Lessons from an Undergraduate Course in Cyber Security and Cyber Warfare:
Is Our Children Securing?

The Circle of HOPE Conference (HOPE 12)
Ming Chow (@0xmchow)
Matthew Weinberg

For an explanation behind our awkwardly titled presentation: http://thehill.com/blogs/congress-blog/education/251317-is-our-children-learning
From The Eleventh HOPE
“Crypto War II: Updates from the Trenches”

Credit: @mattblaze (Matt Blaze) and @sa3nder (Sandy Clark)
Is This a Real Need?

Michael Sulmeyer
@sultanofcyber

Designing a course: What do law students need to know about cyber security?

11:53 AM - 13 Aug 2017

6 Retweets 19 Likes

Source: https://twitter.com/sultanofcyber/status/896806963929112577

Bobby Chesney
@BobbyChesney

What should a course on cybersecurity law & policy cover?

Here's my syllabus (50+ pages of narrative context, questions, linked readings, etc.) Feel free to use it; please share ideas to improve it! Thanks to @EliSugarman & @hewlett_Found for support.

Source: https://twitter.com/BobbyChesney/status/978285676973174786
Course Mission

1.0 Our belief

// Lack of progress in cyber security is due to knowledge and cultural gaps between the technical and non-technical communities

2.0 Our task

// To develop intellectual bridges between students, faculty and the broader cyber security community
Educational Goals

Political Science (PS) / International Relations (IR)
Exposure to the technical aspects of cyber security, which have emerged as major aspects of international security

// Make learning practical, fun and enlightening!
// To encourage students to be active (infosec) citizens
// To engage in constructive and healthy debates

Computer Science (CS)
Exposure to policymaking and the key issues in strategic management of cyber security
Compatriot Courses*

- **PS/Comp 50-01**: *Cyber Security and Cyber Warfare*, Tufts University
- **IGA-236**: *Cybersecurity: Technology, Policy, and Law*, Harvard University, Kennedy School of Government (@schneierblog)
- **E6998-8**: *Cybersecurity, Technology, Policy and Law*, Columbia University (@SteveBellovin, @Jason_Healey and @mattwaxman1)

// *Not exhaustive and growing by the semester!
Alpha Class Composition (Spring 2017)

- Computer Science: 51%
- IR / PS: 40%
- Dual: 9%
Technical Topics

- Security tools including nmap, SHODAN, WHOIS, Metasploit, Kali Linux
- Common Vulnerabilities and Exposures (CVE) and Common Weakness Enumeration (CWE), as well as vulnerability disclosure
- Attack frameworks
- Malware
- Internet of Things
Policy Topics

● Intl. Relations Theory
● Privacy & Surveillance
● Cyber Crime
● Cyber / Information Ops.
● Public / Private Sector Efforts

Thomas Rid’s “Cyber War Will Not Take Place”

Alex Gibney’s “Zero Days”

Trey Herr and Richard Harrison’s “Cyber Insecurity”
Left on the cutting room floor...

- Basic programming
- Packet analysis
- Password cracking
- Reverse engineering

// We do offer Introduction to Computer Security

// Plug: https://tuftsdev.github.io/DefenseAgainstTheDarkArts/
Student Engagement: Capture The Flag

- **CTF Writeup:** Connecting technical deficiencies with the broader implications
- **Practical:** See how software (*doesn’t always*) work; find and exploit vulnerabilities
- **Team-based:** (we will get to this later...)
- **Diversity:**
  - **Gender:** Two male and two female (with the exception of two teams)
  - **Background:** At least one student in Poli Sci or International Relations
  - **Variable experience:** At least one student who I am comfortable with his/her technical abilities or has taken my Security class in the past

// Epiphany #1: *Having non-technical students ride along with technical students during CTFs and incorporating policy implications as part of the CTF writeup*
Student Engagement: “Did you happen to get that memo?”

- **Task**: Explain, analyze and make recommendations without technical jargon in two pages or less (emphasizes writing for brevity, clarity and accessibility)
- **Client-based**: Directed to C-suite, senior policymakers or civil society heads
- **Applicable**: Student memos were directed to real-world decisionmakers (e.g. Facebook’s @alexstamos)

// Ephiphany #2: Process of self-discovery for students; everyone has a unique path to, and through, the infosec field.
Student Engagement: Student “PEP” Talks

- **PEP** = Personal Engagement Projects
- **Open-ended**: Student initiative and taking ownership of their learning
- **Cyber security is a broad field**: Encourage students to discover their interests!

