

Course Information

Course Number:	CSCE 402/702; CYBR 402/602; MARA 403
Course Title:	Cybersecurity Law & Policy
Section:	CSCE 402/500; CSCE 702/600; CYBR 402/500; CYBR 602/600; MARA 403/401
Time:	T, TR 5:30 – 6:45 p.m.
Location:	ZACH 310
Credit Hours:	3

Instructor Details

Instructor:	Paula deWitte, J.D., Ph.D., P.E.
Office:	Peterson 225
Phone:	Preferred mode of communication is email.
E-Mail:	paula.dewitte@tamu.edu

If in reference to homework or exams, please copy:

Class TA:	Lakhan Saiteja Kamireddy at lakhan@tamu.edu
Class Grader:	Siddhant Thakur at sidthakur08@tamu.edu

Office Hours: Thursday 2 – 3 p.m. (in office) or by appointment (in office or by Zoom)

Course Description

This course examines law and policy issues related to cybersecurity for the spectrum of cybersecurity jobs including those defined in the NIST NICE Framework (procurement, operations/maintenance, governance and oversight, protection/defense, analysis, intelligence collection/operation; and investigation) cybersecurity jobs. Tomorrow's cyber workers are exposed to more data and privacy issues that requires them to analyze law, policies, and regulations both under United States jurisdiction and international jurisdiction (Spoiler Alert: *The internet has changed our traditional notion of jurisdiction!*). Law is traceable and based on precedent while technology is disruptive. Law necessarily lags technology resulting in an uncertain legal and ethical framework which requires cyber workers to be able to analyze and distinguish appropriate courses of action as part of their daily tasks without the luxury of relying on legal counsel. This is especially crucial given the dynamics of the threat and response landscape, The course will focus on international and federal law and not specific state data breach laws other than a cursory review and explanation of when states or federal has jurisdiction.

The course first examines the fundamentals and basics of law – jurisdiction, due diligence, case/controversy, standing, statute of limitations, remedies/damages, and evidence standards – to establish a foundation to apply and analyze legal issues that are especially problematic regarding cybersecurity. The course then explores the national and international legal frameworks that govern cybersecurity and their implications for attacks, motives, responses, and counter-attacks through the lens of what is permissible against attacking individuals or entities versus attacking nation-states including legal issues such as “hacking back” and problems such as accurate attack attribution. The course then examines the legal issues raised by the cloud related to privacy and third parties including emerging standards. The overarching goal of this course is to provide a cyber-worker in technical, business or policy domains with the knowledge and skills to better interpret threats and responses in a national and international law framework while understanding (and being sympathetic to) the limits of the current law and how law/policy can evolve for cybersecurity. This course is not intended to make you lawyers, but rather legal-savvy cyber workers.

The course includes current events discussion on relevant information and relies on extensive analysis of laws and policies whereby students will demonstrate their knowledge and skills by preparing short written assignments throughout the semester.

Course Prerequisites

Junior, senior, or graduate classification. Preferred to have some programming experience or understand computer concepts although not required.

Special Course Designation

This is a stacked course. All assignments and exams for undergraduate and graduate students are weighted differently as explained in the Grading Policy section below with all sections having the same assignments and exams.

Course Learning Outcomes

Upon successful completion of this course, a student will be able to:

1. Acquire the common body of knowledge for cybersecurity law including legal concepts and legal terminology.
2. Understand the importance of the United States Constitution and the various Amendments in protecting privacy relative to cybersecurity.
3. Understand the separation of powers between the three branches of government and how that relates to cybersecurity.
4. Differentiate between how each contributes to our legal framework and its scope: laws passed by legislative bodies, regulations by government agencies, opinions from judicial proceedings, presidential executive orders, and industry standards or best practices.
5. Identify the legal authorities applicable to a cybersecurity scenario.
6. Identify and explain common legal issues related to cybersecurity.
7. Assess and explain legal procedural requirements relevant to cybersecurity.

