Cybersecurity for Future Presidents: An Interdisciplinary Non-majors Course

Aparna Das, David Voorhees
Le Moyne College
dasa, voorhedp @lemoyne.edu

Cynthia Choi
Le Moyne College
choicc@lemoyne.edu

Carl E. Landwehr
Le Moyne College
carl.landwehr@gmail.com

ABSTRACT

We discuss the design and implementation of an interdisciplinary non-majors course *Cybersecurity for future presidents,* which broadens the types of computational courses available for non-majors. The goal of our course is to build awareness of cybersecurity issues and to promote thinking critically about them. Student debates on controversial cybersecurity issues facing society today motivate the technical and policy content. We present student assessment results, which demonstrate an increase of students' awareness, and outline directions for future course improvements.

CCS Concepts

• Security and Privacy→Human and societal aspects of security and privacy • Social and professional topics→ Computing / technology policy→Privacy policy, Computer crime, Government technology policy.

Keywords

Computer Science Education; Computing and Society; Security Policy.

1. Introduction

Cybersecurity focuses on protecting computers and data from unintended or unauthorized access. Our digital connectivity and the pervasiveness of digital applications that store and share data brings risk of theft, fraud and abuse. This makes cybersecurity an urgent and ongoing need.

In April 2015, President Obama declared a national emergency to deal with "the increasing prevalence and severity of malicious cyber-enabled activities" which he stated "constitute an unusual and extraordinary threat to the national security, foreign policy and economy of the United States" [1]. Further evidence of the urgency of cybersecurity issues is found in the Global Risks 2015 report published by the World Economic Forum (WEF) which states that "90 percent of companies worldwide recognize they are insufficiently prepared to protect themselves against cyber attacks" [2]. The department of homeland security's webpage also calls out the need for more cybersecurity education: "America needs well trained professionals working in cybersecurity roles. These professionals are critical in both private industry and the government for the security of individuals and the nation."

Given the growing need for cybersecurity, future leaders of government and industry, who may not have a computational background, will nevertheless need to understand the science, technology, and human considerations to make informed decisions about cybersecurity issues. Citizens also need the tools to understand and evaluate the actions of future leaders in the area of cybersecurity. As one response to such demand, we developed and taught an interdisciplinary course that aims to build awareness of cybersecurity issues and understanding of fundamentals of technology. Our course goal is to study the foundations of cybersecurity from technical and policy-oriented perspectives while thinking critically about cybersecurity issues.

Our course broadens the types of computational courses available for non-majors. There are computer literacy courses that may cover best practices of being safe and secure online [3], and non-majors courses that teach programming [4]. However, we have not seen any examples of courses with our intended objective. The interdisciplinary nature of cybersecurity and its growing importance in society makes it an appealing way to introduce computational topics to non-majors. Through studying cybersecurity, students are introduced to several fundamental computer science concepts including digital representation of information, data encryption, time complexity, packet switching networks, distributed computing and big data sets. The coverage of cybersecurity in news and the personal cybersecurity breaches that many students have experienced makes cybersecurity an engaging topic to approach these deep computational concepts.

In this paper, we focus on the course design and implementation of the second offering of this course taught during spring 2016. The organization of our paper is as follows: In section two, we discuss course design including learning objectives and the course format. In section three, we discuss in class debates were used as an instructional strategy. Section 4 discusses our methods and results for assessing student learning and Section 5 discusses lessons learned.

2. Course Design

The vision of our course comes from Richard Muller's *Physics for future Presidents,* a popular course at U.C. Berkeley which teaches physics to non-majors by demonstrating its connections to issues like terrorism, energy, and climate change [5]. Our course is similarly designed to encourage the participation of a broad and diverse student population in cybersecurity education and motivates topics using current real world concerns.

The CS faculty collaborated with Carl Landwehr, a leading expert in cybersecurity, to design the content of the course and to teach the course during two semesters (Spring 2015 and 2016). We were concurrently involved in infusing cybersecurity topics throughout relevant CS courses for majors, which were lacking in our program. During this transition period, CS majors were allowed to take the cybersecurity course to fill some of the gaps in their security knowledge. However, the cybersecurity course was

SIGCSE '17, March 08-11, 2017, Seattle, WA,USA
© 2017 ACM. ISBN 978-1-4503-4698-6/17/03$15.00
DOI: http://dx.doi.org/10.1145/3017680.3017713

designed to be a non-majors course and will be limited to non-majors and minors for future course offerings.

