

**Cybersecurity and International Relations**

Spring 2016

<table>
<thead>
<tr>
<th>Instructor:</th>
<th>John Savage</th>
<th>Time:</th>
<th>MW 3:00 – 4:20</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email:</td>
<td><a href="mailto:John_Savage@brown.edu">John_Savage@brown.edu</a></td>
<td>Place:</td>
<td>CIT 368</td>
</tr>
</tbody>
</table>

## Contents

1. Overview of Writing Assignments  
2. Grading Policies  
   2.1 Grading Rubric  
   2.2 Academic Honesty  
   2.3 Late Days  
   2.4 Contesting a Grade  
3. Labs  
   3.1 Times and Locations  
   3.2 Lab Topics  
4. The Elements of Style  
5. Short Analysis Paper  
6. Group Project  
   6.1 Group Project Grading Rubric  
7. Midterm Assignment  
8. Final Assignment  
   8.1 Proposal  
   8.2 Project Description  
   8.3 Rubric
1 Overview of Writing Assignments

The course will have five types of assignments: analysis papers, lab sections, a group project, a midterm paper, and a final research paper. For elegant writing, please see: The Elements of Style.

Assignments:

1. Analysis Papers
2. Class Participation and Lab Sections
3. Group Project
4. Midterm Project
5. Final Research Paper

2 Grading Policies

2.1 Grading Rubric

<table>
<thead>
<tr>
<th>Grading Rubric</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 Short Analysis Papers</td>
</tr>
<tr>
<td>Group Project</td>
</tr>
<tr>
<td>Midterm Paper</td>
</tr>
<tr>
<td>Final Paper</td>
</tr>
<tr>
<td>Discussion</td>
</tr>
</tbody>
</table>

2.2 Academic Honesty

We adhere strictly to Brown’s Academic Code. Please see here for detailed information. Violation of the Academic Code can result in some or all of the punishments detailed by the university. Note: Copying from your own previously submitted work is also considered a form of plagiarism and will be handled accordingly.

2.3 Late Days

Every student will get 3 late days for the semester, which may be used at their own discretion. You do not need to inform us when you are using a late day, we will distribute your late days at the end of the semester to maximize your grade. Assignments more than three days late will not be graded. Assignments will be lowered one letter grade for each day that they are late when you do not use a late day. Late days may not be applied to the final.

2.4 Contesting a Grade

You are encouraged to look over your papers after they have been graded. If you have any questions regarding your grade, please visit your grader during their TA hours.
3 Labs

Expectations: For each lab, you will be expected to bring in a short written summary (1-2 paragraphs) on the selected readings as well as two discussion questions. You must print or write these out and bring in a physical copy to your assigned lab section. These deliverables will count for 50% of your lab/participation grade and will be graded mostly on completion (though TAs reserve the right to not accept assignments that display inadequate effort).

Attendance Policy: You must attend the lab section you were assigned at the beginning of the semester. If you must attend another lab, you need to give the TAs 24 hour notice prior to your scheduled lab to approve the lab switch. To ask for day of approval, you must specifically write to the Head TAs and explain your situation.

3.1 Times and Locations

<table>
<thead>
<tr>
<th>Time</th>
<th>Location</th>
<th>TAs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monday 12-1</td>
<td>Solomon 004</td>
<td>Jared &amp; Celina</td>
</tr>
<tr>
<td>Tuesday 1-2</td>
<td>CIT Library</td>
<td>Nick &amp; Sachin</td>
</tr>
<tr>
<td>Wednesday 11-12</td>
<td>Sayles 300</td>
<td>Ali &amp; Zoe</td>
</tr>
<tr>
<td>Thursday 4-5</td>
<td>CIT 316</td>
<td>Maddie &amp; Zoe</td>
</tr>
<tr>
<td>Friday 2-3</td>
<td>CIT Library (410)</td>
<td>Nat &amp; Luke</td>
</tr>
</tbody>
</table>

3.2 Lab Topics

These are the topics for each lab, with links to their readings:

1. February 8th - 12th: Hacktivism and Ddos Readings:
   (a) The Rise of Hacktivism
   (b) The Cyber Activist who wants to Shut down ISIS
   (c) Anonymous, Gamergate and the impossible dream of vigilante justice

2. February 15th - 19th: Psychological Hacking and Social Engineering
   (a) Consider the Catfish
   (b) Fallout from Recent Spear Fishing Attacks
   (c) In cyberattacks, hacking humans is highly effective way to access systems