8. Acquire the common body of knowledge related to both national and international laws related to cybersecurity and the differences between United States law and laws of other jurisdictions.
9. Demonstrate the ability to work through a case study identifying legal issues, analyzing the cybersecurity action required, and formulating a plan that complies with applicable laws.
10. Evaluate the relationship and discern the differences between ethics and law and apply the notion of “grey areas” to describing situations where law has not yet caught up to technological innovations.
11. Discern valid legal references for proper research and analysis of cybersecurity legal issues.
12. Apply legal concepts in issues related to cybersecurity including cases/controversies unique to cybersecurity.
13. Demonstrate the ability to use legal knowledge by analyzing cybersecurity issues from a cyber worker perspective such as whether a security incident violates a privacy principle or legal standard requiring specific legal action.

Textbook and/or Resource Materials

Required Text

- Cybersecurity Law, 2nd Edition by Jeff Kosseff, ISBN-13: 978-1119517207

We will read all chapters (1 – 11) and selected Appendices as references.

I recommend that you buy this book!

Referenced Texts:

- Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations by Michael N. Schmitt, ISBN 978-1-316-82252-4. **I do not recommend that you buy this book!**
- You'll see this message when it is too late by Josephine Wolff, ISBN 978-0-262—3885-0.
- Twenty-six Words that Created the Internet by Jeff Kosseff, ISBN-10: 1501714414.
- This is How They Tell Me the World Ends by Nicole Perlroth, ISBN-10 : 1635576059.
- Other readings as assigned and either placed on CANVAS or communicated with web references.

Grading Policy

The student's semester grade will be based on assignments, exams, and a semester paper.

Weekly/Bi-Weekly Assignments (5): There will be a total of 5 writing assignment. The topics for these assignments can be found in the course schedule. Each assignment should be answered in 1-2 pages according to the template posted on the CANVAS Learning Management System for this class.

Semester Paper: Students **should** select a topic to write for this paper before the fifth week of class. The requirements for the paper and the rubric for grading will be posted on the CANVAS Learning Management System for this class.

Exams: Two major exams will be given in this course at five and ten weeks during the course. Both exams will be essay tests. A third exam will be short answer and cover material from the last lectures.

Course grades will be assigned using the following scale:

Requirement:	Undergraduate Points	Graduate Points
Assignments (5 assignments each worth 50pts for undergraduate students and 40 points for graduate students)	250 (25%)	200 (20%)
Semester Paper	250 (25%)	300 (30%)
First Exam	200 (20%)	200 (20%)
Second Exam	200 (20%)	200 (20%)
Third Exam	100 (10%)	100 (10%)
Total	1000 (100%)	1000 (100%)

Points Grading Scale: <i>Out of 1000 assignable points</i>	
A	900 - 1000 points
B	800 - 899 points
C	700 - 799 points
D	600 - 699 points
F	< 600 points

Assignments Rubric

The rubric for the assignment is based on IRAC: Issue + Rule + Analysis + Conclusion

20%	Issue: Did you come up with a relevant legal issue related to the course, and did you tie that issue to the course? Did you explain the problem/issue clearly? (If you fail to describe an issue, it will be difficult to analyze.)
20%	Rule: What makes this a relevant legal issue? What rules of law are you applying? Did you do a thorough research, that is clearly communicated?
20%	Analysis: You do not merely re-state the rule and research, but analyze what is leading to your subsequent conclusion. Tie your analysis to course knowledge to demonstrate what you learned from this course. This is also a good time to bring up any voids or gaps in current laws or to differentiate legal and ethical issues.
20%	Conclusions: Clearly state the conclusions based on the issue, rule, and analysis and ensure that there is a logical pathway to follow.
20%	Presentation: formatting, proper grammar, correct spelling, proper use of words, proper capitalization (e.g., Congress referring to the United States Congress is always capitalized as is the First Amendment. These are proper nouns. Don't use first person.).

