SY406: Cyber Law and Ethics

Instructors: Assistant Professor Jeff Kosseff (1201, 3401, 5601) and Capt. Evan Field (5602)

Course Description: This course examines many of the legal and ethical challenges that cyber operations professionals confront in the public and private sectors. The course begins with an in-depth review of the provisions of the United States Constitution that shape the cyber operations of the military and civilian government agencies. The course then reviews the statutes and regulations that provide the government with the authority to conduct cyber operations, as well as the limits that the statutes impose. The course examines the interplay between public-sector and private sector cybersecurity efforts, and the state and federal laws that regulate private-sector cybersecurity. We also explore the ethical considerations that apply to cyber operations.

Learning Objectives: The goal of this class is to help you understand the legal, ethical, security, and social issues surrounding cyber operations, as well as the global impact of computing and cyber operations on society.

Although this is a law class, this is not intended to train you to be a lawyer. This class, instead, is intended to help you identify, understand, apply, and analyze the legal issues that you will confront as a cyber operations professional in the military, civilian government, or private sector. Although you likely will be working with lawyers, it is essential that you understand the legal foundations -- and limitations -- of cybersecurity.

This class also is designed to provide you, future Naval Officers, with the critical thinking skills to assess whether the current laws are accomplishing their goals, and how policymakers could improve existing cybersecurity law. Throughout this class, I want you to think about not only what the law is, but what it should be.

In particular, you should understand and be able to apply the following concepts:

- Constitutional foundations of government cyber operations
- Constitutional civil liberties that impact military, intelligence, and civilian agency cyber operations
- Federal statutes that limit government cyber operations
- The structure of U.S. government cyber operations
- The laws of war that impact cyber operations
- Public-private cybersecurity partnerships
- Cybersecurity law for the private sector
- Ethical issues that arise with cyber operations

The class assignments are intended to prepare you to communicate your analysis of cyber legal issues in writing and via oral presentations. By the end of this semester, you will have delivered three in-class presentations, participated in a mock appellate argument, written a substantial term paper, and taken two law school-style exams.

Grading

Six-Week exam: 25%

Term Paper: 30%

Final exam: 30%

Current Events and Term Paper Presentations: 5%

Participation and appellate arguments: 10%

Exams

You will have in-class exams at the six-week and semester-end periods.

The exams probably will be unlike any other that you have taken before. For each exam, you will be presented with one or more lengthy hypothetical fact patterns, and in your answers, you will apply the legal rules and principles that we learned in class. Grades will be based on: (1) identification and accurate statement of the key legal issues; (2) quality of analysis; and (3) clarity of writing. These exams are similar to the exams given in law school, and they require you to think critically about the legal rules rather than merely memorize and recite the law. I will post past exams and model answers on Blackboard so that you can get a better understanding of the format.

Please bring your laptops to each exam, as you will type your answers using Blackboard and the Respondus LockDown Browser. If you have not yet downloaded Respondus, please do so **before** the first exam. It is available at http://www.respondus.com/lockdown/download.php?id=487946356

The exams will be closed-book with one important exception: for each exam, you are permitted to bring **one** 8 ½" x 11" sheet of paper. You may write or type whatever you would like on both sides of the paper, and you may only use that sheet of paper. You may not use any other notes, readings, or other materials during the exams. Both exams will be cumulative, and count for a combined 55 percent of your final grade.

Term Paper

You will write a term paper this semester (10-12 pages, double-spaced, Times New Roman). The paper will require you to analyze and research a court opinion related to the issues that we study this semester, assess the implications of the court's decision, argue whether the court was correct in reaching its decision, and consider whether the legal rules that the court decided should change to improve cybersecurity. During the first week of classes, I will separately distribute a more complete paper assignment. Email me your proposed paper topic no later than **Jan. 28.**

Term papers will be due to me in class on **March 26**. On March 26, March 28, and April 2, each student will deliver a 10-minute in-class presentation on the paper. The paper and the presentation each will count toward your final grade.

