Last updated: 2:53 PM 19 January 2017

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

Cybersecurity and Cyberwar

Spring Semester 2017
http://trunk.tufts.edu
https://piazza.com/tufts/spring2017/comp50ps18802/home
Block J+: Tuesdays and Thursdays 3:00-4:15 PM
The Terrace Room, Paige Hall

Associate Prof. Jeff Taliaferro
Department of Political Science
Packard Hall 112
Office Hours: Monday, 9:30-11:30 AM
and by appointment

Sr. Lecturer Ming Chow
Department of Computer Science
Halligan Hall 228A
Office Hours: Wednesdays from 1-4 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 students to the policymaking and intelligence aspects of cybersecurity and political science and international relations 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, civilian liberties groups, and the national security establishment.

The five goals of the course are:

1. To engage political science (PS) and international relations (IR) majors in the School of Arts & Sciences (A&S) 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 computer science (CS) students in A&S and the School of Engineering (SoE) 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 the Computer Science Department, the Political Science Department, and the International Relation Program. 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 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: Introduction to International Relations. No computer science background is required, but academic maturity is required.

For CS students in A&S or SoE: COMP *11:* Introduction to Computer Science and COMP 15: Data Structures. Some technical and academic maturity is required.

READING AND VIDEO ASSIGNMENTS
There are no required books to purchase for this class. All required readings are available on Trunk as *.pdf or links to other websites. There are also links to various videos. You should complete the assigned readings and watch the assigned videos before the class session indicated on the syllabus.

SOFTWARE
Students will need the following software:

- A copy of the Kali Linux Live-CD ISO: Download at http://www.kali.org/downloads/
- One of the following to run the Kali Linux live-CD ISO:
  - Virtual Box (free): 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): Download at http://vmap-tufts.onthehub.com/

TRUNK and PIAZZA
This course makes extensive use of two web-based platforms: Trunk and Piazza. You must submit all written assignments to the Assignment area of Trunk. 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.

This semester we will be using Piazza for class discussion. The system is highly catered to getting you help fast and efficiently from classmates and from us. Rather than emailing questions to us, we encourage you to post your questions on Piazza. If you have any problems or feedback for the developers, email team@piazza.com.

GRADING AND ASSESSMENT
There are four graded assignments for this course

1. Capture the Flags and Risk Analysis (25 percent)
2. Policy Memorandum on a Cybersecurity Issue (25 percent)
3. Personal Engagement Project (25 percent)
4. Class Participation and Attendance (25 percent)

Please note: These assignments are indivisible. In order to earn a passing grade in the course, students must earn passing grades in all four 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 (25 percent)**
   - 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.
   - We will play Capture the Flags in class on Tuesday 9 February. For this assignment, each student will want to have a laptop or tablet computer available. (Please see Class Participation and Attendance below.)
2. **Policy Memorandum (25 percent)**
   - 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.
   - 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.
   - The maximum-length of each memorandum is 8 pages, not including footnotes or a bibliography.
3. **Personal Engagement Project (25 percent)**
   - This assignment is an opportunity to take responsibility for one's own learning. Each student 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. Detailed guidelines will be distributed.
   - Students may submit a short-written report (not more 4 pages) or a short presentation 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. These brief reports may be uploaded to the Assignment area of Trunk at anytime before the last day of spring 2017 semester classes.
   - Students will give brief in-class presentations on their personal engagement projects during the last two weeks of the semester.
4. **Class Participation and Attendance (25 percent)**
   - We expect everyone to arrive on time and to stay until class is dismissed.
   - Please come to class prepared to discuss the assigned readings. Class sessions will be a mix of lectures, discussions, group-activities, guest speakers, and films.
   - 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.*
   - We also encourage you post sane and relevant questions and to contributed to discussions on Piazza. This is one form of class participation. We regularly read questions posted to Piazza and we will try to reply to questions.
   - 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.
   - 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

- ***We ask that you please not use laptops, notebook, tablet computers or smartphones in class, except when we tell you otherwise.*** You will get will get more out of this class if you actively listen, write down a few key points, and participate in the discussion, instead of trying to type every word spoken. More importantly, using electronic devices often distracts others in the class and is considered discourteous. ***Please note there will be some class sessions when you will want to have a laptop on hand. We will let you know ahead of time.***

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 Trunk.
- Tufts University has a site license for *Turnitin*, a leading anti-plagiarism software package. We have set up the Assignments in Trunk 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. Trunk 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 Education ("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 Trunk. 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 and we 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.