- **Assignment Requirements: (Same for undergraduate and graduate students)**
 - **Page Requirement:** 2 – 3 pages (Note: 2 complete pages are required. Not 1 and almost a second page. This does not include sources.
 - **Margins:** 1" on all sides
 - **Line Spacing:** 1.5
 - **Font:** Calibri 11 Preferred; no bigger than 12 point font
 - **References Required:** Each assignment will have a minimum number of required, valid references. If it is not there, assume a minimum of two valid references

Semester Paper

The purpose of the semester paper is to integrate the knowledge and skills for the semester into a meaningful course deliverable related to the course learning objectives. It is to demonstrate that the student has developed the analytical skills necessary to assess real-world cybersecurity scenarios. It is most closely related to the last three learning objectives—to properly discern information about the law and to use analytical skills developed in this course on a topic of the student's choice (subject to instructor approval).

Paper Requirements:

- **Margins:** 1" on all sides
- **Line Spacing:** 1.5
- **Font:** Calibri 11 Preferred; no larger than 12 point font acceptable.
- **References Required:**
- **Minimum of 10 valid references.**
 - References can be formatted with a valid hyperlink. No special formatting required.
 - **What is important is that there are 10 VALID references.**
- **Undergraduate Page Requirements:**
 - **5 - 7 Pages of content (not including references)**
 - Your paper must have a title and author limited to three single spaced lines of the content. It may have a title page (your choice) that does not count to the page requirements.
 - Note: **A minimum of five complete** pages of content are required. **Not 4 and half or three-quarters of a page);**
 - **The five pages of content excludes references.**
- **Graduate Page Requirements**
 - **6 - 7 Pages of content (not including references)**
 - Your paper must have a title and author limited to three single spaced lines of the content. It may have a title page (your choice) that does not count to the page requirements.
 - Note: **A minimum of six complete** pages of content are required. **Not 5 and half or three-quarters of a page);**
 - **The six pages of content excludes references.**

Percentage of Total Point	Criteria	Rubric
20% of total points	Idea selection and explanation: Did you come up with a good idea relative to this course? Did you tie that idea to the content of this course? Did you adequately explain the importance of the problem/issue?	18 – 20% of total pts: Selected idea exceeds expectations. 16% – 17% of total pts: Selected idea meets expectations. 14% - 15% of total pts: Selected idea is not clearly linked to course. 12% - 13% of total pts: Selected idea is weakly linked to course and will undermine other evaluation factors, notably Research and Analysis. 0% - 11% of total pts: Selected idea is not acceptable.
20% of total points	Research process: Did you do good research from valid sources to investigate your idea? Did you clearly communicate that research in the paper? Do you have the correct number of required valid references?	18 – 20% of total pts: Research as described exceeds expectations. 16% – 17% of total pts: Research as described meets expectations. 14% - 15% of total pts: Research is not clearly communicated or there is a lack of required valid references (missing no more than 3 valid references). 12% - 13% of total pts: Research is weak and will undermine other evaluation factors, notably Analysis or there is a significant lack of required valid references (missing more than 3 valid references). 0% - 11% of total pts: Research is not acceptable. References are not valid.
20% of total points	Analysis: Did you analyze your research and draw conclusions based on your research? Did you apply analytical skills to tie that analysis to course knowledge to demonstrate what you learned from this course. Is your analysis clearly communicated in the paper?	18 – 20% of total pts: Analysis of research as described exceeds expectations. 16% – 17% of total pts: Analysis of research as described meets expectations. 14% - 15% of total pts: Analysis may be adequate, but is not clearly communicated and tied to research. 12% -13% of total pts: Analysis is weak and not tied to research. 0% - 11% of total pts: Analysis is not acceptable.