Current Events Presentations

Each student will deliver one 10-minute class presentation/discussion about current events during the semester. The schedule will be distributed the first week of class. The presentation will be based on a cybersecurity law or policy topic that is in the news. You may choose the topic, and email to me a brief (few sentence) description of the topic **no later than 24 hours** before your scheduled presentation. You should summarize the topic, provide your opinions, and lead a brief class discussion on the issue. To stay on top of the latest cybersecurity legal news, I recommend that you subscribe to the free Politico Morning Cybersecurity Update, at http://www.politico.com/cybersecurity.

Please make note of your assigned presentation date, as I will not remind you of the date in advance.

The grades for your presentations will be based on (1) accuracy of your presentation; (2) ability to lead class discussion; and (3) response to questions from classmates and professor.

Participation

I expect you to read all of the required materials and be prepared to discuss them in class. Voluntary class participation is expected, and the quantity and quality of your participation will be the basis of your participation grade. Although I do not prefer the Socratic method, I will randomly call on students if there is not sufficient voluntary participation.

Throughout the class, we will have in-class exercises, including mock appellate arguments. These exercises will be based on the course readings, and will be factored in to your participation grade. You will receive a schedule for the mock appellate arguments during the first week of class.

We periodically will have guest speakers. I expect all of you to take advantage of these opportunities and come to class prepared with questions.

Course Materials

Your textbooks are *Tallinn Manual 2.0* and *Cybersecurity Law* (Second Edition) by Jeff Kosseff (Wiley). Please only buy the books via the USNA Bookstore.

The remainder of the readings will be posted on Blackboard, in a folder for each class date. Due to the constantly evolving nature of cybersecurity law, I may add or remove readings as necessary, and I will notify you of any changes.

I have made every effort to distill the readings so that you have a manageable workload. However, given the complex nature of legal and ethical issues, there likely will be more reading for this class than some other cyber classes. To help you prioritize, I have marked some readings "recommended." These readings still will be helpful for you to understand the materials, and I encourage you to read them in addition to the other materials.

For most of the substantive classes, I will use PowerPoint slides to highlight many of the important points. The slides will be available on Blackboard after the class.

Although I expect you to be prepared to answer questions about any of the topics in our class discussions or required readings, the take-aways are a good indicator of what you should be focusing on as you review your materials.

Class Policies

1. Extra Instruction and Email: We are covering a lot of material in this class, and some of it is quite complex. Accordingly, I strongly encourage you to schedule Extra Instruction with me if you have any questions about the material. Alternatively, you may email me questions about the material, and I will respond promptly.

2. Grading Scale: A: 90-100%; B: 80-89%; C: 70-79%; D: 60-69%; F: 0-59%. I round up by a half point, so for example, if you receive an 89.5-89.99, I will round your grade to an A. I will **not** round up by more than a half-point.

3. Deadlines: Unless you receive **prior** approval from me, no work will be accepted after the stated deadline. If class is canceled or delayed due to inclement weather or another event, I will email the class with an update about how the schedule change affects deadlines or submission procedures. Unless you receive an email from me, assume the stated deadline continues to apply.

4. Academic Integrity: We have a zero-tolerance policy for plagiarism. All work must be your own. For more information about the Naval Academy's policy on plagiarism, visit http://libguides.usna.edu/plagiarism. Under **no circumstances** may you discuss your exams with anyone else (including but not limited to classmates, faculty, and staff) until **after** you have received your grade on the exam.

5. Conduct: We will be studying some cutting-edge legal issues that do not have resolved outcomes. Among policymakers, there is not a clear consensus on many of these topics. I expect (and hope) that we will have a similarly spirited debate in class. I expect that all midshipmen will respect their classmates' points of view.

