SYLLABUS

L578: Cybersecurity Law & Policy
Indiana University
Kelley School of Business
Professor Scott Shackelford
Spring 2020
Online

The course is run according to the terms in the syllabus, which is intended to let students know what they can expect and what is expected of them in the course. Students who remain in the course are presumed to understand and accept the terms in the syllabus; those who object should drop the course.

How to Contact Professor Shackelford

Office: CG2000 (Kelley School of Business), Office #206 (Ostrom Workshop, 513 Park Ave.),
Email: sjshacke@indiana.edu
Office Phone: (812) 856-6728
Mobile: (812) 369-1612 (only to be used for emergencies)

Office Hours

Mondays, 11:00am to 12:00pm. You do not need an appointment to come in during office hours. If these hours aren't convenient for you, I'll be glad to meet with you at another mutually convenient time. To set up an appointment, see me before or after class or contact me by email or phone.

Syllabus Quick Reference

COURSE DESCRIPTION & LEARNING OUTCOMES

Enhancing cybersecurity is a critical issue affecting the competitiveness of firms and the security of governments. Increasingly policymakers are fashioning regulatory schemes around the world that promise to shape not only the day-to-day realities of operating information systems, but also cyberspace itself. This course takes an interdisciplinary, global approach to introduce students to cybersecurity risk management. Course content includes comparative and international law related to managing cyber attacks. Connected topics such as Internet governance, privacy, and cybersecurity codes of conduct will also be addressed. Ultimately, we will analyze regulatory solutions as part of a larger universe of reforms needed to enhance cybersecurity and safeguard intellectual property.

The primary aim of the course is to provide students with a basic working knowledge of cybersecurity law and policy, focusing on the United States but put in a global perspective. The learning outcomes for this course, listed below, relate to the learning goals of the Kelley MSIS Program, which can be found in the appendix at the end of this syllabus. The number in parenthesis indicates to which specific learning outcomes the outcome relates.

Upon successful completion of the course, students will be able to:

- Understand the processes and mechanisms by which laws are made, changed, interpreted, and applied—and how legal disputes get resolved—in the European Union but put in a global context; (5)
- Identify significant legal concepts related to cybersecurity law and policy of interest to businesses and managers; (5)
- Increase your awareness and sensitivity to the legal and ethical implications of cybersecurity decisions; (5)
- Strengthen your critical thinking, logical reasoning, and problem-solving skills; (4) *and*
- Further develop the confidence necessary to work well collaboratively and understand how law and policy fits in with other aspects of information systems, and be a more robust contributor to the marketplace, our civil society, and the common good. (3, 6)

MY EXPECTATIONS

For most of you, the study of law is something new. It involves a new vocabulary and new concepts. Thus, especially at the beginning of the term, the course may seem somewhat confusing. Don't be discouraged. I guarantee that you're not alone. Seek help early. Find a good legal dictionary, such as Black's or this one: http://dictionary.law.com/. And as soon as you find yourself getting overwhelmed or confused, stop by office hours or email me to schedule a time for us to chat.

If you are not prepared for class, you will not get much out of the course. I expect each student to attend each scheduled session and to have read and thought about the assigned materials prior to attending class. I also expect you to participate in class discussions.

ASSIGNED MATERIALS

Text (T):	SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE (Cambridge University Press, 2014) [**Note that both the paperback and the e-book versions are perfectly acceptable*]
Internet (CI):	Materials to be downloaded from Canvas or a website
Handouts (HO):	Handouts occasionally distributed in class

All information for the course will be posted on the course website on Canvas, which students should regularly check.

ASSESSMENT

This course requires significant time and effort. It is designed to challenge students to adopt the work ethic necessary to excel in future academic and professional settings. To help facilitate that purpose, you can expect that I will do my best to: present subject matter that is mentally challenging as clearly as possible and by using frequent examples, be fair and impartial in dealing with students, create an environment in which you should feel free to ask questions and express opinions, assign grades that reflect your ability to apply what you have learned, and hopefully leave you wanting to learn more about cybersecurity law and policy.

Course performance will be assessed as follows:

All students will undertake short assessments throughout the class:

Short Assessments (100 points): To measure students' comprehension of the legal concepts and their proficiency at applying them, students take regular quizzes that test their ability to apply the legal rules in each lesson to hypothetical fact patterns in a limited period of time.