As cybersecurity is the product not only of technology developments, but also of economic, societal and political factors that drive the deployment and use of technology, our course presents topics from these perspectives and fulfilled the interdisciplinary course requirement that students complete as part of our College's core curriculum.

2.1 Course content

The course content is posted at web.lemoyne.edu/dasa/incubate. While the materials were developed by a leading cybersecurity expert, computer science instructors with moderate security expertise should be able to use this material to lead a similar course.

The course had three learning objectives which are listed in Table 1. These objectives align with the educational goals for non-computer science students delineated in a final report on education in secure software [6]. The first two focus on raising awareness of cybersecurity foundations from both the technical and societal/policy perspectives. The third objective is to provide students with opportunities to practice critical thinking about cybersecurity issues. Roughly a third of the time was spent on each goal.

Topics mapping to each learning objective are shown in Table 1. The technical foundations topics (learning objective #1) focused on building an understanding of how cybersecurity threats work and the capacity and limitations of cyber defenses. The policy topics (learning objective #2) focused on understanding relevant regulations including those pertaining to surveillance (for law enforcement and national security), individual privacy, development of secure software, and intellectual property. Economic and societal factors which govern the development of software and use of cybersecurity were also discussed. Students practiced critical thinking (learning objective #3) by participating in debates on controversial cybersecurity issues that society is currently facing, such as whether or not cell phone manufacturers should be required to provide law enforcement with back doors to access encrypted data on customer phones. The critical thinking column of Table 1 lists all debate resolutions. The debates required students to draw upon the technical and policy knowledge to reason about the different viewpoints.

Brian Kernighan's *D is for Digital* was used as the textbook for the majority of the technology topics [7] and various articles were used to cover the policy topics. Students were also required to watch and review debates available from Intelligence Squared [8].

2.2 Course Format

The course met twice a week throughout a 15-week semester. Carl Landwehr as the cybersecurity expert was the lead facilitator for the first session each week where students generally learned aspects of the technical and policy foundations of cybersecurity. The second weekly session was used to review technical foundational topics and was led by the College's CS faculty. This format was chosen to maximize content delivery from the primary instructor, Carl, who was only visiting our College once a week.

All course topics were organized around five in-class student debates which were dispersed throughout the semester. Debates were held roughly every other week after an initial three week period. The lectures prior to each debate focused on both the technology and policy topics which were most relevant to the upcoming debate. Thus debates gave motivation and purpose for learning the foundational topics by making connections to real world concerns. As an example, the first debate was held on week 4 and concerned whether law enforcement should have legal access to a back door for encrypted data. The technical concepts covered prior to this debate were: data representation - how is data stored digitally?; encryption - how is data encrypted and how hard it is to break?; and, packet switching networks - how are messages passed in a network and how does wiretapping work? In terms of policy, students learned the current laws governing search and seizure, wiretapping and for obtaining warrants. The differences in objectives and policies for law enforcement versus foreign surveillance were also discussed.

3. Debates

In-class debates were the primary tool used to provide students with opportunities for critical thinking (learning objective #3) and were used to motivate the foundational concepts. This section describes the format of these debates.

3.1 Resolutions

Debate resolutions were chosen from prevalent cybersecurity issues which involved thinking about both policy and technology. See Table 1's, critical thinking column, for the resolutions used in the most recent course. Since debates were dispersed throughout the semester care had to be taken to ensure that resolutions were ordered so that the technical and policy background required for each debate increased gradually at the pace of student learning.

3.2 Debate Format

Students worked in teams of three to support either the pro or con side of a resolution. The following debate format was used:

- Opening Arguments Pro #1, Con #1, 10 mins per side
- Prep Time to confer with team, 3 mins total
- Rebuttals:Pro#2,Con #2, 10 mins per side
- Prep Time to confer with team, 3 mins total
- Closing arguments: Pro #3, Con #3, 10 mins per side
- Questions from audience: one per debater, 15 mins

The debate format required each debater to have a speaking role and answer at least one audience question.