20% of total points	Presentation: Did you properly format your paper according to the requirements? Did you use proper grammar, correct spelling, proper capitalization (e.g., Congress referring to the United States Congress is always capitalized as is the First Amendment as proper nouns.) Does your paper look professional?	<p>18 – 20% of total pts: Presentation of content exceeds expectations and is properly formatted and follows rules for proper grammar and spelling.</p> <p>16% – 17% of total pts: Presentation of content meets expectations with some minor errors in grammar, spelling, or capitalization.</p> <p>14% - 15% of total pts: Presentation of content is not clearly communicated.</p> <p>12% - 13% of total pts: Presentation of content has some serious issues with grammar, spelling, capitalization, etc.</p> <p>0% - 11% of total pts: Presentation of content is not acceptable with major problems with grammar, spelling, capitalization, etc.</p>
20% of total points	Writing Style: How well does your paper read? How well do you organize your ideas? Is the paper substantial and would be of interest for other students in the class?	<p>18 – 20% of total pts: The paper is informative and exceeds expectations in terms of clarity and presenting the ideas, research, and analysis.</p> <p>16% – 17% of total pts: The paper is informative and meets expectations in terms of clarity and presenting the ideas, research, and analysis.</p> <p>14% - 15% of total pts: The paper has not clearly communicated the idea, research, and analysis.</p> <p>12% - 13% of total pts: The paper is difficult to read and understand the idea, research, and analysis.</p> <p>0% - 11% of total pts: The paper is unacceptable and fails to present the idea, research, and analysis in a coherent manner.</p>

Late Work Policy

Late work is work that is not turned in according to the class process by the assigned due date. The instructor may accept late work if the student notifies the instructor BEFORE the assigned due date except in truly emergency situations.

Typically, late and/or make-up work will not be accepted without a university excused absence. (See [Student Rule 7](#).) If an absence is excused, then the student will be provided an opportunity to make up any homework assignments, quizzes, exams, or other work that contributes to the final grade with a due date that extends the original due date by the number of days of the excused absence. Individual arrangements will be made for exams and quizzes missed due to an excused absence. In all cases, TAMU Student Rule 7 will govern the process.

Course Schedule

Date	Topics	Assignment Milestones
Week 1 Aug 25 – Sept 1	<p>Introduction to Course & Expectations. Walk-through course syllabus. Discussion of Semester Paper.</p> <p>Using on-line resources and finding relevant current events.</p> <p>Differences between engineering and legal mindsets (“<i>It depends.</i>”).</p> <p>Basic cybersecurity terminology and concepts.</p> <p>Overview of the American legal system</p> <p>Legal concepts: Due diligence, Jurisdiction, Standing; Venue; Case/Controversy, Statute of Limitations; Evidence Standards (Civil vs Criminal); Remedies/Damages; “Reasonableness standards,” etc.</p> <p>Other American legal concepts: Right to face accuser, double jeopardy, the role of “public policy” in court decisions, etc.</p> <p>Legal Infrastructure:</p> <p>State and federal laws.</p> <p>Federal executive, legislative, and judicial branches.</p> <p>Appellate review process— federal and state (or how a federal law can be interpreted differently within different areas of the US).</p>	<p>Read Kosseff Chapter 1: Data Security Laws and Enforcement Actions (skip Section 3.1 pp 48 - 56); don’t worry about specific case names and descriptions; focus on “Key Lessons” and look for the commonality in those key lessons for class discussion.</p> <p>Appendix A: Section 5 of the FTC Act</p> <p><u>Reading Kosseff Chapter 1 this week is essential.</u> The remaining reading can be in the first two weeks. Don’t be overwhelmed! This is background material (but – <i>it’s so interesting!</i>).</p> <p>Focus specifically on legal terminology and concepts as discussed in class.</p> <p>Read SANS Paper: OPM vs. APT: How Proper Implementation of Key Controls Could Have Prevented a Disaster (on CANVAS). Periodically through the semester, we’ll refer to this SANS paper. As your legal analysis knowledge grows, you will realize how much you have learned using this paper as your guide. Your first read will probably be overwhelming. Your last read of the semester will be – <i>I know that!</i></p> <p>Read US Constitution (Articles I, II, III, IV, and VI). http://constitutionus.com/ and https://www.law.cornell.edu/constitution</p> <p>Read Federal Courts and what they do: https://www.fjc.gov/content/federal-courts-and-what-they-do-2</p> <p>At the end of Week 1 (3 lectures), you may not be able to recall all concepts and terminology from memory, however you should be able to analyze how and where to find the answer! We will refer to this as our framework of legal analysis that we will use through the rest of the course.</p>

