PROFESSORS JOAN FEIGENBAUM, OONA A. HATHAWAY, SCOTT SHAPIRO
THE LAW AND TECHNOLOGY OF CYBER CONFLICT
YALE LAW SCHOOL/YALE UNIVERSITY
FALL 2016

Class web site (URL above):
Required materials will be posted on the class web site under "Course Documents." Please check the class web site regularly for course announcements, homework assignments, and materials.

Course Meetings:
In Fall 2017, this course will meet on Wednesdays 9:25 am to 11:15 am in Baker Hall, Room A005. Non-law students will need to be granted access to Baker Hall. On the first day of class, we will make sure someone is at the entrance to let students in, but please arrive on time.

In Spring 2017, the same meeting time (Wednesdays 9:25 am - 11:15 am) will be reserved for the course, but we do not expect the class as a whole to meet every week. Instead, the faculty will hold individual and small-group meetings with students as needed to review progress on projects, and the class as a whole will meet every three to four weeks. The default time for individual and small-group meetings will be W 9:25 - 11:15, but students or faculty members can request other times if they are more convenient.

Overview (of this class and its Spring 2017 companion class):
This new cross-disciplinary, year-long course on cyber security will be taught jointly by faculty from the Law School and Computer Science Department. The course is motivated by the conviction that the field of cyber security in general and the emerging subfield of cyber conflict are plagued by the failure of experts to talk across disciplinary divides: Lawyers do not know what technologies are available to address cyber threats and so are often oblivious to technical problems and solutions. Cyber security technologists are often indifferent to the social or political context in which cyber attacks take place and ignorant of the legal regimes that apply. As a result, they often focus solely on technical solutions and fail to leverage the power of law to make bad actors cease and desist. As a matter of international law, "countermeasures" can be undertaken when there is both "necessity" and "proportionality," but, from a technological perspective, what do these legal terms mean? Progress on cyber security policy is hampered when technologists do not fully grasp the problems that lawyers and regulators are trying to solve and when lawyers and regulators do not understand the possibilities and limitations of technological responses.

The first semester of this year-long course will be a classroom seminar that will address the fundamental disconnect between the state of the law and the state of technology by engaging in a joint exercise of learning and teaching. Law students and faculty will participate in a crash course on the relevant technology, and computer science students and faculty will engage in a complementary and coordinated crash course on the relevant law. The course assumes no prior technological or legal expertise and is aimed at building common knowledge and creating a community of shared terminology and inquiry.

A year-long (2-semester) commitment is required. The second semester will be a hands-on practicum in which students will write papers, develop the computational theory of cyber conflict, and/or design and prototype novel technology. These projects will be designed to address some of the critical research gaps that have hindered long-term development of effective policy and technological responses to cyber conflict, including issues such as cyber deterrence in operations short of war, cyber vandalism and terrorism, and international cyber regulation. Specific project topics will be formulated based on the first semester's explorations and in consultation with policymakers who work on issues of cyber security.

Course Requirements:
You are expected to attend *every* class and to be prepared to discuss *all* the assigned reading. If you find you cannot attend, please notify Professors Hathaway, Shapiro, and Feigenbaum in advance.

Each student is expected to complete four 1200-word reflection papers during the course of the fall term. Papers are due by 5:00 p.m. the day before the class in which the material will be discussed by email to Annie Cooper, Ido Kilovaty, and Professors Hathaway, Shapiro, Feigenbaum (ann-marie.cooper@yale.edu; oona.hathaway@yale.edu; scott.shapiro@yale.edu; joan.feigenbaum@yale.edu; ido.kilovaty@yale.edu). In addition, there will be problem sets and other technical assignments throughout the fall term.

Students will be required, at the end of first semester, to submit proposals for their second-semester projects. Proposals should be substantial and may include an outline or technical specifications relevant to the project. They should be 8-10 pages long or the equivalent and are due on the last day of the fall term. For law students, substantial and SAW credit may be available.

In the spring term, as noted above, students must complete a substantial papers, develop the computational theory of cyber conflict, and/or design and prototype novel technology.

In the fall, grades will be based on written work (75%) and participation in the course (25%). Quality of participation is of course more important than quantity, though regular involvement in the discussion is helpful. If you find it difficult to speak in class for any reason, please come talk to us. In the Spring, grades will be based entirely on the written work.

Please bear in mind that this is a new course, so we reserve the right to make mid-course corrections. We also welcome feedback.

Enrollment:
Enrollment is capped. If you are a Yale College or Graduate School student interested in enrolling, please see http://www.cs.yale.edu/homes/jf/CyberConflictEnrollment.pdf for the selection criteria and application procedure. Refer to the course's OCI entry for pre-requisites.

Policy on Electronics and Media:
No laptops, smart phones, or other electronic devices may be used in class. Class discussions may not be recorded. Chatham House rules apply to all class discussions: Participants are

free to use the information received, but neither the identity nor the affiliation of any participants may be revealed without express permission. In addition, written class material is not to be shared with anyone not enrolled in the course. We welcome feedback on these policies as the semester progresses.

Reading Assignments:
Below please find reading assignments. Please note that these are subject to substantial revision as the semester proceeds.

