COMP 50 / PS 188: Cyber Security and Cyber Warfare

Tufts Innovates Grant 2016

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

The Course's Mission: To develop intellectual bridges among students and faculty members in the Computer Science, Political Science, and International Relations. We are convinced that the lack of progress in cyber security is due to knowledge gaps between the technical community and policymakers / non-technical community.

Course Goals

1. To engage Political Science (PS) and International Relations (IR) undergraduates in a sustained discussion of the technical aspects of cyber security and cyberwar, which have emerged as major aspects of international relations and United States national security.
2. To expose Computer Science (CS) undergraduates to the realm of policymaking and to help them understand key issues in strategic management of cyber security in the private sector and in government.
3. To encourage students to be engaged citizens; to inform and discuss the political, legal, and ethical aspects of cyberspace with the public.
4. To engage in constructive and healthy debates, as the issues in cyberspace are political, complex, controversial, and have tradeoffs.

Assignments

- **Capture The Flag (CTF)** - A *team-based exercise* to find and exploit vulnerabilities in a system (unpatched Windows Server 2008) to gain access to information one should not have access to.
- **Policy Memorandum** - A policy memorandum on a pressing issue in cyber security directed to a information technology (IT) company, an intelligence agency, a congressional committee, or senior executive branch policymakers.
- **Personal Engagement Project** - An *open-ended* project for students to *actively engage* with the cyber security and policy community outside of the classroom as the field is very broad.

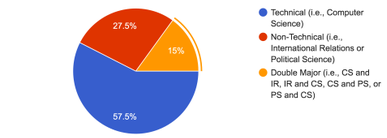
Topics

- Basic Networking
- Security tools including nmap, SHODAN, whois, Metasploit, Kali Linux
- Vulnerabilities and Vulnerability Disclosure
- Common Vulnerabilities and Exposures (CVE) and Common Weakness Enumeration (CWE)
- Exploitation
- Malware and Zero Days
- Privacy and Surveillance
- US Intelligence Community
- Cyber Crime
- Espionage
- Counterintelligence and Law Enforcement
- Denial and Deception
- Covert Operations
- Cyber War

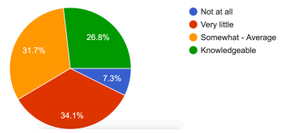
Outcomes

47 students total in inaugural class. We asked students to complete a survey at the end of the course. 40 total responses.

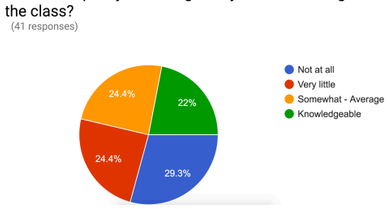
What is your first major? (40 responses)



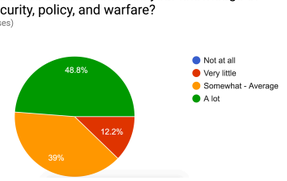
How much cyber security knowledge did you have coming into the class?
(41 responses)



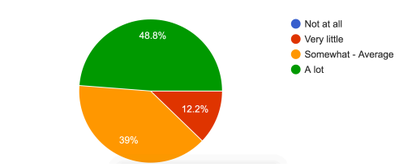
How much policy knowledge did you have coming into the class?
(41 responses)



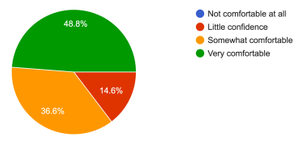
Do you feel this course enhanced your knowledge of cyber security, policy, and warfare?
(41 responses)



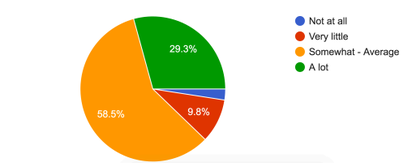
Do you feel this course enhanced your knowledge of cyber security, policy, and warfare?
(41 responses)



How comfortable do you now feel talking to students outside your first major about cyber security and policy?
(41 responses)



One of the goals of this course was to have students become comfortable working with others from different academic backgrounds. Do you feel that you learned from each other in this course?
(41 responses)



What We Learned

- The idea of cyber warfare is not that special. While the techniques are unique, many ideas are similar to traditional warfare. The word "cyber" should be dropped.
- Very difficult to keep up with current events and new readings every day.
- There is a problem with vocabulary in this field. Many words have different context to different groups in this field.

Improvements To Be Made

1. Need more assignments, perhaps small labs.
2. Incorporate an event similar to the Atlantic Council Cyber 9/12 Student Policy Competition into the class.
3. Add a second team based project (in addition to CTF), with each team comprised of IR/PS and CS students.
4. Have more in-class debates on topics such as vulnerability disclosure.

Future Works

1. Develop additional undergraduate courses dealing with specific aspects of cyber security and policy.
2. Make this a required course in future graduate degree program in cyber security and policy at Tufts.
3. Publications and talks on our work to International Relations and Political Science forums and journals.

Special Guests and Acknowledgements

- Matt Weinberg, Teaching Assistant
- Kade Crockford, Director of Technology for Liberty Program at ACLU of Massachusetts. Guest lecture on Tuesday, March 7th. Topic: Surveillance and Privacy (social media surveillance by local, state, and federal law enforcement agencies)
- Ely Kahn, Co-Founder / VP Business Development and Marketing at Sqrrl. Guest lecture on Thursday, March 16th. Topic: Cyber Defense: Past, Present, and Future
- Seth Milstein, Vice President at JP Morgan Chase & Co. Guest lecture on Tuesday, April 4th. Topic: Cyber Security in Public vs Private Sectors