	<p>Common law (state) civil causes of action: Contract breach; breach of implied warranty; negligence; unjust enrichment; fraud; slander; invasion of privacy.</p> <p>Privileges: Attorney-client, Work Product Doctrine, and Non-testifying Expert ... <i>in anticipation of litigation</i></p> <p>Chapter 1: Data Security Laws and Enforcement Actions – specifically FTC Act Section 5</p>	<p>And remember – first step -- always check to see if a term has a legal definition!</p>
<p>Week 2</p> <p>Sept 6 - 8</p>	<p>The concept of “standing” – Article III of the Constitution and SCOTUS interpretation</p> <p>Fun facts: Google the cases in the footnotes regarding standing on pages 52 – 53, especially Whitmore v. Arkansas for the type of case/controversy. <i>Whoa! Did not see that coming!!!!</i></p> <p>Putting it all together to bring a cybersecurity case to court—walk-thru the legal process—both civil and criminal.</p> <p>(Free legal advice: <i>Never ever ignore when served by a court of competent jurisdiction. Never. Ever.</i>).</p>	<p>Read Kosseff Chapter 2: Cybersecurity Litigation</p> <p>We will emphasize the legal concept of standing and how lack of standing affects cybersecurity cases.</p> <p>We will not discuss specific state consumer protection or data breach laws.</p> <p>Assignment 1: Write a one-to-two page paper on a fundamental legal issue as being confusing/critical to cybersecurity.</p> <p>Due in one week. Submit through CANVAS.</p> <p>5% of course grade for undergraduate students and 4% of course grade for graduate students.</p>
<p>Week 3</p> <p>Sept 13</p> <p>No Class on Sept 15!</p>	<p>Privacy (“The right to be let alone”): Is there a “right” to privacy? If so, how do we define privacy so that we can effectively legislate protecting that right?</p>	<p>Read Kosseff Chapter 7: Surveillance and Cyber and Appendix E: Electronic Communications Privacy Act</p> <p>US Constitution Amendments 1, 3, 4, and 5</p> <p>Assigned readings on CANVAS</p>

	<p>Legislative:</p> <p>The Privacy Act (1974);</p> <p>The Stored Communications Act (1986)</p> <p>The Wiretap Act (Title III of the Omnibus Crime Control and Safe Streets Act of 1968)</p> <p>The Electronic Communications Privacy Act (1986)—amendment to the Wiretap Act</p> <p>Judicial: SCOTUS opinions on privacy (Griswold v. Connecticut, Roe v Wade, Lawrence v. Texas), expectation of privacy (Katz v. United States), recent decisions strengthening 4th Amendment protections (Carpenter v United States).</p> <p>4th Amendment: Review of SCOTUS decisions on the requirements for Fourth Amendment Warrants. <i>What's next after Carpenter v United States?</i></p> <p>14th Amendment: Review of Scotus decisions on due process.</p>	
<p>Week 4</p> <p>Sept 20</p> <p>- 22</p>	<p>Continue Privacy.</p> <p>Federal Laws on Hacking Back: Computer Fraud Abuse Act -- CFAA (1986) and proposed revisions; effect on hacking back Digital Millennium Copyright Act (1998).</p>	<p>Read Kosseff Chapter 9: Privacy Laws</p> <p>Read Kosseff Chapter 10 (Section 10.1, pages 386 – 396)</p> <p>Read Kosseff Chapter 5: Anti-Hacking Laws</p> <p>Appendix C: Section 1201 of the Digital Millennium Copyright Act (DMCA) and</p> <p>Appendix D: Computer Fraud and Abuse Act</p> <p>Read assigned paper(s) on “hacking back;”</p> <p>Read: 2018 National Cyber Strategy</p>