3. February 29th - March 4th: The Dark Web
   (a) What is the Dark Web?
   (b) The Darknet: Is the Government Destroying ‘the Wild West of the Internet?’
   (c) The Silk Road (Optional)

4. March 7th - March 11th: Mid Semester Project Info and Legislation
   (a) The Problems CISA Solves: ECPA Reform in Disguise
   (b) CISA in Context: Privacy Protections and the Portal
5. March 14th - March 18th: Cybercrime and Cybereconomics:
   a) How you could become a victim of cybercrime in 2015
   b) Cyber Crime Still on the Rise, Using Nine Basic Attack Methods
   c) Why your cyber insurance investment may not pay off
   d) Video: Hackers Remotely Kill a Jeep on the Highway With Me in It

6. March 21st - March 25th: Open TA Hours for Design Checks

7. March 28th - April 1st: SPRING BREAK

8. April 4th - April 8th: Internet Governance (Wasserman Arrangement)
   a) What Is Internet Governance?
   b) Internet governance too US-centric, says European commission
   c) Why the ITU is the wrong place to set Internet standards
   d) Internet governance: What if the sky really is falling?

9. April 11th - April 15th: Cyberwar
   a) Mysterious 08 Turkey Pipeline Blast Opened New Cyberwar
   b) Americas secret arsenal

10. April 18th - April 22nd: Political Protest and the Internet
    a) Why Did the Twitter Revolutions Fail?
    b) The truth about Twitter, Facebook and the uprisings in the Arab world

11. Week 13 April 25th - April 29th: Final Paper Q&A
4 The Elements of Style

"Analogies in science writing are like forklift trucks when used correctly they do a lot of heavy lifting, but if you don’t know what you’re doing you’ll quickly drive them into a wall of laboured metaphors and cause some major damage” – Jacob Aaron

1. Condescension
   (a) Even though you should assume no technical sophistication from your reader, you should still explain concepts in a respectful way with the assumption that your reader is intelligent.

2. Boring
   (a) At times it is critical to discuss minute technical details but that is no excuse for writing an uninteresting piece. Make sure to revise your explanations so that they still engage your reader.

3. Weak Writing
   (a) Never use I, Stuff, Got, Thing(s), Went
   (b) Sparingly use Is, Was, Are
   (c) Avoid weak words such as Big, Small, Important, In Love With, Interesting
   (d) Cut excessive adverbs and adjectives
      i. Introduced a new
      ii. Absolutely necessary
      iii. Extremely critical

4. Keep It Simple
   (a) "President Obama collaborated with the International Telecommunications Union” sounds much better than "Barack Obama, President of the United States of America, worked both collaboratively and synchronously with the International Telecommunications Union.”

5. Cite Liberally
   (a) Even if you paraphrase, site it

6. And . . .
   (a) Oxford commas can clarify sentence structure
   (b) Every paragraph should have a unifying idea
   (c) Every sentence should provide new information or analysis
   (d) Always proofread
5 Short Analysis Paper

Cybersecurity and International Relations is a course designed to encourage computer scientists to think about policy and international relations issues, and to encourage political scientists to consider issues rooted in technology. Throughout the semester, students are required to submit 5 short papers in response to the week’s readings, contributing their own analysis of the piece. Students are required to turn in papers according to the due dates listed on the course website, with the responses referring to the readings available between response dates.

Criteria for grading:

1. Please do not use the first person (“I”) in your papers. For example, we will mark you down if you say, “I believe that...”.

2. 3 - 4 pages double spaced

3. 1 inch margins, 12 pt. standard font (Times New Roman, Cambria, Arial)

4. Only respond to one required reading (Do not respond to optional or lab readings)

5. Strong argument throughout, with an original thesis (not restating an author’s position) that incorporates the student’s knowledge of the subject.

6. Correct citations when referring to the text. In line citations or footnotes are fine, just be consistent. Use of outside sources is discouraged. If they are used, please include a bibliography.

7. Use of academic language. Avoid colloquial or informal language.

8. You are welcome to LaTex your papers!

These papers aim to have students think critically about the readings, not regurgitate facts or opinions. As a WRIT designated course, TAs will grade on the above listed criteria, and provide feedback on the writing style. Feel free to use the Writing Center and other resources to receive help as well.
6 Group Project

A group project will be assigned approximately one third of the way through the course. The goal is to plan an emergency response to a cybersecurity crisis. Each project team will consist of 4-7 students with a mixture of computer science and policy knowledge. Each team will make a five-minute presentation to the class. The project will represent 10% of the course grade.

