy & Fourth Amendment * **Lesson 14:** U.S. Constitution: First Amendment: Speech Protections, Anonymity & Surveillance |
| **8** | * **Lesson 15:** U.S. Constitution: Fifth, Sixth and Fourteenth Amendments * **Lesson 16:** U.S. Statutory Framework of Law |
| **9** | * **Lesson 17:** U.S. Statutory Framework of Law * **Lesson 18:** U.S. State Cyberlaw Legislation |
| **10** | * **Lesson 19:** U.S. Common Law as a Source of Cyberlaw: Torts, Contracts, Evidence * **Lesson 20:** U.S. Regulatory Agencies |
| **11** | * **Lesson 21:** The Role of International Law in Cyber Operations |
| **MODULE IV. CYBER OPERATIONS** | |
| **11** | * **Lesson 22:** The Cyber Threat-Response Framework: An Overview |
| **12** | * **Lesson 23:** Cyber Operations By and Against Private Actors * **Lesson 24:** Shared Responsibility for Cyber Governance |
| **13** | * **Lesson 25:** The International Right To Conduct Cyber Operations Against International Actors (1) * **Lesson 26:** The International Right to Conduct Cyber Operations Against International Actors (2) |
| 14 | * **Lesson 27:** Rules for Conducting Cyber Operations Against State Actors (1) * **Lesson 28:** Rules for Conducting Cyber Operations Against State Actors (2) |
| 15 | * **Lesson 29:** Rules for Conducting Cyber Operations Against Non-State Actors * **Lesson 30:** Course Review |

***Course Developers: Biographies***

**James W. Houck**

James W. Houck, Vice Admiral, Judge Advocate General’s Corps, U.S. Navy (Ret.), is a Distinguished Scholar in Residence at Penn State Law and the School of International Affairs and the inaugural director of the Center for Security Research and Education at Penn State. He joined Penn State in 2012 after a 32-year career in the United States Navy, beginning as a qualified destroyer officer of the deck and culminating in appointment as the 41st Judge Advocate General of the U.S. Navy. From 2013-2017, he served as the interim dean of the unified Dickinson School of Law and the School of International Affairs, as well as interim dean of Penn State Law in University Park for the school’s first two years. As a member of the Penn State Law and School of International Affairs faculty, he focuses on national security law, international law, law of the sea, law of armed conflict, and legal issues within the military.

As the Judge Advocate General of the Navy, Admiral Houck was the principal military legal counsel to the Secretary of the Navy and Chief of Naval Operations and led the 2,300 attorneys, enlisted legal staff, and civilian employees of the worldwide Navy Judge Advocate General’s Corps. As the Judge Advocate General, he led creation of the Navy JAG Corp’s first cyber division.  He also served as the Department of Defense Representative for Ocean Policy Affairs and oversaw the Department of the Navy's military justice system. Among his assignments as a Navy lawyer, Admiral Houck served as deputy legal counsel to the Chairman of the Joint Chiefs of Staff, and as principal legal counsel to the Commander, U.S. Atlantic Fleet, and the Commander, U.S. Naval Forces Central Command in Bahrain. Admiral Houck served in the Navy’s Office of Legislative Affairs and was also a Navy prosecutor and defense attorney. Admiral Houck is a member of the Council on Foreign Relations and has previously served as a member of the Hoover Institute's Arctic Security Initiative.

Admiral Houck can be reached at [jwh32@psu.edu](mailto:jwh32@psu.edu).

**Anne Toomey McKenna**

Anne Toomey McKenna is Distinguished Scholar of Cyber Law & Policy with Penn State’s Dickinson Law and Institute for CyberScience. Professor McKenna teaches Information Privacy Law, Cyberlaw, Civil Procedure, Evidence, and Media Law. She is an attorney with more than 24 years of federal and state court litigation and practice experience in cyber, privacy, electronic surveillance and cellular law. Professor McKenna has co-authored two treatises, *Wiretapping & Eavesdropping: Surveillance in the Internet Age, 3rd Ed*., and *Jones on Evidence, 7th Ed*., both of which are widely cited by federal and state courts. Professor McKenna is currently writing a new casebook, *Cyberlaw in Practice*, under contract for publication in 2019 with Wolters Kluwer.

Professor McKenna is routinely cited and quoted by media, including NPR’s *Morning Edition*, *The Washington Post*, *The Baltimore Sun*, *The Boston Globe*, VICE News, Bloomberg Radio, The Intercept, FOX News and CBS News, among others. Prior to her fulltime faculty appointment in 2016, Professor McKenna was a partner in a large mid-Atlantic law firm where she represented large and small businesses, educational clients, and individuals in matters involving workplace privacy and surveillance, computer hacking, data practices, data breach, online privacy policies and terms of use, cellular practices, geolocation tracking, online content and speech, online torts, electronic surveillance, and privacy. She served as the Principal Legal Consultant for the Department of Justice’s COPS division on the use of UAVs by domestic law enforcement. She continues to consult with government officials about wiretapping, computer and cellular searches, geolocation tracking, and unmanned aerial vehicles (UAVs).

Professor McKenna can be reached at [atm19@psu.edu](mailto:atm19@psu.edu).

**Scott Sigmund Gartner**

Dr. Scott Sigmund Gartner is Professor of International Affairs and Director of the Penn State School of International Affairs. Professor Gartner’s research focuses on national security and dispute mediation. Prior to joining Penn State he was Professor of Political Science and Director of the International Relations Program at the University of California Davis. He has an AB (History) and AM (International Relations) from the University of Chicago and a MA and PhD from the University of Michigan (Political Science).

Professor Gartner's publications include *Strategic Assessment in War*, *International Conflict Mediation: New Approaches and Findings* and *The Historical Statistics of the United State*s, in addition to articles in top journals in political science, sociology, international affairs, history, military intelligence, public policy, law, and communications.  He received the Jefferson award for the Best Government Resource, the RUSA Outstanding Reference Award, Booklist Editor's Choice Award, Library Journal Best Reference Award and the American Political Science Association's best policy thesis award.

Gartner’s op-eds include *The Huffington Post*, *USA Today*, and *The Christian Science Monitor*, and he and his research have appeared in *The Washington Post, Wired, USA Today, Newsweek, The Atlantic*, The History Network, MSNBC, NPR, and ABC.

Professor Gartner can be reached at [ssg13@psu.edu](mailto:ssg13@psu.edu).