		<p>https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf</p> <p>and the companion document: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF</p> <p>and the Solarium Report either the Executive Summary (22 pages) or the report (182 pages)</p>
<p>Week 5</p> <p>Sept 27 - 29</p>	<p>Continue Federal Laws on Hacking Back: Computer Fraud Abuse Act -- CFAA (1986) and proposed revisions; effect on hacking back Digital Millennium Copyright Act (1998).</p> <p>Take-home Exam 1! Due in one week.</p>	<p>Read Kosseff Chapter 9</p> <p>Read Kosseff Chapter 10.1</p> <p>Read Kosseff Chapter 5: Anti-Hacking Laws and Appendix C: Section 1201 of the Digital Millennium Copyright Act (DMCA) and Appendix D: Computer Fraud and Abuse Act</p> <p>Assigned paper(s) on “hacking back;”</p> <p>Read: 2018 National Cyber Strategy https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf</p> <p>and the companion document: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF</p> <p>and the Solarium Report either the Executive Summary (22 pages) or the report (182 pages)</p> <p>Assignment 2: Research the legal issues of privacy related to cybersecurity and write a one-to-two page paper discussing some legal issue.</p> <p>Due in one week. Submit through CANVAS. 5% of course grade for undergraduate students and 4% of course grade for graduate students.</p>
<p>Week 6</p> <p>Oct 4 - 6</p>	<p>US Federal Cybersecurity Laws:</p> <p>Legislative: FISMA (Federal Information Security</p>	<p>Read Kosseff Chapter 8: Cybersecurity and Federal Government Contractors</p>

	<p>Management Act) and how it relates to common law recognition of NIST Standards and FIPS 199 and FIPS 200</p> <p>NIST Standards in a Legal Sense: Documentation and <u>how applying good cybersecurity practices may cause legal risk!</u> [Note: NIST is NOT a federal regulatory agency.]</p> <p>Executive: (1) Presidential Directives and Introduction to Executive Orders. (2) Executive agencies (e.g., FTC). (3) Federal agencies—later lecture.</p> <p>Judicial: Common law.</p>	<p>Readings as assigned. Obviously one excellent source is https://csrc.nist.gov/publications/sp800 (as discussed and navigated in class).</p> <p>Review SANS paper on OPM regarding NIST controls</p> <p>Should have selected a topic for a semester paper by this week.</p>
<p>Week 7</p> <p>No Class</p> <p>October 11 (Fall Break)</p> <p>Oct 13</p>	<p>Cybersecurity and the Cloud: FEDRAMP</p> <p>Catch up week – this is our first semester “breather” week to either catch up (if we’re behind) and/or to take time to fully digest information so far. At least one lecture will be devoted to “Point/Counterpoint” classroom discussion where students will be given positions and argue whether to defend or reject. More fun if your assigned position is counter to your personal beliefs.</p>	<p>Readings as assigned. Obviously one excellent source is www.fedramp.gov.</p> <p>Assignment 3: Write a one-to-two page paper on a specific NIST family of controls (pick out one or two controls) and think through any legal issues that should be considered. This is where the OPM paper might provide some ideas.</p> <p>Due in one week. Submit through CANVAS.</p> <p>5% of course grade for undergraduate students and 4% of course grade for graduate students.</p>
<p>Week 8</p> <p>Oct 18 – 20</p>	<p>Scope and effect of federal regulations and how enforced.</p> <p>Regulatory Agencies (FTC, FCC, SEC, CFPB, DHS, Department of Education; other financial/banking regulations)</p>	<p>Kosseff Chapter 3 (skip Section 3.7 pp 147 – 154) Cybersecurity Requirements for Specific Industries;</p> <p>Kosseff Chapter 4 Cybersecurity and Corporate Governance</p>