**Resulting projects included:**
- Talks at the Berkman Klein Center
- Students meeting cyber security practitioners at Black Duck Software
- Attending BSides Boston and local security meetups

*Epiphany #3: Students must engage with the community and that those experience will make lasting impressions*
Release Notes: Features

- **Addressed diversity shortcomings** (e.g. background, gender)
- **Timing is everything:** Met demand in cybersecurity
- **Planted the seed:** Students succeeded in follow-on competitions and career-entry in cybersecurity
Release Notes: Bugs

- **Teaching across boundaries:** More time for students to work/teach each other (e.g. “what is rule 41?”)

- **Class environment:** Open-space lab classroom for team-oriented work

- **More creative friction:** Class debates on knotty issues (e.g. Vulnerabilities Equities Process (VEP), surveillance)
Release Note: Issues

● 13 weeks is not a lot of time: Laying the groundwork for lifelong learning

● Weather and scheduling guest speakers: We had to reschedule both CTF game and guest speakers

● Keeping up with events: SHA-1 was cracked after we talked about it in the course. News breaking during class).
Release Notes: Lessons Learned

- **Common vocabulary:** Many words (and acronyms!) have different meaning to different groups
- **Surprise!:** Non-technical students want technical content
- **Role models:** Best to invite speakers who students can relate to and show the diversity of paths to infosec
  - See “My Weird Path to Infosec” Twitter thread [here](#)
Future Releases

- Training Computer Science students in **ethics and basic civics**
- "CS for Future Presidents" — Joint-course taught by the Tufts University Computer Science Department and The Fletcher School of Law & Diplomacy (Thanks Hewlett Foundation!)
- Build some technical depth for non-Computer Science folks
  - How the Internet works
  - Cloud and Internet of Things
  - Privacy and Security
  - Cryptography 101
  - Machine Learning and fairness
“Two students from Tufts University, claimed the grand prize of $10,000 for their development of **Sanity Check**, an app that utilizes natural language processing, bot detection, source greylisting, risk rules, and reverse image searching to identify information operations over social media, as well as suspicious unverifiable information.”

Where are they now?

- 3 engineers and 1 intern at MITRE
- Business Analyst at Clutch.co
- Threat Analyst at Recorded Future
- IBM X-Force
- Two interns at FireEye

Source: https://clutch.co/it-services/failings-cybersecurity-education-interview-professor-ming-chow

Acknowledgements

The author gratefully acknowledges the invaluable contributions and in-depth research of Gabriella Roncone, a research assistant at the Belfer Center's Cyber Security Project. Many other colleagues offered important insights and assistance, including Thomas E. Donilon, Matt Dogas, Eric Goldstein, Andrew Grotto, Heather King, Tim Maurer, Ross Nodurft, George Perkovich, Charley Snyder, Ari Schwartz, Michael Sulmeyer, Kathryn Taylor, Kiersten Todt, two anonymous peer reviewers for the Belfer Center, and multiple current/former officials at NIST, OMB, GSA, DHS, DOD, and NSC. Any errors, of course, are solely those of the author.

Source: https://www.belfercenter.org/sites/default/files/files/publication/Understanding%20Federal%20Cyber%20security%2004%202018_0.pdf
Acknowledgements

- Jeffrey Taliaferro, Susan Landau, Michele Malvesti, Kathleen Fisher, Debbie Schildkraut, Soha Hassoun
- **Tufts Innovates Grant**: Underwrote course development and execution
- **Kade Crockford**, Director of Technology for Liberty Program at ACLU of Massachusetts. Guest lecture on *Surveillance and Privacy*
- **Ely Kahn**, Co-Founder / VP Business Development and Marketing at Sqrrl. Guest lecture on *Cyber Defense: Past, Present, and Future*
- **Seth Milstein**, Vice President at JP Morgan Chase & Co. Guest lecture on *Cyber Security in Public vs Private Sectors*

*Colleagues across academia running great programs!*
References

- Syllabus: https://mchow01.github.io/docs/comp50ps18802-s2017.pdf
- Poster: https://mchow01.github.io/docs/comp50ps18802-s2017-poster.pdf