Title: Cybersecurity and Cyberwarfare

Course Description (Bulletin):
Cross-listed between Department of Political Science and the Department of Computer Science.

Faculty Information:
Jeff Taliaferro, Associate Professor, Political Science
Ming Chow, Senior Lecturer, Computer Science

Course Description:

In spring 2005, a course "Security, Privacy, and Politics in the Computer Age" was offered by the Experimental College. The following was part of the course description:

"New technological innovations also have major political and social implications. Unfortunately, basic knowledge and understanding of the security, political, and social issues concerning the use of technologies is lax, and is a major reason why people are continually affected by computer security breaches and technology misuse. Granted, the problems are only getting worse."

A decade later, those words unfortunately still hold true. Society has become even more reliant on technology and on networked computer systems. The dependence has created greater complexities and more vulnerability. This has led to a spike of exploits and attacks internationally. The magnitude of the problem has propelled cyber security to a national and international security issue.

Jim Waldo, Professor of the Practice and CIO at Harvard University stated, "Despite the magnitude of the problem, the field of cybersecurity strategy, policy, and management remains incipient." There are five goals of this course:

1. Engage International Relations and Political Science students is a sustained discussion on a topic that has transcended to an international security issue.

2. Expose Computer Science and Engineering students to the realm of policy-making, understanding key issues in the strategic management of cybersecurity for the organizations of industry and government.

3. Develop intellectual bridges between students and faculty in International Relations and Computer Science. One of the reasons behind the lack of progress in cybersecurity is because of the technical and non-technical knowledge gap. In addition, partisanship in this country is getting worse: too often, people cannot sit down at the same table to discuss the issues.

4. Encourage the students to be involved, be active citizens. Currently, there is a lack of ownership in educating and informing the public about the politics, risks, and legal issues in technology. Being involved and being bipartisan is the best form of citizenship. Involvement can be as simple as talking to people who are just curious about the issues, to being active in the local, state, or

even federal governments.

5. Engage in constructive and healthy debates, as the issues in cybersecurity are political, complex, and controversial. Students will understand that tradeoffs are necessary in security and privacy.

Prerequisites:
* For International Relations and Political Science students: no Computer Science background is required. PS 61: Introduction to International Relations is recommended
* For Computer Science students: COMP 11 and COMP 15. Some technical and academic maturity is required.

Textbooks:
* None

Grading and Assessment:
* Capture The Flags and Risk Analysis (15 percent)
  * Team-based
  * Understand how software works
  * Learn how to find and exploit vulnerabilities in software (black box)
* Position papers (30 percent)
  * There will be 6 in the class, no more than one page each
  * References must be provided (does not count towards page limit)
* Policy memorandum, not more than 8 pages (25 percent)
* Personal Engagement project (15 percent)
  * Take responsibility for one's own learning
  * Actively engage with a larger community outside the classroom (e.g., a professional group, a conference)
  * Report back to the students and instructors
* Class participation (15 percent)
  * Participate in class debates
  * Ask good and sane questions in class and on Piazza

In order to earn an overall passing grade in the course, students must earn passing grades in all five requirements. In other words, failing or not submitting any one requirement will lead to an overall failing grade in the course. Please plan accordingly.

Course Schedule:

Week 1:
* Topics: How We Dug Ourselves into A Deep Hole, Social Engineering
* Required Reading: "A Disaster Foretold --and Ignored" http://www.washingtonpost.com/sf/business/2015/06/22/net-of-insecurity-part-3/
* Required Reading: "Programmers: Stop Calling Yourselves Engineers" http://www.theatlantic.com/technology/archive/2015/11/programmers-should-not-call-themselves-
* Required Reading: "Verizon 2015 Data Breach Investigations Report (DBIR)" http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-

report-2015_en_xg.pdf
* Required Reading: "United States. Executive Office of the President. Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communication Infrastructure. May 2009." http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
* Required Watching: James Mickens' "Not Even Close: The State of Computer Security" https://vimeo.com/135347162
* Required Watching: Dan Geer's keynote at the Black Hat 2014 Conference https://www.youtube.com/watch?v=nT-TGvYOBpI

Week 2:
* Topics: Networking, the World Wide 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

Week 3:
* Topic: Cryptography
* Tools to be Used: John the Ripper (password cracker)

Week 4:
* Topic: Vulnerabilities, 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 http://tuftsdev.github.io/DefenseOfTheDarkArts/notes/predicting_the_future_veracode.pdf
* 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

Week 5:
* Topic: Malware (Viruses, Worms, Backdoors, Rootkits, Trojan Horses)
* Case Study: tini http://ntsecurity.nu/toolbox/tini/

Week 6:
* Topic: Is Cyber War Inevitable or a Chimera?
* Required Reading: Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," International Security, Vol. 38, No. 2 (2013), pp. 7-40.
* 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.
* Required Watching: PBS Frontline, “The Cyberwar Threat” (53 minutes), originally aired 15 October 2015 http://www.pbs.org/wgbh/nova/military/cyberwar-

threat.html

Week 7:
* Topic: NSA Electronic Surveillance and Individual Privacy
* 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: GPO, 2014) p. 11. https://www.nsa.gov/public_info/_files/speeches_testimonies/NSAImplementationofFISA70216Apr2014.FINAL.pdf

Week 8:
* Topic: Cyberespionage targeting Government and the Private Sector
* Required Reading: Permanent Select Committee on Intelligence, House of Representatives, Cybersecurity Threats: The Way Forward (Witness: Admiral Michael Rogers, Commander, U.S. Cyber Command and Director, National Security Agency), 20 November 2014.
* Required Reading: Jon R. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," International Security, Vol. 39, No. 3 (2015), pp. 7-47.
* Required Reading: Mandiant Intelligence Center, Apt1: Exposing One of China's Cyber Espionage Units, 2013 (Alexandria, VA: Mandiant), p. 78.

Week 9:
* Topic: Denial & Deception (D&D) 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.

Week 10:
* Topic: Deterrence in Cyberspace
* Required Reading: Paul K. Davis, "Deterrence, Influence, Cyber Attack, and Cyberwar," New York University Journal of International Law and Politics, Vol. 47, No. 2 (2015), pp. 327-355.
* Required Reading: Thomas Rid, and Ben Buchanan, "Attributing Cyber Attacks," Journal of Strategic Studies, Vol. 38, No. 1-2 (2015), pp. 4-37.

Week 11:
* Topic: Cyberspace and Battle Space Operations (Land, Sea, and Air)
* Required Reading: The Joint Staff, "Joint Publication 3-13: Information Operations " in Joint Chiefs of Staff, ed., 27 November 2012, Incorporating Change 1, 20 November 2014 (Washington, DC: Department of Defense, 2012) p. 89.
* Required Reading: Office of the Secretary of Defense, DoD Cybersecurity Strategy, 2015 (Washington, DC: U.S. Department of Defense), p. 42.

Week 12:

* Topic: Counterintelligence
* Required Reading: National Counterintelligence and Security Center, "National Counterintelligence Strategy of the United States of America, 2016," in Office of the Director of National Intelligence, ed. (Washington, DC: National Counterintelligence Executive, 2015) p. 20.
* Required Reading: Aaron F. Brantly, "Cyber Actions by State Actors: Motivation and Utility," International Journal of Intelligence and Counterintelligence, Vol. 27, No. 3 (2014), pp. 465-484.

Week 13
* Topic: Conclusions