Prior to a debate each team prepared a position paper which presented arguments to support their side of the resolution and addressed each of the four perspectives taken from the NRC report *The Nexus of Cybersecurity and Public Policy:* (1) economic; (2) innovation; (3) civil liberties, and (4) international relations / national security / law enforcement [9].

Students not participating in the current debate (the audience members) read about both sides of the issue and documented arguments they found most convincing. Each non-debater also submitted an insightful question for each side.

3.3 Debate Assessments

Each debater received three grades: one for the position paper; one for their debate performance; and one for their ability to work well with their teammates.

The first two grades were assessed by the instructor. The position paper was graded for the team as a whole, but debate performance was assessed individually. See Table 2 for rubrics used. For the last grade each debater assessed how well their group worked together by splitting a total of 100 point between each member of their group including themselves. This additional assessment was introduced after the first two debates as several students complained of group members not contributing equally to writing the position paper. Non-debaters questions and arguments was graded by instructors using the rubric shown in Table 3.

Table 1. Course Learning Objectives and Topics

Technical Foundations **(Objective #1)**	**Policy Foundations** **(Objective #2)**	**Critical Thinking** **(Objective #3)**
Be able to explain fundamental concepts of computing and cyber security, including information theory, computability, cryptography, authentication, access control, information flow, anonymity, privacy, accountability, how vulnerabilities arise and how attacks work.	Be able to explain relevant laws, policies, societal and market forces that will continue to shape policy surrounding cyber security and privacy.	Be able to apply their understanding of technology and policy to assess critically arguments put forth in favor of alternative policy positions.
Topics – Background		
- Data Representation - Digital vs. Analog - Bit Manipulations - Basic computer architecture - Security Mechanisms (access control - Examples of attacks: Denial of service, inputs, supply chain, side channel, social engineering, network /system configuration, buffer overflow	- Government's role in cybersecurity - Economic influences -Cyber warfare	
Topics – Preparation for Debate 1		
- Cryptography - Packet Switching networks	- Foreign and domestic policies on surveillance and wiretapping policies - Encryption policies - History of legislation, court cases -intellectual property	*Debate 1*: The U.S. government should mandate that communication and storage technology providers include a mechanism by which protected data (including encrypted data) can be obtained under lawful court order.
Topics – Preparation for Debate 2		
- Cybersecurity Foundations - Balancing security goals	- Privacy policy	*Debate 2*: The US should adopt the E.U. "right to be forgotten" online.
Topics – Preparation for Debate 3		
- Mechanisms for accountability, Authentication, authorization -Forensics -Crypto tools for elections	- Current voting process - Policies related to elections - requirements for electronic voting systems	*Debate 3*: The U.S. Election Assistance Commission should promote internet voting for public elections on a model similar to Estonia.
Topics – Preparation for Debate 4		
- Nature of genomic data - Uses/ benefits of genomic data - Potential abuses of genomic data	- Regulations for genomic data	*Debate 4:* Commercially stored genomic data requires no further government regulatory controls.
Topics – Preparation for Debate 5		
- Cryptographic hashing - Block chains - Anonymity: Onion routing - Digital currencies - Byzantine agreements		*Debate 5* Bitcoin transactions are better for consumers than credit card transactions.