(1) Introduction and Course Overview (August 31)

P.W. Singer and Allan Friedman, Cybersecurity and Cyberwar: What Everyone Needs to Know (2014) – Part I, "How it All Works," required; rest recommended. (This book is available in the Yale bookstore and on Amazon in both paper and Kindle formats. An electronic version is available through the Yale library.)
Ralph Langner: Cracking Stuxnet, a 21st-century Cyber Weapon, TED talk
Ralph Langner, To Kill a Centrifuge (2013) (executive summary, prologue, and Part B required; rest optional)

(2) Legal Background I (September 7)

Charter of the United Nations (especially art. 2(4), art. 51, and Ch. VII)
Oona A. Hathaway et al, "The Law of Cyber Attack," Cal. L. Rev. (2012)

(3) Legal Background II (September 14)

ICRC, International Humanitarian Law: Answers to Your Questions, https://www.icrc.org/eng/assets/files/other/icrc-002-0703.pdf.
Review all of the Geneva Conventions here. Read Common Article 3 closely.
Additional Protocols I & II
Recommended:
ICRC Databases on international humanitarian law:
https://www.icrc.org/eng/resources/ihl-databases/index.jsp

(4) Security-Technology Background I (September 21)

Charles P. Pfleeger, Shari Lawrence Pfleeger & Jonathan Margulies, Security in Computing (5th edition, 2015). Chapter 1 required, Chapters 2 and 3 recommended (This book is available on Amazon in both paper and Kindle formats. An electronic version is available through the Yale library at http://proquest.safaribooksonline.com/9780134085074?uicode=yaleu.)

(5) Security-Technology Background II (September 28)

Pfleeger, Pfleeger, and Margulies, Chapter 4 required, Chapters 5, 6, and 8 recommended

(6) Espionage vs. Conflict (October 5) (Case Studies: OPM Hack, DNC Hack & Stuxnet)

Ashley Deeks, An International Legal Framework for Surveillance, 55 Virginia Journal of International Law 291 (2015) (only Part I required, rest is recommended) (this piece is a good overview of the applicable law, though it does not focus on cyber)
Russel Buchan, Cyber Espionage and International Law (Research Handbook)

Michael Adams, Why the OPM Hack is Far Worse Than You Imagine, Lawfare (March 11, 2016)
Ellen Nakashima, U.S. Gives 'No Press Pass' to Russia, Other Nations on Cyberespionage, Justice Official Warns, Washington Post (Sept. 15, 2016)
Recommended:
Christopher Yoo, Cyber Espionage or Cyber War?: International Law, Domestic Law, and Self-Protective Measures
Russel Buchan, The International Legal Regulation of State-Sponsored Cyber Espionage, *in* International Cyber Norms (2016)

(7) "Zero Days," a movie directed by Alex Gibney (October 12)

October 12 is Yom Kippur, and we expect limited attendance. "Zero Days" will be shown in class to those who attend; those who do not attend class on this day are expected to watch it online; it is available on YouTube, iTunes, and Amazon Video.

Yale College Fall Recess (October 19): Class will not be held.

(8) Use of Force, Self Defense, and "Armed Attack" (October 26)
Carlo Focarelli, Self-Defence in Cyberspace (Research Handbook)
Marco Roscini, Cyber operations as a Use of Force (Research Handbook)
Peter Elkind, Hack of the Century, Fortune, http://fortune.com/sony-hack-part-1/ (read parts 1, 2, and 3).
Michael Schmitt, International Law and Cyber Attacks: Sony v. North Korea
Kim Zettner, Stuxnet Attack on Iran was Illegal "Act of Force," Wired Magazine
Recommended:
U.S. Department of Defense Law of War Manual, 16.3 CYBER OPERATIONS AND JUS AD BELLUM

(9) "Offensive" Countermeasures (November 2)
Tallinn Manual, Countermeasures
Oona Hathaway, The Drawbacks and Dangers of Active Defense
The NSA Is Likely 'Hacking Back' Russia's Cyber Squads, abcnews
Ashley Deeks, The Sony Hack: Will the United States Take Countermeasures Against North Korea?, Lawfare

(10) Attribution (November 9)
Tor Overview: https://www.torproject.org/about/overview.html.en
Joan Feigenbaum and Bryan Ford, Seeking Anonymity in an Internet Panopticon, Communications of the ACM, Vol. 58, No. 10, 58-69 (Oct 2015), http://www.cs.yale.edu/homes/jf/FeigenbaumFord2015.pdf
David D. Clark and Susan Landau, Untangling Attribution, in Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy, http://www.nap.edu/catalog/12997.html
Thomas Rid & Ben Buchanan, Attributing Cyber Attacks, The Journal of Strategic Studies, Vol. 38, Nos. 1–2, 4–37 (2015)
"Identification and Attribution Problems," in Marco Roscini, Cyber Operations and the Use of Force in International Law (Oxford, 2014)

(11) Civilian Targeters and Targets (November 16)

David Turns, Cyber Warfare and the Notion of Direct Participation in Hostilities, Journal of Conflict & Security Law (2012)

Yoram Dinstein, The Principle of Distinction and Cyber War in International Armed Conflicts, Journal of Conflict & Security Law (2012)

Thanksgiving Vacation (November 23)

(12) Encryption is not a panacea (FBI vs. Apple) (November 30)

Governments Turn to Commercial Spyware to Intimidate Dissidents, NY Times (May 29, 2016)

Going Dark, Going Forward, A Primer on the Encryption Debate, House Homeland Security Staff Report

Daniel Castro & Alan McQuinn, Unlocking Encryption: Information Security and the Rule of Law (March 2016)

(13) Stepping Back: Lessons learned about the integration (or lack thereof) of cyber law and cyber technology (December 7)

Review your notes and earlier readings. No new reading.