You may either submit one full report, minimum 5 pages double spaced, that addresses both policy and technical issues. Or, you may choose to submit separate policy and technical reports, which together should be minimum 5 pages. **We will accept longer submissions** - but try your best to be concise!

6.1 Group Project Grading Rubric

<table>
<thead>
<tr>
<th>Deliverables</th>
<th>25%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Addresses Policy Issues</td>
<td></td>
</tr>
<tr>
<td>Addresses Technical Issues</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Presentation</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Description of problem</td>
<td>10%</td>
</tr>
<tr>
<td>Tech and policy responses</td>
<td>20%</td>
</tr>
<tr>
<td>Effectiveness in response to questions</td>
<td>20%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bonus Points (10% MAX)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Being in character</td>
<td>5%</td>
</tr>
<tr>
<td>Asking tricky questions to other teams</td>
<td>5%</td>
</tr>
</tbody>
</table>
7 Midterm Assignment

You have two options for the midterm assignment:

1. Critical Infrastructure
2. Encryption Midterm
8 Final Assignment

8.1 Proposal

The final research paper will allow students to critically engage with a cybersecurity topic of their choosing, completing a 10-12 page research paper. This paper will require students to research using academic sources, cybersecurity blogs, and other news sources. Please look over the Final Research Paper Description for a full understanding of what is expected from this assignment. In order to help you begin thinking about your topic and potential sources, please prepare a one-page double-spaced proposal. This proposal should include the following:

1. A description of your proposed topic and its relevance to cybersecurity and international relations.
2. Supporting material and additional points you expect to cover in your research paper.
3. A bibliography (Chicago Manual of Style format) of at least one strong academic source and several other sources you expect to use in your paper. This does not need to be your full bibliography, but should reflect a strong preliminary research effort.

This should not be an exhaustive description, but rather show a clear focus and understanding of your topic and how you want to tackle it. If you take this proposal seriously, you should have a strong start to the paper. Feel free to discuss potential topics with the TAs and ask questions if you need assistance with how to approach a research paper or proposal. You may also consult the Writing Center for additional help if necessary.

8.2 Project Description

The final research paper is designed to allow students to think critically about an issue or concept related to international relations and cybersecurity that they would like to research further. While the paper can expand upon course material and previous assignments, it should also include academic sources, news articles, and other vetted sources that could provide supplementary information about the chosen topic. The instructor and TAs will be available to discuss potential topics, and they should approve all final topics. The deadline of May 6th is final late final papers will not be accepted (so make sure to use your late days before the final paper!)

Criteria:

1. 10-12 pages long, double-spaced.
2. 1-inch margins, 12 pt. standard font (Times New Roman, Cambria, Arial).
3. Strong argument throughout, with an original thesis that incorporates the student’s knowledge of the subject and addresses a greater concern.
4. Correct citations when referring to texts and other sources - in line citations or footnotes are fine please use the Chicago Manual of Style format.
5. A full bibliography of all sources this should include all bibliographical information, rather than urls. Any non-academic sources will be judged on their legitimacy and usefulness to the overall argumentation use of non-academic sites is discouraged. Feel free to use readings from the course, but again, cite them!
6. Reasonable use of academic sources to justify your argument. We are hesitant to set a minimum number of sources, but will use our discretion.
7. Academic language - avoid colloquial or informal language.
8. Proper section divisions to help with the flow and argumentation of the paper.

Because this is a research paper, we would like students to include a variety of sources. Cybersecurity blogs, news media, and national and international governmental and non-governmental reports can be useful assets in formulating arguments with up-to-date information. Academic journals, resource books, and other publications are also useful sources feel free to access sites such as jstor.org and online journals provided through the Brown University Library. If you need help finding sources, please talk to the TAs or a librarian (depending on what you need help with).

Potential topics (to consider, do not feel you need to write on any of these unless you wish to):

1. Methods for reducing the level of cybercrime
2. Establishing norms of governance on the Internet
3. How to mitigate international risk in cyberspace
4. Assess risk of catastrophic attacks on critical infrastructure
5. Differences in approach to cybersecurity by region (USA vs. Asia, European Union, etc)
6. Impact of commercial cyber-espionage on economies
7. Freedom of expression in different governmental regimes
8. Infrastructure and security needs in developing economies and regions
9. Implications of current events topics for future legislation

8.3 Rubric

This is the rubric for the final assignment:

1. Final Project Rubric