Cybersecurity Law for Undergraduates

By Jeff Kosseff[1]

Abstract: Undergraduate cybersecurity programs can – and should – educate students about cybersecurity law. This Paper outlines the U.S. Naval Academy's approach to the cybersecurity law class that is required for undergraduate cyber operations majors. Although the students have no previous legal education, they grasp many of the complex laws relevant to cybersecurity professionals. A successful undergraduate cybersecurity law class provides a foundational overview of legal concepts, integrates current events, evaluates students' written and oral communication skills, and requires students to think critically about legal issues.

In 2016, the United States Naval Academy graduated its first class of cyber operations majors – 27 midshipmen out of about 1,100 graduates. Two years later, the ABET-accredited program has quadrupled in size, with 110 freshmen choosing the major.

The Naval Academy requires all cyber operations majors to complete a cybersecurity law class, usually in their final semester. I joined the Naval Academy faculty in fall 2015, and I spent much of that semester designing the new class. I spoke to cybersecurity lawyers and operational professionals in the military, civilian government, private sector, and civil liberties groups. Most of the experts agreed on a core set of topics that they would like to see in an undergraduate cybersecurity law class.

I filled a whiteboard with more than 100 possible topics, but I did not yet have a structure for the class. I faced two primary challenges. First, I needed to whittle down the list to a manageable set of topics for a semester-long course. Second, the Naval Academy is an undergraduate institution. Law school students typically can take cybersecurity law as an elective in their second or third years, after completing the required first-year classes on contracts, criminal law, torts, property, and civil procedure. Undergraduate students, in contrast, have not received that foundational legal education before enrolling in cybersecurity law.

[1] Assistant Professor, Cyber Science Department, United States Naval Academy. The views in this article are only those of the author, and do not represent the U.S. Naval Academy, Department of Navy, or Department of Defense.

I attempted to structure the class in a logical format that tells the story of what we generally conceive of as cybersecurity law, moving from broad constitutional contours to more specific laws, and concluding with international cybersecurity norms. The class is broken into five general units, each consisting of approximately three weeks of classes:

- **Constitutional Foundations of Cybersecurity Law:** Executive power; legislative power; judicial review, and constitutional liberties (First, Fourth, Fifth, Tenth, and Fourteenth Amendments).
- **Statutory Foundations of Cybersecurity Law:** Statutory authorities for government cyber operations (with a focus on Titles 6, 10, 18, 32, and 50 of the United States Code); statutory limits on government cyber operations and surveillance (Electronic Communications Privacy Act and Posse Comitatus Act); foreign intelligence surveillance (FISA, Executive Order 12333, and PATRIOT Act); and division of governmental responsibilities for U.S. cybersecurity among federal and state agencies.
- **Private Sector Cybersecurity Law:** Federal Trade Commission data security actions; sectoral data security laws; state data security and breach notification laws; data breach litigation; attorney-client privilege for cyber forensics investigations; cyber-threat information sharing; encryption and the All Writs Act; privacy law; and General Data Protection Regulation.
- **Computer Crime and Hacking Laws:** Computer Fraud and Abuse Act; state computer crime laws; Section 1201 of the Digital Millennium Copyright Act; and Economic Espionage Act.
- **International Cybersecurity Law:** Law of war in cyberspace (jus ad bellum, jus in bello, cyber sovereignty, and jurisdiction); Budapest Convention.

Because Naval Academy students have not received a first-year law school education, each section begins with a general overview of the foundational concepts that underlie the legal issues. For instance, the Constitutional Law section begins with a brief history of judicial power dating back to *Marbury v. Madison*, and the Private Sector Cybersecurity Law section includes an overview of the stages of civil litigation.

Law school classes typically evaluate student performance almost entirely based on final-exam performance. The final exam usually requires a student to identify and analyze issues in lengthy hypothetical fact patterns. This allows the professor to evaluate a student's ability to spot legal issues, identify applicable legal rules, and analyze how those rules apply to the facts in the hypothetical. The law-school grading model does not work well for the Naval Academy, which requires grades at the six-week, 12-week, and final exam period. Nor does the model adequately evaluate other skills that we hope to teach our cyber operations majors, including presentation delivery and expository writing. Accordingly, each student is evaluated based on the following assignments:

- A hypothetical issue spotter mid-term exam
- A term paper on a current cybersecurity law issue of the student's choice, and a class presentation about the topic
- An in-class appellate argument in which students argue for and against the reversal of a district court cybersecurity-related opinion, with practicing lawyers and faculty as judges
- A final exam with 2-3 hypothetical issue spotter fact patterns
- Two in-class presentations about current events in cybersecurity law
- Class participation

I have taught nine sections of the class since Spring 2016, and have honed the material each semester to ensure it is current. Based on this experience, I conclude with the following lessons:

- Undergraduates are far more capable of learning complex cybersecurity law concepts than I had expected. This is partly because most of the students are seniors who have taken a number of challenging technical cybersecurity classes; thus, they can understand some material more easily than technological novices. For instance, when I teach the encryption dispute between Apple and the FBI, the students already are familiar with the mechanics of encryption, allowing us to focus on legal concepts such as the All Writs Act.
- Cybersecurity law is rapidly evolving, requiring constant evaluation of course topics for currency. For instance, after courts issued many Fifth Amendment opinions regarding compelled unlocking of smartphones, I added a section about the topic. Many legal issues, such as the Fourth Amendment and the Computer Fraud and Abuse Act, always will be relevant to cybersecurity law. Current event presentations help to ensure that students critically analyze new developments in cybersecurity law.

- Undergraduate cybersecurity law classes should not aim to prepare students to perform the work of lawyers; indeed, unless the graduate has a juris doctor and active bar admission, such work would be illegal. Instead, the undergraduate cybersecurity law class should expose students to the fundamental legal issues that they will encounter throughout their careers in cybersecurity, and to understand when they need legal advice. The class also should cause students to think broadly and critically about the role of the cybersecurity profession in a society of laws and norms.
- Cybersecurity education is not a binary choice between technical and non-technical subjects. The students in my class apply their technical knowledge to the relevant laws, resulting in productive discussions. For instance, when we assessed the privacy implications of the Dark Web, much of the class involved a discussion of the mechanics of TOR. Relatedly, students tell me that the cybersecurity law class causes them to think carefully about the legal implications of their technical cybersecurity research.
- The course is most effective when it forces undergraduates to critically evaluate not only how current laws shape cybersecurity, but also how future laws *should* affect the field. As future cybersecurity leaders in the private sector or government, they may have the ability to shape the rapidly evolving body of cybersecurity law.