UN Security Council (UNSC) Cybersecurity Simulation (50 points): In order to better understand how the international community can meet the challenge of mitigating cyber risks, students will role play as members of the UN Security Council in a simulation designed by the Council on Foreign Relations. This is also an opportunity to integrate lessons across the curriculum in an effort to strategize about cybersecurity risk management at the highest policy levels.

Students will have a choice on how they would like to earn the remainder of the available points. The choice is between participating in a service-learning project, writing a research paper, or taking a final exam. **Only 1 of the 2 following options is required.**

Research Project (100 points): Students electing this option can draft a cybersecurity research paper on a topic of your choosing. Papers will consist of a 10-15-pages of original research, though students may work in pairs to undertake more ambitious projects. Projects must make use of at least 10 sources, and reference course content. A menu of options will be discussed in class, but students are encouraged to think creatively.

Final Exam (100 points): Students electing to take the comprehensive final exam will participate in a true/false, multiple choice, and short answer exam during the final exam period. Note: at least 10 students must elect this option for it to be offered.

	Total Available Points:	
Paper/Final Exam:	100	40%
Short Assessments:	100	40%
UNSC Simulation	50	20%
TOTAL:	**250**	100%

GRADING SCALE

The grading scale for the course is as follows:

Score	Grade	Score	Grade	Score	Grade	Score	Grade
97.50-100	A+	87.50-89.49	B+	77.50-79.49	C+	67.50-69.49	D+
91.50-97.49	A	81.50-87.49	B	71.50-77.49	C	61.50-67.49	D
89.50-91.49	A-	79.50-81.49	B-	69.50-71.49	C-	59.50-61.49	D-

***Please note that I rarely curve to arrive at final grades**, and I will not deviate from the grading scale unless necessary to achieve an appropriate grade distribution for the class. Such a departure will only raise, not lower, students' grades.*

****I reserve the right to create extra credit opportunities**, but do not guarantee that there will be extra credit opportunities in the course. Any extra credit opportunities will be open to the entire class.*

MAKEUP POLICY

This makeup policy is designed to allow you to miss an assessment without suffering adverse consequences for one of life's unfortunate events (including the alarm not going off), mental health days, or opportunities that do not rise (or fall) to the level of a compelling emergency as defined below. To be fair to students who are struggling with documentable, life-altering events beyond their control, I will entertain requests to make up an exam or weekly assessment if you meet ***all three of these conditions***:

> **(1)** You have a **compelling emergency** that will cause you to miss the exam or assessment;
>
> **(2)** You provide **written and dated evidence** that proves the compelling emergency, such as a note from a physician stating that you were too ill to attend class on the day of the assessment or exam or a dated obituary notice that mentions you by name' and
>
> **(3)** You **contact me** by email, phone, or in person and secure my permission to take a makeup **before** you miss the exam or assessment.

The burden of proof is on you to provide adequate evidence of the compelling emergency. You must provide your evidence prior to taking the makeup and I reserve the right to revoke my permission to provide a makeup if your evidence does not demonstrate the claimed

emergency or if it is not provided in what is, in my judgment, a timely manner.

The following are examples of compelling emergencies:

- Hospitalization or illness that is severe enough for you to seek medical attention
- Death in your immediate family
- Military deployment
- Jury duty or other mandatory court proceeding that cannot be rescheduled

The following are examples of reasons that are NOT compelling:

- Oversleeping
- Missing the bus
- Medical, legal, or other appointments or interviews that *can be rearranged*
- Traveling or leaving campus early for a university break or other holiday
- Studying for or working on an assignment for another course
- Any other activity that can be rescheduled

APPEALS OF GRADED WORK

Appeals of exams and other graded work must be submitted in writing within one week of the date on which the graded work is returned to you. You may do this by email, phone, or in person. In any appeals, I do not require explanations for why you misread or otherwise did not understand the question, but instead only why the question/answer is wrong as a substantive matter. I expect that most appeals will be unsuccessful on these criteria.

ATTENDANCE

Attendance is required in this class, and it is factored into the participation grade. It will provide the opportunity for you to get to know your classmates and the course material. If you do miss class, it is your responsibility to find out from your classmates what occurred in class.