Table 2. Rubrics for Debaters

Position Paper				
Criteria	**20 points**	**15 points**	**10 points**	**5 points**
Addresses Issues	Arguments clear and convincing	Arguments are sometimes clear and convincing	Arguments are rarely clear and convincing	Arguments are never clear and convincing
Support with Facts	Uses many facts that support topic	Uses some facts that support topic	Uses few facts that support topic	Does not use facts that support topic
Persuasiveness	Arguments clear and convincing	Arguments are sometimes clear and convincing	Arguments are rarely clear and convincing	Arguments are never clear and convincing
Writing	Clear and concise	Mostly clear and concise. Few minor flaws.	Somewhat clear and concise. Many minor flaws or a major flaw.	Not clear and concise; A few major flaws
Organization	Structure is logical; Transition sentences help connect topics; Progression of ideas evident	Structure is logical but a bit faulty; Transition sentences may be missing for a few topics; Progression of ideas exists but a bit faulty	Structure is partly logical and partly random; Transition sentences may be missing for a many topics; Progression of ideas exists but faulty	Structure is mostly random; Transition sentences are lacking; Progression of ideas does not exist
In class Debate				
Addresses Issues	Always addresses topic	Usually addresses topic	Rarely addresses topic	Did not address topic
Support with Facts	Uses many facts that support topic	Uses some facts that support topic	Uses few facts that support topic	Does not use facts that support topic
Persuasiveness	Arguments clear and convincing	Arguments are sometimes clear and convincing	Arguments are rarely clear and convincing	Arguments are never clear and convincing
Teamwork	Used team member effectively; Equal timing	One member does the talking 75% of the time	One member does the talking 100% of the time	No one talks
Organization	Electrifies audience in opening statement Closure convinces audience	Grabs attention; Brings closure to the debate	Introduces topic and brings some closure to the debate	Does not introduce topic; no closure

Table 3. Rubric for Non Debater Preparation

Criteria	**20 points**	**16 points**	**10 points**	**0 points**
Arguments: Connection to debate topic	Clear connection to topic	Mostly connected to topic	Somewhat connected to topic	Partial or no answer submitted
Arguments: writing Style	Clear and concise	Mostly clear and concise; many minor flaws or a major flaw	Somewhat clear and concise; a few major flaws	Partial or no answer submitted
Questions: connection to debate topic	Clear connection to topic	Mostly connected to topic	Somewhat connected to topic	No question submitted
Questions: insightful	Solid understanding of topic	Mostly understanding of topic	Somewhat of an understanding of topic	No question submitted
Questions: writing style	Clear and concise	Mostly clear and concise; many minor flaws or a major flaw	Somewhat clear and concise; a few major flaws	No question submitted

4. Assessing Student Learning

For the spring, 2016 (second) course offering, we administered a pre-survey during the first week of the course and a post-survey during the last week of the course. The purpose of this survey was to gauge changes in student awareness of the cybersecurity topics covered in the course. The pre-survey was taken by 31 students and the post-survey by 30. The survey (see Table 4) asked students to rate their own level of knowledge of 25 cybersecurity topics on a scale from 0-3 where 0 corresponded to "none", and 3 corresponded to "a great deal". Ratings of 0 or 1 are characterized as a low level of knowledge and 2 or 3 are characterized as having some familiarity. Table 4 shows survey topics clustered by course learning objective. For each topic it gives the % of students assessing as having some familiarity.

In the pre-survey, at least half of the students (15 or more) reported their knowledge as low in 20 of the 25 cybersecurity topics. Of the 5 remaining cybersecurity topics, only the first topic – meaning of "cybersecurity" – had over 65% of students reporting some familiarity.

In the post-survey, at least 22 out of 30 students reported some familiarity with each of the 25 topics covered in the survey. In fact, 90% or more of the students reported having some familiarity with 19 of the 25 topics.

Looking at the topics clustered along learning objectives, the eleven technical foundational topics (1 to 11) show positive results in the post-survey. Ninety percent or more of the students felt they had some familiarity with all topics except topic 3 (networks), where only 73% of students felt they had some familiarity.

Table 4. Student Self Assessment

% Students reporting some familiarity (ratings 2 and 3)		
	Pre	**Post**
Technical Foundations Topics		
1. The components of a computer	58	90
2. How information is encoded in computers to reflect numbers, colors, sounds, instructions	58	100
3. How computer networks function	35	73
4. The fundamentals of cryptography	13	93
5. Why cryptography is important	29	97
6. How authentication maintains cyber security	29	93
7. How cyberattacks occur	42	97
8. The meaning of privacy in cyber security	55	93
9. The meaning of anonymity in cyber security	52	90
10. Meaning of accountability in cybersecurity	52	93
11. Relationship among privacy, anonymity and accountability	32	97
Policy Foundations Topics		
12. The types of U.S. Government agencies and their role in cyber security	39	77
13. How intellectual property relates to cyber security	32	87
14. The incentives in government that influence cyber security	29	83
15. The incentives in business that influence cyber security	35	90
16. The incentives in society that influence cyber security	32	90
17. Existence of public policies that govern cyber security	26	80
18. The nature of cyberwarfare	26	100
19. How cyber security issues impact international relations	35	93
Critical Thinking /Debate Topics		
20. Issues surrounding the use of computers for electronic voting	13	93
21. Issues surrounding the use of digital currencies	29	97
22. Privacy issues surrounding genomic information	13	87
Miscellaneous Topics		
23. The meaning of "cyber security"	90	100
24. How cyber security issues affect me as an individual	61	97
25. What cyber security issues may confront future Presidents.	39	93