Class Schedule

I. Constitutional Foundations of Cyber Operations

January 9

Introduction to Class; Introduction to Legal Reasoning; Cybersecurity Law Fundamentals

- Orin Kerr, How to Read a Legal Opinion

January 14

Executive Power, Separation of Powers, and Judicial Review

- Marbury v. Madison overview
- David Opderbeck, *Cybersecurity and Executive Power*, Washington University Law Review (pages 812-829, skim the rest)
- Youngtown Sheet & Tube v. Sawyer
- Section 706 of the Communications Act of 1934

January 16

Fourth Amendment Principles

- Kosseff, pages 291-311, 663-682
- Barry Friedman and Orin Kerr, The Fourth Amendment

Recommended:

- Russell Galloway Jr., Basic Fourth Amendment Analysis, Santa Clara Law Review

January 22

Fourth Amendment in Cyber, Fifth Amendment and Encryption

- Kosseff, pages 336-342, 682-714
- Jack Goldsmith, The Cyberthreat, Government Network Operations, and the Fourth Amendment
- Carpenter v. United States (2018) (majority opinion only, skim the rest)
- United States v. Keith (D. Mass. 2013)

Recommended:

- Thomas K. Clancy, The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer, Mississippi Law Journal
- U.S. Justice Department, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations
- Einstein summary, http://www.dhs.gov/Einstein

January 23
First Amendment; Other Constitutional Issues in Cyber

First In-Class Appellate Argument, US v. Apple MacPro Computer

- Reno v. ACLU (1997)
- Rodney Smolla, Speech Overview
- David Fidler, Countering Islamic State Exploitation of the Internet, Council on Foreign Relations
- Javier Lesaca, Fight Against ISIS Reveals Power of Social Media, Brookings
- The ISIS Twitter Census (Executive Summary Only)
- Michael Smith, The Third Amendment and Cybersecurity: Quirky but Mistaken

II. Laws Affecting Military and Civilian Government Cyber Operations

January 28

Platforms, Moderation, and Section 230

- Kosseff, Twenty Years of Intermediary Immunity
- Jones v. Dirty World Entertainment (6th Cir. 2014)

January 30

Stored Communications Act, Pen Register Act, Wiretap Act, Metadata

- Kosseff, Chapter pages 311-335
- Orin Kerr, A User's Guide to the Stored Communications Act -- And a Legislator's Guide to Amending It, George Washington University Law Review
- Daniel Monnat & Anne Ethen, A Primer on the Federal Wiretap Act and its Fourth Amendment Framework
- Ben Kerschberg, Can the Government Seize Your Email Without a Warrant?, Forbes

February 4

Title 10 and TItle 50 Authorities for Cyber Operations

- Kosseff, pages 269-289
- American Security Project, Fact Sheet, U.S.C Title 10, Title 22, and Title 50.
- Andru E. Wall, Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities, & Covert Action, Harvard National Security Law Journal

February 6

Catch-up and review

February 11

Six-week exam

III. Structure of U.S. Government Cyber Operations

February 13

Guest Speakers from U.S. Cyber Command

February 18

Foreign Intelligence Surveillance Act; Executive Order 12333, *Cyber Command and DOD Cyber Operations; NSA; Zero-Day Vulnerabilities*

- Chris Inglis and Jeff Kosseff, In Defense of FAA Section 702: An Examination of its Justification, Operational Employment, and Legal Underpinnings (Hoover Institution 2016)
- John N. Greer, Square Legal Pegs in Round Cyber Holes: The NSA, Lawfulness, and the Protection of Privacy Rights and Civil Liberties in Cyberspace
- Alexander Joel, The Truth About Executive Order 12333
- Charlie Savage, Reagan-Era Order on Surveillance Violates Rights, Says Departing Aide
- NSA Chief Privacy and Civil Liberties Officer, NSA's Implementation of FISA Section 702

February 20

Department of Homeland Security, FISMA; Ethics of Government Cybersecurity Efforts

Second In-Class Appellate Argument (United States v. Hasbajrami)