READING ASSIGNMENTS

I expect you to have completed the assigned reading BEFORE class. You should also read the required Canvas/Internet texts that will be available through Canvas. Background materials are not required but are beneficial for students wanting a better grounding in a particular area.

ACADEMIC INTEGRITY

The Kelley School's policy on academic integrity will be strictly enforced in this class. I consider plagiarism, unauthorized assistance, and other forms of dishonesty on extra credit projects and short assessments to be as serious as dishonesty on exams. Unless I expressly authorize you to work with another student on any assignment or extra credit project, discussing anything about the assignment or project other than the required format and due date is academic dishonesty. Students are subject to the *Kelley Student Honor Code* (http://www.kelley.iu.edu/ugrad/honorCode.cfm) and the *Code of Student Rights, Responsibilities, and Conduct* (http://www.iu.edu/~code/code/index.shtml).

Special Note on Plagiarism: Plagiarism is a particularly common – but serious – form

of academic misconduct. Any work with your name on it signifies that the ideas and the text are your own. If you quote an author or use ideas from another source, you must properly cite your source to indicate the origin of your ideas. Failure to do so is considered plagiarism. Depending on the severity of the case, plagiarized work will be assessed a penalty, ranging from a lowered grade on the assignment to failure of the course.

If you are unsure what constitutes plagiarism, talk to me, talk to the Campus Writing Program's Writing Tutorial Services ("WTS"), and/or consult WTS's informational pamphlet, *Plagiarism: What It Is and How to Avoid It*, *available at* http://www.indiana.edu/~wts/wts/plagiarism.html.

ADMINISTRATIVE MATTERS

A. Students with Disabilities

Any student with a disability requiring reasonable accommodation should inform me by email within the first two weeks of class so that we can make the necessary accommodation(s). You also must provide to me a completed copy of the "Testing / Classroom Modifications" form from the Office of Disability Services.

B. Religious Holidays

Any student who has a religious conflict with an assignment or is otherwise unable to participate in the class for religious reasons must inform me by email within the first two weeks of class so that we can make alternative arrangements. Forms are available at http://www.indiana.edu/~vpfaa/holidays.shtml.

PROJECTED COURSE CALENDAR & ASSIGNED READINGS

T = Denotes passages from textbook
C/I = Document or case to be downloaded from Canvas or a website
HO = Handout distributed in class

The course will begin with an introduction to law, the U.S. legal system, and ethical reasoning. It will then proceed to examine cybersecurity law and policy in three units:

Date	Topic	Reading Assignments	Deliverables
Week #1 R Mar. 25	Welcome & Orientation to the Course / Unpacking the Cyber Threat, & Launch of UNSC Simulation (*time permitting)* Cyber Risk Insurance & Internet Governance	**T**: Preface, Pages 19-49 **C/I**: *Computer Security is Broken From Top to Bottom*, ECONOMIST (Apr. 8, 2017), https://www.economist.com/news/science-and-technology/21720268-consequences-pile-up-things-are-starting-improve-computer-security **C/I**: Michael Schwartz & Joseph Goldstein, *Russian Espionage Piggybacks on a Cybercriminal's Hacking*, NEW YORK TIMES (Mar. 12, 2017), https://www.nytimes.com/2017/03/12/world/europe/russia-hacker-evgeniy-bogachev.html?_r=1 **C/I**: *Back to the Future of Internet Governance?*, GEORGETOWN, http://journal.georgetown.edu/back-to-the-future-of-internet-governance/	*Sign up for Politico Cybersecurity Morning Report (or similar service, see Appendix)