E-mail Etiquette

- Please ask all substantive questions in class or on Piazza. We do regularly read and reply to questions posted on the Piazza.
- We cannot provide technical support for TRUNK, Piazza, Student Information Services (SIS), MS Office 365, or any other software program or web-based platform. You should direct all technical support questions to the Tufts Technology Services Help Desk.
- ***Please only send us email to discuss private matters or emergencies.***

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 19 January and the last day of classes on 27 April.* You can find any updates on Trunk under "Announcements." We also make an announcement in class. Please treat the syllabus on Trunk as the most recent and definitive version.

Part I: Understanding the Nature of the Problem

19 Jan.: Introduction to the Course

- No reading assignment

24 Jan.: How We Dug Ourselves into a Deep Hole: Social Engineering

- Required Reading: Intelligence Community Assessment, *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution* (Washington, DC: National Intelligence Council, Office of the Director of National Intelligence, 6 January 2017), unclassified, 25 pages. https://www.dni.gov/files/documents/ICA_2017_01.pdf
- Required Watching: Dan Geer's keynote at the Black Hat 2014 Conference https://www.youtube.com/watch?v=nT-TGvYOBpI
- Required Watching: James Mickens' "Not Even Close: The State of Computer Security" https://vimeo.com/135347162
- Required Reading: "A Disaster Foretold --and Ignored" http://www.washingtonpost.com/sf/business/2015/06/22/net-of-insecurity-part-3/

26 Jan.: Who Will Protect US? A Primer on the US Intelligence Community

- Required Reading: Joint Statement for the Record to the Senate Armed Services Committee, *Foreign Cyber Threats to the United States*, 5 January 2017 (Hon. James R. Clapper, director of national intelligence; Hon. Marcel Lattre, undersecretary of defense for intelligence; and Admiral Michael S. Rogers, USN, commander, US Cyber Command and director, National Security Agency), unclassified, 7 pages.
- Required Reading: Office of the Director of National Intelligence (ODNI), Frequently Asked Questions (FAQ), https://www.dni.gov/index.php/about/faq?tmpl=component&format=pdf
- Required Reading: National Security Agency (NSA), FAQ, https://www.nsa.gov/about/faqs/about-nsa-faqs.shtml
- Required Reading: Scott E. Jasper, "U.S. Cyber Threat Intelligence Sharing Frameworks," *International Journal of Intelligence and Counterintelligence*, Vol. 30, No. 1 (2017), pp. 53-65.

31 Jan.: Networking, 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

2 Feb.: Cryptography
- Tools Used: John the Ripper (password cracker)

4 Feb.: 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

7 Feb.: Malware: Viruses, Worms, Backdoors, Rootkits, and Trojan Horses
- Case Study: http://ntsecurity.nu/toolbox/tini/

9 Feb.: Capture the Flags and Risk Analysis
- Tools Used: Students should bring their laptops and tablets

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

14Feb.: Cyber Crime Targeting Companies and Individuals
- 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.

16 Feb.: Cyber Espionage Targeting Governments, Political Parties, and the Private Sector
- Required Reading: Mandiant Intelligence Center, *Apt1: Exposing One of China's Cyber Espionage Units, 2013* (Alexandria, VA: Mandiant), 78 pages
- Required Reading: "GRIZZLY STEPPE – Russian Malicious Cyber Activity" https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf
- Required reading: GRIZZLY STEPPE Indicators at https://www.us-cert.gov/security-publications/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity

21 Feb.: Counterintelligence and Law Enforcement
- Required Reading: *National Counterintelligence Strategy of the United States of America, 2016* (Washington, DC: National Counterintelligence Executive, Office of the Director of National Intelligence, 2015) p. 20.

23 Feb.: SUBSTITUTE MONDAY'S SCHEDULE ON THURSDAY

28. Feb.: Denial & Deception and Covert Operations in Cyberspace

- Required Reading: Christopher Bronk, and Eneken Tikk-Ringas, "The Cyber Attack on Saudi Aramco," *Survival*, Vol. 55, No. 2 (2013), pp. 81-96.
- Required Reading: Ronald J. Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War," *Security Dialogue*, Vol. 43, No. 1 (2012), pp. 3-24.