	relative to cybersecurity and/or privacy.	
Week 9 Oct 25 - 27	International Law: Tallinn Manual 2.0 on International Law on Cyber Operations: Sovereignty Due diligence Jurisdiction United Nations Charter (Jus ad bellum) Hague Conventions & Geneva Conventions (Jus in bello) Posse comitatus	Read Kosseff Chapter 10: International Cybersecurity Laws and Chapter 11: Cyber and the Law of War Read Chapters 1, 2, & 3 of the Tallinn Manual: Sovereignty, Due Diligence, and Jurisdiction Skim through Table of Contents and organization of Tallinn Manual PLEASE DO NOT CONFUSE THE TALLINN MANUAL 2.0 AS ACTUAL BINDING INTERNATIONAL LAW!!!! Read Kosseff 6.4 Military Involvement in Cybersecurity and Posse Comitatus
Week 10 Nov 1 - 3	Other federal laws of interest. Take-home Exam #2. Due in one week.	
Week 11 Nov 8 – 10	Critical Infrastructure as a cybersecurity threat. Executive: Presidential Directives and Executive Orders related to Securing Critical Infrastructure and the United States Patriot Act. Legislative: The <i>Cybersecurity Information Sharing Act</i> -- CISA (2015), Cybersecurity Enhancement Act (2014); NIST Cybersecurity Framework	Read Kosseff Chapter 6: U.S. Government Cyber Structure and Public-Private Partnerships Assignment 4: Research a legal issue related to protecting critical infrastructure from one of the critical infrastructure sectors and write a one-to-two page paper Due in one week. Submit through CANVAS. 5% of course grade for undergraduate students and 4% of course grade for graduate students.
Week 12	Intellectual Property Theft as a Cyber Threat	Assignment 5: Summarize and write a one-to-two page paper on your assessment of the current state of ethics in cybersecurity – think through the Tallinn Manual, hacking back, CFAA, etc. and class discussions. Potential topics

Nov 15 - 17	Legislative: Economic Espionage Act (1996) Uniform Trade Secrets Act -- UTSA (1985) & DMCA	could include some aspect that causes controversy or conflict with US law. Due in one week. Submit through CANVAS. 5% of course grade for undergraduate students and 4% of course grade for graduate students.
Week 13 Nov 22	Cybersecurity Ethics New and emerging issues in cybersecurity law & policy since class started.	Assigned readings. Cyber Ethics: What's right, what's wrong, what's legal, and what's ethical.
	No Class November 24.	Happy Thanksgiving!
Week 14 Nov 29 - Dec 1	New and emerging issues in cybersecurity law & policy since class started. December 1: In class Exam #3.	Semester papers due! – 25% of course grade for CSCE 402 & MARA 403, 35% for CSCE 702.
Week 15 Dec 6	Course Evaluations; Wrap-Up.	

Attendance Policy

The university views class attendance and participation as an individual student responsibility. Students are expected to attend class and to complete all assignments.

Please refer to Student Rule 7 in its entirety for information about excused absences, including definitions, and related documentation and timelines.

Makeup Work Policy

Students will be excused from attending class on the day of a graded activity or when attendance contributes to a student's grade, for the reasons stated in Student Rule 7, or other reason deemed appropriate by the instructor.

Please refer to Student Rule 7 in its entirety for information about makeup work, including definitions, and related documentation and timelines.

Absences related to Title IX of the Education Amendments of 1972 may necessitate a period of more than 30 days for make-up work, and the timeframe for make-up work should be agreed upon by the student and instructor” (Student Rule 7, Section 7.4.1).

“The instructor is under no obligation to provide an opportunity for the student to make up work missed because of an unexcused absence” (Student Rule 7, Section 7.4.2).

Students who request an excused absence are expected to uphold the Aggie Honor Code and Student Conduct Code. (See Student Rule 24.)

Academic Integrity Statement and Policy

“An Aggie does not lie, cheat or steal, or tolerate those who do.”

“Texas A&M University students are responsible for authenticating all work submitted to an instructor. If asked, students must be able to produce proof that the item submitted is indeed the work of that student. Students must keep appropriate records at all times. The inability to authenticate one’s work, should the instructor request it, may be sufficient grounds to initiate an academic misconduct case” (Section 20.1.2.3, Student Rule 20).

You can learn more about the Aggie Honor System Office Rules and Procedures, academic integrity, and your rights and responsibilities at aggiehonor.tamu.edu.

NOTE: Faculty associated with the main campus in College Station should use this Academic Integrity Statement and Policy. Faculty not on the main campus should use the appropriate language and location at their site.

Americans with Disabilities Act (ADA) Policy

Texas A&M University is committed to providing equitable access to learning opportunities for all students. If you experience barriers to your education due to a disability or think you may have a disability, please contact Disability Resources in the Student Services Building or at (979) 845-1637 or visit disability.tamu.edu. Disabilities may include, but are not limited to attentional, learning, mental health, sensory, physical, or chronic health conditions. All students are encouraged to discuss their disability related needs with Disability Resources and their instructors as soon as possible.

NOTE: Faculty associated with the main campus in College Station should use this Americans with Disabilities Act Policy statement. Faculty not on the main campus should use the appropriate language and location at their site.

Title IX and Statement on Limits to Confidentiality

Texas A&M University is committed to fostering a learning environment that is safe and productive for all. University policies and federal and state laws prohibit gender-based discrimination and sexual harassment, including sexual assault, sexual exploitation, domestic violence, dating violence, and stalking.

With the exception of some medical and mental health providers, all university employees (including full and part-time faculty, staff, paid graduate assistants, student workers, etc.) are Mandatory Reporters and must report to the Title IX Office if the employee experiences, observes, or becomes aware of an incident that meets the following conditions (see [University Rule 08.01.01.M1](#)):

- The incident is reasonably believed to be discrimination or harassment.
- The incident is alleged to have been committed by or against a person who, at the time of the incident, was (1) a student enrolled at the University or (2) an employee of the University.

Mandatory Reporters must file a report regardless of how the information comes to their attention – including but not limited to face-to-face conversations, a written In-Class Work or paper, class discussion, email, text, or social media post. Although Mandatory Reporters must file a report, in most instances, you will be able to control how the report is handled, including whether or not to pursue a formal investigation. The University's goal is to make sure you are aware of the range of options available to you and to ensure access to the resources you need.

Students wishing to discuss concerns in a confidential setting are encouraged to make an appointment with [Counseling and Psychological Services \(CAPS\)](#).

Students can learn more about filing a report, accessing supportive resources, and navigating the Title IX investigation and resolution process on the University's [Title IX webpage](#).

NOTE: *Faculty associated with the main campus in College Station should use this Title IX and Statement on Limits of Liability. Faculty not on the main campus should use the appropriate language and location at their site.*

Statement on Mental Health and Wellness

Texas A&M University recognizes that mental health and wellness are critical factors that influence a student's academic success and overall wellbeing. Students are encouraged to engage in proper self-care by utilizing the resources and services available from Counseling & Psychological Services (CAPS). Students who need someone to talk to can call the TAMU Helpline (979-845-2700) from 4:00 p.m. to 8:00 a.m. weekdays and 24 hours on weekends. 24-hour emergency help is also available through the National Suicide Prevention Hotline (800-273-8255) or at suicidepreventionlifeline.org.

Personal Illness and Quarantine

Students required to quarantine must participate in courses and course-related activities remotely and **must not attend face-to-face course activities**. Students should notify their instructors of the quarantine requirement. Students under quarantine are expected to participate in courses and complete graded work unless they have symptoms that are too severe to participate in course activities.

Absences will be excused only if the absence due to COVID (or other medical conditions) complies with university regulations.

Students experiencing personal injury or illness that is too severe for the student to attend class qualify for an excused absence (See [Student Rule 7, Section 7.2.2.](#)) To receive an excused absence, students

must comply with the documentation and notification guidelines outlined in Student Rule 7. While Student Rule 7, Section 7.3.2.1, indicates a medical confirmation note from the student's medical provider is preferred,