		C/I: *Should Your Firm Invest in Cyber Risk Insurance?* **Background**: **C/I**: *How is the Internet Governed?*, https://globalchallenges.org/en/the-prize/materials/how-is-it-governed/how-is-the-internet-governed **C/I**: Former Secretary Clinton, *Remarks on Internet Freedom*, STATE DEPARTMENT, http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm	
UNIT ONE: FOUNDATIONS OF CYBERSECURITY LAW & POLICY			
Week #2 T Mar. 30	Intro to Cybersecurity Law and the FTC & Defining "Cyber Law" I: Torts & Fiduciary Duties	**C/I**: Kosseff FTC Reading **C/I**: The T.J. Hooper, 60 F.2d 737, 740 (2d Cir. 1932) (L. Hand, J.), http://guweb2.gonzaga.edu/~dewolf/torts/pdf/TJHooper.pdf **C/I**: *Toward a Global Standard of Cybersecurity Care?*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2446631 (skim Parts I and II)	*Cybersecurity Project Choice Due *Note, please watch the online tutorial "Intro to U.S. Law/Legal Research" on Canvas prior to class
Week #2 R Apr.1 ***Quiz 1***	Defining "Cyber Law" II: Standing, Smart Contracts, & IP Protection	**T**: Pages 79-84 **C/I**: *Block-by-Block*, YALE JOURNAL OF LAW & TECHNOLOGY, http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1131&context=yjolt **Background**: **C/I**: Intellectual Property, http://www.law.cornell.edu/wex/intellectual_property **C/I**: Contracts, http://www.law.cornell.edu/wex/contract	
Week #3 T Apr. 6	U.S. Federal Cybersecurity Law & Policy Primer	**T**: Pages 174-80, 235-46, 315-17, skim 52-79 **Background**: **C/I**: Cyber Policy Task Force Exec. Summary for the 45th Presidency, https://www.csis.org/news/cybersecurity-agenda-45th-president **C/I**: Trump Administration Cybersecurity Executive Order, https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal **C/I**: Michael Daniel, *Improving the Security of the Nation's Critical Infrastructure*, WHITE HOUSE, http://www.whitehouse.gov/blog/2013/02/13/improv	*Thesis and Outline due to Instructor (Research Projects)

		ing-security-nation-s-critical-infrastructure?utm_source=related **C/I**: Obama Administration Cyberspace Policy Review, pages iii-vi, https://www.whitehouse.gov/cyberreview/documents/ **C/I**: International Strategy for Cyberspace Fact Sheet, https://www.whitehouse.gov/sites/default/files/rss_viewer/International_Strategy_Cyberspace_Factsheet.pdf **C/I**: Clinton Administration CNI Directive, http://www.fas.org/irp/offdocs/pdd/pdd-63.htm **C/I**: Bush Administration National Strategy to Secure Cyberspace, pages vii-xiii, http://www.dhs.gov/national-strategy-secure-cyberspace	
Mid-Semester Course Evaluation *Your opportunity to anonymously evaluate the course*			
UNIT TWO: DIMENSIONS OF CYBER CONFLICT			
Week #3 R Apr. 8 ***Quiz 2***	Cyber War, Crime, Espionage, & Terrorism *Review Special Agent Alford Recording	**T**: 7-17, Chapter 6 **Background:** **C/I**: Michael Schmitt, *Tallinn Manual 2.0 on the International Law of Cyber Operations: What It Is and Isn't*, https://www.justsecurity.org/37559/tallinn-manual-2-0-international-law-cyber-operations/ **Background:** **C/I**: Criminal Law Primer, http://www.law.cornell.edu/wex/criminal_law **C/I**: *How Far Should Organizations be able to go to Defend Against Cyberattacks?*, CONVERSATION (Feb. 15, 2019), https://theconversation.com/how-far-should-organizations-be-able-to-go-to-defend-against-cyberattacks-110143 **C/I**: *Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis* (skim), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2573787	
FRIDAY, APRIL 17 – CYBER PEACE COLLOQUIUM (OSTROM WORKSHOP)			
Week #4 T Apr. 13	UN Security Council Simulation		*UNSC Position Memos Due
UNIT THREE: THE LAW, POLITICS, AND PROMISE OF CYBER PEACE			