The eight policy foundational topics (12 to 19) show mixed results in the post-survey. Ninety percent or more of the students had some familiarity with incentives in business and incentives in society (15, 16) and about cyberwarfare and international relations (18, 19). The other four policy topics – government agencies (12), intellectual property (13), incentives in government (14) and public policies (17) – had 77%, 87%, 83% and 80% of students with some familiarity, respectively. The 77% is perhaps reflective of the fact that the role of US government agencies is in fact complex as it is fragmented and somewhat overlapping. Nevertheless these are notable results which we plan to address in a future course offering, since these topics were an intended focus of the course.

The change towards familiarity was greatest (i.e. more than 20 students shifted from low to having some familiarity) for topics 4, 5, 18, 20, 21, and 22. Note that topics 20, 21 and 22 were directly related to debate resolutions, which is a positive indication that the debates were useful learning tools. Topics 4 and 5 are foundational concepts that came up frequently and thus students had many opportunities to learn cryptography. The big change for topic 18, the nature of cyberwar, may be explained by the topic's obscurity and the fact that it was covered close to when students filled out the post-survey.

In the pre-survey, 90% of students reported that they knew the meaning of cybersecurity and this went up to 100% in the post-survey. However, from these results, it is unclear whether students began with a *good* definition of cybersecurity. For future work, it would be interesting to measure whether students changed their definitions of cybersecurity between the pre- and post- surveys.

During Spring 2016, students were assessed by instructors using assignments, debates and exams. Table 5 summarizes student scores for some key assessments: the final exam, the in class debate, and the assignments where they had to come up with questions for the debaters.

Table 5. Key Instructor Assessments

Assessment	**Average out of 100**	**Std. Dev**
Final Exam – Technical Foundations	60.6	15
Final Exam – Policy Foundations	66.7	17
Final Exam – Critical Thinking	85	14
In class Debate	90.8	6
Assignments – Questions for debaters	90.7	7

On the final exam, students were evaluated separately for each learning objective. Students performed much lower than they rated themselves on the technical and policy foundations. The average score out of 100 was 60.6 with a standard deviation of 15 for technical foundations, and 66.7 with a standard deviation of 17 for policy foundations. Future course offerings need to make improvements to raise average student grades in both areas to at least 80%. See next section for plans for improvement.

The average score for critical thinking on the final was 85 with a standard deviation of 14. Students also performed well on both the in class debate and on coming up with questions for debaters. The average score was around 90 for both with standard deviations for 6 or 7. This gives some evidence that debates were an effective active learning tool.

5. Lessons Learned and Future Plans

The course design described above, with foundational topics organized around debates, was a significant revision and improvement over the sequencing of topics in our initial course offering (spring 2015). In our initial course, all foundational topics were presented first and the course ended with debates. While in theory that allowed students to draw upon all the foundational knowledge during debates, in practice we found that students often did not understand why they were learning a particular foundational topic. Ordering foundational topics around debates gave students context and motivation.

To address low student final scores on technical foundations we plan to develop more in class hands-on activities to allow students to gain experience with technical concepts. Some ideas include allowing students to encrypt, decrypt and break a simple encryption scheme, giving students the opportunity to play with network sniffing tools, and using ideas from CS Unplugged for introducing data representation, message passing and packet switching [10]. We also plan to combine delivery of information with discussions and hands-on activities in every class session, rather than devoting one weekly class session entirely to a lecture and the other to a review/discussion. Additionally, restricting the course to non-majors and minors, we believe, will help students feel more confident about learning technical topics and allow the instructor to cover topics at a more appropriate pace.