- Kosseff, pages 269-289
- Catherine Karia, FISMA Updated and Modernized
- Jeh Johnson, *Federal Cybersecurity Needs Improvement*
- Sean Gallagher, Why the 'Biggest Government Hack Ever' Got Past the Feds
- Aaron Boyd, Could OPM Have Prevented the Breach?
- Sean Lyngaas, *Security Experts: OPM Breach Shows Einstein Isn't Enough*

IV. **Private Sector Cyber Operations**

February 25

FTC Oversight of Data Security

- Kosseff, pages 1-42
- FTC v. Wyndham (3d Cir. 2015)
- LabMD v. FTC (11th Cir. 2016)
- Rita Heimes - LabMD article

February 27

Data Breach Litigation/Attorney-Client Privilege

- Kosseff, pages 57-104
- Douglas Meal, Privacy and Data Security Breach Litigation in the United States
- Krottner v. Starbucks (9th Cir. 2010)
- Reilly v. Ceridian (3d Cir. 2011)

March 3

Computer Fraud and Abuse Act

- Kosseff, pages 171-217, 633-663
- David Bitkower, Hacking into the Computer Fraud and Abuse Act
- Congressional Research Service, Overview of the Computer Fraud and Abuse Act
- The Hill, Judges Struggle with Cybercrime Punishment
- Andrea Peterson, The Law Used to Prosecute Aaron Swartz Remains Unchanged After His Death
- Orin Kerr and Stewart Baker, *The Hackback Debate*

March 5

Computer Fraud and Abuse Act II; Intellectual Property/Digital Millennium Copyright Act, *Economic Espionage Act*

Third In-Class Appellate Argument (Linkedin v. NetIQ)

- Kosseff, pages 220-267
- Stoel Rives, The Anti-Circumvention Rules of the DMCA
- MDY v. Blizzard Entertainment (9th Cir. 2010)
- Chamberlin v. Skylink (Fed. Cir. 2004)

SPRING BREAK

March 17

Guest Speaker: Virginia Seitz, former Assistant Attorney General, U.S. Justice Department Office of Legal Counsel

March 19

Data Breach Notification Laws; Securities and Exchange Commission rules; *State Data Security Laws, Security of Sensitive Information; Securing Critical Infrastructure*

- Kosseff, pages 42-56, 155-170
- Jeff Kosseff, Notified About a Data Breach? Too Late, Wall Street Journal,
- Marc Krotoski, et. al., Need to Repair Data Breach Notification Maze
- SEC Cybersecurity Disclosure Guidance No. 2 (2011)
- Congressional Research Service, Critical Infrastructures: Background, Policy, and Implementation

March 24

Espionage Act; U.S. Privacy Law

- Kosseff, pages 361-384
- Chase Madar, The Trials of Bradley Manning
- Charlie Savage, In Closing Argument, Prosecutor Casts Soldier as 'Anarchist' for Leaking Archives

March 26
Term Paper Presentations

March 31
Term Paper Presentations

April 2

Term Paper Presentations

April 7

Posse Comitatus and Cyber; Introduction to Law of Cyber War

Fourth In-Class Appellate Argument (Beck v. McDonald)

- Kosseff, pages 413-424
- U.S. v. Dreyer (9th Cir. 2014)
- International Hacker Arraigned After Extradition
- Josephine Wolf, NATO's Empty Cybersecurity Gesture
- Siobhan Gorman, Cyber Combat: Act of War

April 9

Cyber Sovereignty, Jurisdiction, Non-Intervention, Countermeasures

- Council of Europe Convention on Cybercrime (articles 2-8, 11, 13, 15, 22-26, 35)
- Tallinn Manual, pp 11-78

April 14

Jus ad Bellum, Tallinn Manual pp 328-372, 401-504

April 16

Jus in Bello, and Cyber (When to go to war?)

April 21

Introduction to Cyber Ethics

- *Readings TBD*

April 23

Existing Cyber-Ethics Codes; In-class ethics exercise

- Tallinn Conference Cyber Ethics Papers
- ISC2 Code of Ethics

April 28

Wrap-Up and Review