Week #4 R Apr. 15 ***Quiz 3***	Law of Cyber Peace & Comparative Cyber Risk Mitigation Strategies	**T**: Pages 325-28, 356-66 **Background**: **C/I**: *The Need for a Digital Geneva Convention*, MICROSOFT (2017), https://tinyurl.com/gwgd6q2 **C/I**: *The Law of Cyber Peace*, CHICAGO JOURNAL OF INTERNATIONAL LAW (forthcoming 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2805061	*Lit Review/Rough Draft (optional but recommended)
Week #5 T Apr. 20	Cybersecurity Ethics	**C/I**: Ethics and CSR (Richards & Shackelford Textbook) **Background:** **C/I**: *A Framework for Thinking Ethically*, http://www.scu.edu/ethics/practicing/decision/framework.html **C/I**: Bruce Weinstein, *If It's Legal, It's Ethical…Right*?, http://www.businessweek.com/managing/content/oct2007/ca20071011_458606.htm **C/I**: *Should Cybersecurity be a Human Right?,* CHRISTIAN SCIENCE MONITOR (2017), https://theconversation.com/should-cybersecurity-be-a-human-right-72342 **C/I**: *Microsoft Cyberethics*, http://www.microsoft.com/security/online-privacy/cyberethics-practice.aspx	
Week #5 R Apr. 22	IU Wellness Day		
Week #6 T Apr. 27 ***Quiz 4***	Research Paper Presentations Hot Topics: Making Democracy Harder to Hack Securing the Internet of Things National Cybersecurity Safety Board	**C/I**: *When Toasters Attack*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2715799 (skim) **C/I**: *Making Democracy Harder to Hack*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852461 (skim) **C/I**: *The Tech Behind Bitcoin Could Reinvent Cybersecurity*, https://tinyurl.com/j2ce9t2 Good luck!	*Slides Due *Reflections Due *Final Capstone Project Due *Peer Evaluations Due *Final Research Projects Due
Week #6 R Apr. 29	Final Exam Review Session (if applicable)	Good luck!	

APPENDIX A: KELLEY MSIS PROGRAM LEARNING GOALS

Goal 1: Technical Expertise

Demonstrate a thorough command of the technical aspects of information systems.

Goal 2: Managerial and Organizational Frameworks

Explain how managerial and organizational issues affect the use of information systems in organizations.

Goal 3: Integration with Other Functional Areas of Business

Integrate information systems and information technology with other business topics to analyze and recommend solutions to business problems.

Goal 4: Critical Thinking and Communication

Apply critical thinking skills to develop evidence-based recommendations and effectively communicate them to non-technical professionals.

Goal 5: Risk, Compliance and Ethical Considerations

Demonstrate an understanding of the risk management, compliance and ethical issues in the use of information systems in organizations.

Goal 6: Teamwork and Collaboration

Demonstrate effective teamwork and collaboration skills and the ability to work with clients professionally.

APPENDIX B: WHO'S PROFESSOR SHACKELFORD?

I'm a native Hoosier, having grown up in Indianapolis, Nashville, Greenwood, and Bloomington. I earned my Bachelor's degree in Economics and Political Science from IU, was part of the Liberal Arts Management Program, and studied abroad in Spain and Britain.

Following my time as a student at IU, I went on to earn a Master's in International Relations from the University of Cambridge as a Rotary Ambassadorial Scholar (a program that I'd love to talk to any of you about if you're interested). I went on to earn a Ph.D. from Cambridge. As if that wasn't enough school, I also earned J.D. from Stanford Law School. These days, I'm the Chair of the IU Cybersecurity Program, and the Executive Director of the Ostrom Workshop.

Prior to joining the faculty at Kelley, I worked for several law firms, consulted for the U.N. Development Program in India, clerked at the NASA Office of General Counsel, helped create an elder law pro bono program at the San Mateo Legal Aid Society in California, and taught law to undergraduates at Stanford University. My research focuses on cybersecurity law and policy, as well as sustainability and international law. For fun, I like to travel, write sci-fi, jog, kayak, and try to keep up with my three girls.

APPENDIX C: USEFUL CYBERSECURITY WEBSITES

- State of Indiana CISO Blog, http://www.in.gov/iot/cisoblog.htm
- IU Cybersecurity Program, www.cybersecurityprograms.indinaa.edu
- IU Cybersecurity Site, www.cybersecurity.iu.edu
- Stanford Cybersecurity, http://cisac.stanford.edu/research/2956/

- Center for Strategic and International Studies Cybersecurity Page, http://csis.org/category/topics/technology/cybersecurity
- International Association for Privacy Professionals, https://iapp.org/
- Politico Cybersecurity Report, http://www.politico.com/cybersecurity
- Cyber-wire, https://thecyberwire.com/
- Ostrom Workshop Program on Cybersecurity and Internet Governance, https://ostromworkshop.indiana.edu/research/internet-cybersecurity/index.html