2 March: Screening of *Zero Days* (2016)

- In-class screening of *Zero Days* (2016).
- Please note the running time of the film is 1 hour and 56 minutes, while out class session is only 75 minutes. If need to leave at 4 PM, please do so quietly.

7 March: Guest speaker

- Kade Crockford, Director of the Technology for Liberty Program, ACLU of Massachusetts

9 March: NSA Meta Data Collection and Mass Surveillance after the Snowden Leaks

- Required Reading: Loch K. Johnson, Richard J. Aldrich, Christopher Moran, David M. Barrett, Glenn Hastedt, Robert Jervis, Wolfgang Krieger, Rose McDermott, David Omand, Mark Phythian, and Wesley K. Wark, "An INS Special Forum: Implications of the Snowden Leaks," *Intelligence and National Security*, Vol. 29, No. 6 (2014), pp. 793-810.
- Required Reading: NSA Director of Civil Liberties and Privacy Office, "NSA Implementation of Foreign Intelligence Surveillance Act Section 702," in National Security Agency, ed. (Fort Mead, MD: NSA, 16 April 2014) p. 11.

14 March: Guest speaker

- Seth Milstein, Senior Vice President, JP Morgan Chase

16 March: Guest speaker

- Ely Kahn, Co-founder and Vice President, Business Development, Sqrrl; former Director of Cybersecurity, National Security Council (NSC) Staff, 2009-2010

21 and 23 March: SPRING RECESS

28 March: TBA

30 March: Is Cyber War Inevitable or a Chimera?

- Required Reading: Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies*, Vol. 35, No. 1 (2013), pp. 5-32.
- Required Reading: Gary McGraw, "Cyber War Is Inevitable (Unless We Build Security in)," *Journal of Strategic Studies*, Vol. 36, No. 1 (2013), pp. 109-119.

4 April: Cyberspace and Battle Space Operations (Land, Sea, and Air)

- Required Reading: Office of the Secretary of Defense, *DoD Cybersecurity Strategy, 2015* (Washington, DC: U.S. Department of Defense), p. 42.
- Required Reading: Trey Herr and Drew Herrick, “Understanding Military Cyber Operations,” in Richard M. Harrison and Trey Herr, eds., *Cyber Insecurity: Navigating the*

Perils of the Next Information Age (Lanham, MD: Rowman & Littlefield, 2016), pp. 259-276.

6 April: US CYBERCOM and Offensive Cyber Operations

- Required Reading: "U.S. Cyber Command, Beyond the Build: Delivering Outcomes through Cyberspace - the Commander's Vision and Guidance for US Cyber Command, June 3, 2015," in Jeffrey T. Richelson, ed., *National Security Archives Electronic Briefing Book no. 539* (Washington D.C.: 2015) http://nsarchive.gwu.edu/dc.html?doc=2692135-Document-27
- Required Reading: Herbert S. Lin and Taylor Grossman, "The Practical Impact of Classification Regarding Offensive Cyber Operations," in Richard M. Harrison and Trey Herr, eds., *Cyber Insecurity: Navigating the Perils of the Next Information Age* (Lanham, MD: Rowman & Littlefield, 2016), pp. 313-328.

Part III: The Way Forward?

11 April: Can We Make the Internet-of-Things (IOT) More Secure?

- Required reading: Joshua Carman and Beau Woods, "Safer at Any Speed: the Roads Ahead for Automotive Safety Policy," in Richard M. Harrison and Trey Herr, eds., *Cyber Insecurity: Navigating the Perils of the Next Information Age* (Lanham, MD: Rowman & Littlefield, 2016), pp. 47-68.

13 April: Barriers to Partnership between the Tech Community and Government

- Required reading: TBA

18 April: Student Presentations

20 April: Student Presentations

25 April: Student Presentations

27 April: Conclusions

PS 188-02/COMP 50 Calendar of Assignments (Spring 2017)	
Capture the Flag and Risk Analysis	In-Class on 9 February
Personal Engagement Project (PEP)	Distributed on Trunk on: 12 PM on 15 February Deadline for submitting Written Report to Trunk: 5 PM on Monday 1 May (Last Day of Classes) Brief Student Presentations in class on 18, 20, and 23 April
Policy Memorandum	Guidelines Distributed on Trunk: 12 PM on Friday 10 March Deadline for Submission: 12 PM on Friday, 21 April