We plan to address the mixed results on policy foundations topics in several different ways. Since students performed well on in-class debates and seemed to enjoy participating in them, our first idea is use some class discussion time as *mini debates.* Students will work in teams to come up with arguments either in support of or against a cybersecurity issue. The instructor would then *facilitate* the mini debate by asking each side to state *particular types* of arguments and the other side to offer counter arguments. Gearing the discussion around policy topics would provide opportunities for review. Mini-debates would also give students additional debate experience which will hopefully lead to more interesting exchanges in in-class debates.

Our second idea to reinforce policy foundations is to add discussions about the latest NIST cybersecurity framework which encourages organizations to think of cybersecurity as a continuous process starting with identification of current risks to planning for recovery from potential attacks [11]. The NIST recommendations could be contrasted with other public policies to govern cybersecurity, providing additional opportunities to review policy topics where students assessed themselves to have low knowledge. We hope this will also result in higher scores on exams.

Overall, students performed well on debates and also seemed to enjoy participating in them. Nonetheless, we plan to improve the students experience in the following way. Some students found it challenging to split up the task of writing their position papers between their group members. In contrast, no student had similar complaints regarding the in-class debate. This could be due to the fact students were given clear roles in the debate where as they had to come up with their own roles for writing the paper. To address this prior to the due date, we will require each team to submit a list of the arguments their position paper will present along with the name of a team member who will be responsible for addressing it. Additionally, we will ask teams to identify who will be responsible for specific tasks such as gluing the various arguments together, writing an introduction and writing a conclusion. These tasks will also encourage students to not wait till the date due to combine their respective pieces.

6. ACKNOWLEDGMENTS

This project is partially supported by NSF SaTC-EDU 1500033. We would like to thank our SLA expert, Cathy Leogrande from the College's Department of Education.

7. References

[1] Scott, T. 2015. *Strengthening and Enhancing Federal Cybersecurity for the 21st Century*. (July 31, 2015).

Retrieved July 7, 2016 from https://www.whitehouse.gov/blog/2015/07/31/strengthening-enhancing-federal-cybersecurity-21st-century

[2] White & Case. 2015. Cyber Risk: Why Cyber Security is Important. *Latitudes* 3 (Summer 2015).

Retrieved July 7, 2016 from http://latitudes.whitecase.com/cyber-risk-why-cyber-security-is-important

[3] Turner, C. F., Taylor, B. and Kaza, S. Security in computer literacy: A model for design, dissemination, and assessment. In *Proceedings of the 42nd ACM Technical Symposium on Computer Science Education* (Dallas, TX, March 09-12, 2011). SIGCSE '11. ACM, New York, NY, 15-20.

[4] Sullivan, D. G. A data-centric introduction to computer science for non-majors. In *Proceedings of the 44th ACM Technical Symposium on Computer Science Education* (Denver, CO, March 06-09, 2013). SIGCSE '13. ACM, New York, NY, 71-76.

[5] Muller, R. n.d. *Physics for Future Presidents.* (n.d.). Retrieved July 7, 2016 from http://muller.lbl.gov/teaching/Physics10/PffP.html

[6] Burley, D. L. and Bishop, M. 2011. *Summit on Education in Secure Software: Final Report*. Technical Report. UC Davis: College of Engineering.

[7] Kernighan, B. W. 2011. *D is for Digital: What a Well-Informed Person Should Know about Computers and Communications.* DisforDigital.net

[8] Intelligence Squared U.S. n.d. *Intelligence Squared Debates.* (n.d.). Retrieved July 7, 2016 from http://intelligencesquaredus.org/.

[9] Clark, D., Berson, T., and Lin, H. S. (Eds.). 2014. *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues.* The National Academies Press, Washington, DC. Also,

[10] CS Education Research Group. n.d. *CS Unplugged: Computer Science without a Computer.* (n.d.). July 7, 2016 from http://csunplugged.org/.

[11] National Institute of Standards and Technology. 2014. *Framework for Improving Critical Infrastructure Cybersecurity, Ver. 1.* (Feb. 12, 2014). Retrieved July 7, 2016 from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf