

Political Science 188-02: Topics in International Relations
Computer Science 50: Special Topics
Cybersecurity and Cyberwar

Spring Semester 2019
Block D +: Tuesday and Thursday 10:30 to 11:45 AM
Anderson Wing SEC Room 206

Prof. Jeff Taliaferro
Political Science Department
Packard Hall 112
Office Hours: Mondays 10 to 11:30 AM
and by appointment

Sr. Lecturer Ming Chow
Computer Science Department
Halligan Hall 228A
Office Hours: Wednesdays from 1 to 4 PM

This course is an interdisciplinary analysis of cybersecurity and cyberwar in the United States and other countries. It is intended to introduce computer science (CS) students to the policymaking and intelligence aspects of cybersecurity and political science (PS) and international relations (IR) students to the technical constraints of computer networks and software. The course will involve hands-on activities such as packet analysis, exploiting a vulnerable system, password cracking, social engineering, reconnaissance, and malware analysis. We will examine state and non-state actors engaged in cyber-espionage, counterintelligence, deterrence, and offensive cyber-operations. There will be guest speakers from the private sector, the military and intelligence community.

The five goals of the course are:

1. To engage PS and IR majors in a sustained discussion of the technical aspects of cybersecurity and cyberwar, which have emerged as major aspects of international relations and United States national security;
2. To expose CS majors to the realm of intelligence and policymaking and to help them understand key issues in strategic management of cybersecurity in the private sector and in government;
3. To develop intellectual bridges among students and faculty members in different disciplines and schools. We are convinced that the lack of progress in cybersecurity is due to knowledge gaps between the technical community and policymakers and between the technical community and the public.
4. To encourage all students to be engaged citizens. Currently, there is a lack of ownership in education and informing the public about the political, legal, and ethical aspects of cyberspace. Being informed and involved are perquisites for civic engagement.
5. To engage in constructive and healthy debates, as the issues in cyberspace are political, complex, and controversial. There will always be trade-offs between secrecy and public disclosure, individual privacy and convenience, technological innovation and vulnerability.

PREREQUISITES

For PS and IR Majors: PS 61: Intro. to International Relations. No computer science background is required, but academic maturity is expected.

For CS students in A&S or SoE: COMP 11: Intro. to Computer Science. No political science course work is required, but some academic maturity is expected.

SOFTWARE

Students will need the following software:

- A copy of the Kali Linux Live-CD ISO: [Download at http://www.kali.org/downloads/](http://www.kali.org/downloads/)
- One of the following to run the Kali Linux live-CD ISO:
 - [Virtual Box \(free\)](https://www.virtualbox.org/wiki/Downloads): Download at <https://www.virtualbox.org/wiki/Downloads>
 - [VMware Fusion for Mac OS X or VMware Workstation for Windows or Linux \(free one year license via Tufts CS\)](http://vmap-tufts.onthehub.com/): Download at <http://vmap-tufts.onthehub.com/>

PS 160 Canvas <http://Canvas.tufts.edu>

This course makes extensive use of Canvas. The required readings are available on Canvas. We will use the Canvas Discussion Boards for weekly discussions of the readings. You must upload all written work to the Assignment of Canvas. The deadlines appear on the last page of this syllabus. Please note we do not accept paper copies or email copies of assignments under any circumstances. There are no exceptions. Please plan accordingly.

GRADING AND ASSESSMENT

There are seven graded assignments for this course:

1. Capture the Flags and Risk Analysis (20 percent)
2. Weekly Reading Discussions (10 percent)
3. Individual Video Project (10 percent)
4. In-Class Debate on GDPR (15 percent)
5. Policy Memorandum on a cybersecurity policy issue (20 percent)
6. Team Personal Engagement Project (15 percent)
7. Class Participation, Attendance, and Decorum (10 percent)

Please note: These assignments are indivisible. In order to earn a passing grade in the course, students must earn passing grades in all assignments. In other words, failing, not participating, or simply not submitting any one requirement will lead to a failing grade for the course. There are no “do-overs” or opportunities for “extra credit.” Please plan according.

1) Capture the Flags and Risk Analysis (20 percent)

- a) This is a team-based exercise designed to show how software works and how to find and exploit vulnerabilities in software and hardware. We will provide detailed instructions and guidelines.
- b) We will begin the Capture the Flags and Risk Analysis in class on Thursday 7 February. For this assignment, each student will want to have a laptop computer available. The competition will conclude in class on Tuesday 12 February.

2) Weekly Reading Discussion (10 percent)

- a) The required readings for this course include articles in peer-reviewed scholarly journals and policy-oriented journals in IR, policy briefs, reports and working papers from various think tanks, cybersecurity firms, and some government bodies, and few articles from general-interest publications. All of the readings are available on CANVAS as either *.pdf or hyperlinks.

- b) We expect you to complete all readings by the class meeting for which they were assigned. We also expect you to regularly participate in the weekly Discussions of the readings on Canvas.
- c) The Discussion area of the PS 188-02/COMP 50 Canvas site is organized in different “pinned threads.” There is a “pinned thread” for each class meeting/topic. Discussion posts will be evaluated on a complete/incomplete basis. Each student must make a minimum of fifteen distinct and substantive posts to the Discussion area over the course of the semester in order to earn a “complete” grade.

3) Individual Video Project (10 percent)

- a) Each student will produce a brief video (no more than 2 minutes) designed to teach a single topic to people outside his/her/their major discipline.
- b) A list of possible topics is posted on Canvas.
- c) Your video must be made publicly available. You can submit video on Canvas or a URL of your video on YouTube or some other video sharing website. If you submit video on Canvas, we will make your video publicly available. The deadline for uploading your video to Canvas or posting the link to YouTube or another site 12 PM (noon) on Thursday 31 January.

4) In-Class Debate on General Data Protection Regulations (15 percent)

- a) There will be a debate on whether the United States ought to adopt the European Union’s General Data Protection Regulations (GDPR) in class on Tuesday 12 March.
- b) The class will be divided into several teams representing stakeholders in consumer data privacy debates (e.g., the technology companies, congressional committees, law enforcement and intelligence agencies, etc.). Each team will be responsible for researching its position in the days before the debate. To assist each team in preparing its position, there will be a Research Guide prepared by the Tisch Library available in mid-February.
- c) Additional details, the team assignments, and the grading rubric will be posted on Canvas in mid-February.

5) Policy Memorandum (20 percent)

- a) Each student will submit a policy memorandum on a pressing issue in cybersecurity. Each memorandum should identify a technical or policy issue, analyze that issues, and make recommendations to appropriate stakeholders.
- b) The memorandum may be directed to the information technology (IT) company, an intelligence agency, a congressional committee, or senior executive branch policymakers. Detailed guidelines will be distributed on Canvas.
- c) The maximum-length of each memorandum is 6 pages, not including footnotes or a bibliography. The deadline for submitting the memorandum to Canvas is 12 PM on Friday 12 April.

6) Team Personal Engagement Project (15 percent)

- a) This assignment is an opportunity for pairs of students to take responsibility for their own learning. Each pair of students is required to actively engage with the larger community by participating in a public meeting, a professional group, a seminar, or conference on a substantive issue in cybersecurity and policy. Detailed guidelines appear on Canvas.
- b) Each pair of students will give brief a 5-minute presentation on their team personal engagement projects (PEPs) during the last two weeks of the semester. *The time limit for presentations will be strictly enforced.* If you wish to use slides (e.g., PowerPoint, Keynote, Prezi, etc.), then please restrict your presentation to no more than 4 slides.

- c) Each pair of students must also submit a short-written report (not more 4 pages) that details: (1) the reason why they chose this direction, (2) what they learned the venture, and (3) what, if anything, they might do differently if they had had more time.
- d) The deadline for submitting the short-written report (and any slides) to Canvas is 12 PM on Monday 29 April (the last day of spring 2019 semester classes).

7) Class Participation, Attendance, and Decorum (10 percent)

- a) We expect everyone to arrive on time and to stay until class is dismissed. Class sessions will be a mix of lectures, discussions, group-activities, guest speakers, and films.
- b) In addition to the Tuesday and Thursday class meetings in Anderson Wing SEC Room 226, all students in the class are required to attend the First Annual Tufts University Student Cybersecurity and Policy Symposium. The symposium will begin on the afternoon on Friday 4 April and continue on Saturday 5 April in the Cheryl Chase Center (adjoining the Carmichael Residence Hall).
- c) We encourage you to ask questions during class, provided that those questions are relevant to the topic under discussion. Chances are that if you are confused on an issue, a good number of your classmates are confused as well. *However, we strongly discourage “snarky” questions or comments, polemics disguised as questions, conspiracy theories, or asking questions just to demonstrate “how smart” you are.*
- d) An excessive number of absences or simply disappearing for weeks without explanation will have a very negative effect on the class participation and attendance portion of your course grade. Likewise, an excessive number of “bathroom breaks,” “water cooler breaks,” and other disruptive behaviors during class will have a very negative effect on the class participation and attendance portion of your course grade.
- e) If you must miss a class meeting due to illness, a family emergency, or the observance of a religious holy day, it is your responsibility to notify us and to get the notes from a classmate. It is not our responsibility to repeat materials discussed in class. It is not your classmates’ responsibility to inform us of your illness, your family emergency, or your observance of a religious holy day.

UNIVERSITY AND CLASS POLICIES

Academic Honesty

- You should be familiar with [Academic Integrity for Graduate and Undergraduate Students](#), available on the Dean of Student Affairs website.
- Tufts University policy states: “Faculty members who encounter an instance where substantial evidence of academic dishonesty exists must report the situation to the Dean of Student Affairs office. This policy assures consistency in the treatment of academic dishonesty and allows the institution to identify repeat offenders. The Dean of Student Affairs office will work with the faculty member in applying university and departmental policies and assist in determining an academic outcome.”
- Academic dishonesty includes the following: buying papers; borrowing papers; lending papers (or parts of papers) to other students; submitting the same assignment for two different classes without the express permission of both instructors; plagiarism, defined as quoting material from other sources without using quotation marks or paraphrasing materials without proper citation; and uploading corrupted files to Canvas.
- Tufts University has a site license for *Turnitin*, a leading anti-plagiarism software package. We have set up the Assignments in Canvas so that students must run the

policy memorandum through Turnitin before submitting it. You will be able to view the report generated by Turnitin. Doing so, will give you greater peace of mind. We do read the originality reports generated by Turnitin for assignments.

Late Papers

- *All late submissions incur a penalty of 10% (i.e., a letter grade) per each day or portion thereof after the deadline.* This means, an assignment submitted anywhere from one minute to one day late that might otherwise have earned a 90% (A-), will instead earn an 80% (B-). If the same assignment were two days late, it would earn a 70% (C-). Any assignment submitted five days after the deadline automatically earns a 50% or lower (F). *No exceptions.* Please plan accordingly. The late penalties are not negotiable. Canvas automatically time stamps all submissions, thus enabling us to see who has or has not submitted an assignment on time.
- *Only students with legitimate and documented reasons are exempt from the late penalties.* There are only three legitimate reasons:
 - Bereavement (e.g., the death of a parent, a step parent, a sibling, or another close relative);
 - A life-threatening illness in your immediate family that requires you to leave campus; or
 - A serious illness or medical emergency that requires you to receive immediate medical attention
- In the case of bereavement or a family emergency, the student must ask his or her Associate Dean of Undergraduate Advising (“alpha dean”) in Dowling Hall to send us notification. In the case of a serious illness or medical emergency, the student is required to provide medical documentation from Health Service or other medical provider information if the student is too ill to take an in-class mid-term or in-class final examination.
- Please remember that any student in such unfortunate circumstances is still responsible for obtaining documentation from your alpha dean and/or Health Services in a timely fashion. A timely fashion means a within a day or two, not three or four weeks.
- We are stringent in enforcing deadlines to reward the overwhelming majority of students who submit assignments on time. We also seek to prevent collective action problems and chaos.

Grading Standards

- There is no grade curve in this class. All excellent work will earn an A (90-99%); all meritorious work will earn a B (80-89%); work without any marked merit or defect will earn a C (70-79%); and all unsatisfactory or mediocre work will earn a D (60-69%). Abysmal, incompetent, or non-existent work will earn an F (59% or lower). These are the standards set in the [Bulletin of Tufts University: School of Arts and Sciences and School of Engineering](#).
- Tufts University policy states: “Effective education requires timely and objective evaluation of students’ academic work, using clear, standard, fair and public criteria. Such standards should be listed in the course syllabus. While criteria differ across disciplines and faculty, and while the ultimate responsibility for setting standards and evaluating performance rests with departments and individual faculty, submitted grades are final and not subject to negotiation.”

- Please do not attempt to bargain, negotiate, or plead for a higher grade. The grading guidelines for the policy memorandum and the personal engagement project appear on Canvas. Please remember, that in the interest of fairness to everyone, we evaluate all work according to these guidelines. When the people grading you give you the playbook, then “common sense” suggests you read and follow the playbook!
- Please remember, we can only evaluate the work submitted. We cannot grade the amount of “effort” you put into an assignment or the course as a whole. We do not award “extra credit.” Remember, we must hold all students to the same standards. We also have limited time to grade assignments.

Students with Disabilities, ESL Students, and Academic Help

- Students with Disabilities: If you have a disability that requires reasonable accommodations, please contact the Student Accessibility Services Office at Accessibility@tufts.edu or 617-627-4539 to make an appointment with an SAS representative to determine appropriate accommodations. Remember it is your responsibility to notify the SAS Office of any disability at the **beginning** of the semester. Please be aware that accommodations cannot be enacted retroactively.
- English as Second Language (ESL) Students: If English is not your first language or you are not proficient in standard written English, please seek assistance at the Academic Resources Center (ARC) in Dowling Hall.
- Tutoring, Time Management, and Academic Skills: The ARC also offers *free* peer tutoring, help with writing, and workshops on efficient reading, note taking, and time management.

SCHEDULE OF READINGS AND TOPICS

We will try to maintain the following schedule of readings and topics. However, we may need to make changes because of guest speakers, current events, snow days, or because we spend more time on a particular topic than anticipated. Furthermore, *we assure you there will be a major cyber incident (or several incidents) between the start of spring semester classes on 17 January and the last class on 29 April.* You can find any updates on Canvas under "Announcements." We also make an announcement in class. Please treat the syllabus on Canvas as the most recent and definitive version.

Part I: Understanding the Nature of the Problem

17 Jan.: What is Cybersecurity? What is Cyberwar?

22 Jan.: Who Will Protect US?

- Required Reading: Michael E. DeVine, "Defense Primer: National and Defense Intelligence," *CRS In Focus*, 20 December 2018, p. 2. Available on Canvas
- Required Reading: Michael Warner, "Intelligence in Cyber- and Cyber in Intelligence," in George Perkovich and Ariel E. Levite, eds., *Understanding Cyber Conflict: 14 Analogies* (Washington, DC: Georgetown University Press, 2017) pp. 17-30. Available on Canvas

24 Jan: Networking and the Worldwide Web

- Required Reading: "How the Web Works: In One Easy Lesson" <http://mkcohen.com/how-the-web-works-in-one-easy-lesson>
- Required Reading: "Thousands of computers open to eavesdropping and hijacking" <https://nakedsecurity.sophos.com/2014/08/15/thousands-of-computers-open-to-eavesdropping-and-hijacking/>
- Tools Used: Wireshark, nmap, SHODAN

29 Jan.: Cryptography

- Tools used: John the Ripper (password cracker)

31 Jan: Vulnerability and Exploitation

- Required Reading: "OWASP Top 10" https://www.owasp.org/index.php/Top_10_2013-Release_Notes
- Required Reading: "CWE/SANS TOP 25 Most Dangerous Software Errors" <https://www.sans.org/top25-software-errors/>
- Required Reading: "We See the Future and It's Not Pretty Predicting the Future Using Vulnerability Data" by Chris Wysopal, CTO Veracode
- Required Watching: Cross-Site Scripting (XSS) Tutorial by Chris Eng (Veracode) <http://www.veracode.com/security/xss>
- Tools to be Used: Burp (proxy), static analysis

5 Feb.: Malware—Viruses, Worms, Backdoors, Rotkits, and Trojans

- Case Study: <http://ntsecurity.nu/toolbox/tini/>

7 Feb.: Capture the Flag and Risk Analysis Competition Begins

- The Capture the Flag competition will begin in class. Team assignments will be posted on Canvas beforehand. It is critically important that every student bring a laptop computer to class.

12 Feb.: Capture the Flag Competition Concludes

Part II: Malicious Actors in Cyberspace and Government and Private Spector Responses

14 Feb.: Cyber Crime and Law Enforcement

- Required Reading: Sasha Romanosky, and Trey Herr, "Understanding Cyber Crime," in Richard M. Harrison and Trey Herr, eds., *Cyber Insecurity: Navigating the Perils of the Next Information Age* (Lanham, MD: Rowman & Littlefield, 2016), pp. 89-104. Available on Canvas
- Required Reading: Eric Jardine, "The Trouble with (Supply-Side) Counts: The Potential and Limitations of Counting Sites, Vendors or Products as a Metric for Threat Trends on the Dark Web," *Intelligence and National Security*, Vol. 34, No. 1 (2019), pp. 95-111. Available on Canvas

19 Feb.: Cyber Espionage and Counterintelligence

- Required Reading: Steven Loleski, "From Cold to Cyber Warriors: The Origins and Expansion of NSA's Tailored Access Operations (TAO) to Shadow Brokers," *Intelligence and National Security*, Vol. 34, No. 1 (2019), pp. 112-128. Available on Canvas
- Required Reading: Chris Jaikaran, "DHS: Cybersecurity Missions," *CRS In Focus*, 19 December 2018, p. 2. Available on Canvas
- Required Reading: Jack Goldsmith, and Robert D. Williams, "The Failure of the United States' Chinese Hacking Indictments," *Lawfare*, 28 December 2018, p. 4. Available on Canvas

21 Feb.: Substitute Monday's Schedule on Thursday
No class meeting

26 Feb: Challenges of State-to-State Coercion in Cyberspace

- Required Reading: Erica D. Borghard, and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies*, Vol. 26, No. 3 (2017), pp. 452-481. Available on Canvas

5 March: Cyber Threat Intelligence

Guest speaker: Winona Di Sombre, *LA 2018; threat intelligence researcher, Recorded Future*

7 March: Covert Operations, Disinformation, and Psychological Warfare in Cyberspace

- Required Reading: *Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations*, 2018 (Washington, DC: United States Senate Select Committee on Intelligence, 114th Congress, 2nd session), p. 6. Available on Canvas

- Required Reading: Benjamin Jensen, Brandon Valeriano, and Ryan Maness, "Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist," *Journal of Strategic Studies* (2019), pp. 1-23. Available on Canvas

12 March: In-Class Debate: Should the United States adopt GDPR?

14 March: The Politics of Attribution in Cyberspace

- Required Reading: Michael Poznansky and Evan Perkoski, "Rethinking Secrecy in Cyberspace: The Politics of Voluntary Attribution," *Journal of Global Security Studies*, Vol. 3, No. 4 (2018), pp. 402-416. Available on Canvas

16-24 March Spring Recess

26 March: Financial Sector Cyber Threat Analysis

Guest speaker: Matt Weinberg, *LA 2007, MALD 2017; analyst, Morgan Stanley*

2 April: Cyber Threats to Strategic (Nuclear) and Conventional Arsenals

- Required Reading: *Report to the Committee on Armed Services, US Senate: Weapon Systems Cybersecurity: DoD Just Beginning to Grapple with Scale of Vulnerabilities*, GAO-19-128 (Washington, DC: General Accountability Office, October 2018), p. 50. Available on Canvas
- Required Reading: Beyza Unal and Patricia Lewis, *Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities, and Consequences*, 2018 (London: Chatham House, Royal Institute of International Affairs), p. 26. Available on Canvas

4 April: The Role of USCYBERCOM

Guest speaker: Amanda C. Current, *Advanced Strategic Planning and Policy PhD Fellow, The Fletcher School; major, US Army, USCYBERCOM*

- Required reading: Catherine A. Theohary, "Defense Primer: Cyberspace Operations," *CRS In Focus*, 18 December 2018, p. 2.

5 and 6 April: First Annual Tufts University Student Cybersecurity and Policy Symposium

All students in PS 188-02/COMP 50 are required to attend the symposium. The symposium will begin on Friday afternoon and conclude early Saturday afternoon.

Part III: The Way Forward?

9 April: Can We Make the (Civilian) Internet-of-Things More Secure?

- Required Reading: TBA

11 April: TBA

16 April: Team Personal Engagement Project (PEP) Presentations

Last updated: 7:59 AM 16 January 2019

18 April: Team PEP Presentations

23 April: Team PEP Presentations

25 April: Conclusions

PS 188-02/COMP 50 Calendar of Assignments and Events (Spring 2019)	
Individual Video Project	Deadline for uploading video or posting link on Canvas: 12PM Fri. 1 Feb.
In-Class Debate on GDPR	Team Assignments Distributed on Canvas: 12 PM on Friday 15 Feb. Team Position Papers Due on Canvas: 10: 30 AM on Tues. 12 March In-Class Debate: Tues. 12 March
First Annual Tufts University Student Cybersecurity and Policy Symposium	Cheryl Chase Center: 1:30 to 6:00 PM, Friday 4 April and 9:30 AM to 1:30 PM, Saturday 5 April
Policy Memorandum	Deadline for Submission: 12 PM on Friday, 12 April
Team Personal Engagement Project (PEP)	Brief Presentations in class on 18, 20, and 23 April Deadline for submitting Written Report to Canvas: 12 PM Monday 29 April (last day of Spring 2019 Classes)

Reminder

The deadlines for assignments apply to all students enrolled in this class. These deadlines are not negotiable. We cannot grant an extension or move assignment due dates because you are "stressed out" or because you have other commitments, including but not limited to the demands of other classes, athletic competitions, EPIIC, ALLIES, NIMEP, political protests, job or internship interviews, or other extracurricular activities. PLEASE DO NOT ASK.

We have tried to ensure that due dates do not fall on the holy days listed on the **2018-2019 Tufts University Academic Calendar**. It is not always possible, however, to avoid conflicts with holy day observances. If your observance of a holy day that appears on the Tufts University Academic Calendar conflicts with one of these due dates, then please let us know as soon as possible.