Spring 2019

New in Spring 2019!

- Removed two individual reflection assignments.
- Added Red Team OSINT assignment.
- Conducted hands-on cybersecurity workshop with School of Journalism.

Info 290. Public Interest Cybersecurity: The Citizen Clinic Practicum.

Spring 2019.

Course description.

For individuals and organizations involved in political advocacy, cybersecurity threats are an increasingly common reality of operating in the digital world. Civil society has always been under attack from ideological, political, and governmental opponents who seek to silence dissenting opinions, but the widespread adoption of connected technologies by the individuals and organizations that make up civil society creates a new class of vulnerabilities.

Citizen Clinic at the Center for Long-Term Cybersecurity provides students with real-world experience assisting politically vulnerable organizations and persons around the world to develop and implement sound cybersecurity practices. Clinic students will participate in both a classroom and clinic component. In the classroom, students will study the basic theories and practices of digital security, the intricacies of protecting largely under-resourced organizations, and the tools needed to manage risk in complex political, sociological, legal, and ethical contexts. In the clinic component, students will work in teams supervised by the Clinic staff to provide direct cybersecurity assistance to civil society organizations. Students' clinic responsibilities will include learning about an organization's mission and context, assessing its vulnerabilities, and ultimately recommending and implementing mitigations to the identified security risks. The emphasis will be on pragmatic, workable solutions that take into account

the unique operational needs of each partner organization.Weekly lectures will provide students with the background information and tools they will need to engage with partners. Coursework will focus on partner-facing, hands-on projects. Students will be expected to work an average of 12 hours per week, although the distribution of this workload may fluctuate based upon the availability and needs of the partner.

Schedule.

In the first half of the semester, class meetings will be a mix of lectures & discussions with more technical & project-oriented labs. In the second half of the semester, these class times will be reserved for work with the teaching team and check-ins tailored to the specific needs of your partner organization.

Note: This schedule is tentative and may be adjusted - assignment dates may change, additional readings may be assigned, speakers/lectures may be shuffled, etc. The teaching team will announce when changes are made.

Week 1: Introduction / What is Public-Interest Cybersecurity?

Read:

- Access Now. "Spyware in Mexico: an interview with Luis Fernando García of R3D Mexico" [https://www.accessnow.org/spyware-mexico-interview-luis-fernando-garcia-r3d-mexico/]
- Jorge Luis Sierra "Digital and Mobile Security for Mexican Journalists and Bloggers" [https://freedomhouse.org/sites/default/files/Digital%20and%20Mobile%20Security%20for%20Mexican%20Journalists%20
- Netgain "Digital Security and Grantcraft Guide" [fordfoundation.org/media/3334/digital-security-grantcraft-guide-v10-final-22317.pdf]
- **(Skim)** Citizen Lab's "About Us" Paper. [https://citizenlab.ca/wp-content/uploads/2018/05/18033-Citizen-Lab-booklet-p-E.pdf]
- **(Skim)** Tactical Tech's Annual Report [https://tacticaltech.org/media/news/annual-report-2017.pdf]

- **(Optional)** Sean Brooks “Defending Politically Vulnerable Organizations Online” [https://cltc.berkeley.edu/wp-content/uploads/2018/07/CLTC_Defending_PVOs.pdf]
- **(Optional)** Rus Shuler. “How Does the Internet Work?” [web.stanford.edu/class/msande91si/www-spr04/readings/week1/InternetWhitepaper.htm]

Assignments Due:

- *1/22 11:59PM:* **Submit application materials to enroll in this course. You will be notified of your enrollment status prior to the next class meeting on January 24th.**
- *1/24 In-Class*: Code of Conduct Signed *[Individual]*
- *1/27 11:59PM:* Equipment Setup Completed (with Reflection & Partner Preference Submitted) *[Individual]*

Tuesday 1/22:

We will introduce the content and methods of the course, answer your questions, and everyone will introduce themselves to one another.

- Introduction to Public Interest Cybersecurity

Thursday 1/24:

- Citizen Clinic “Rules of the Road”:
- Citizen Clinic Code of Conduct.
- Personal Risk of Citizen Clinic.
- How to talk about Citizen Clinic.
- Ethical Considerations.
- Security Response Plan.
- Personal Communications setup and equipment issue
- Partner Overview

Week 2: Threats to Civil Society's Cybersecurity

Read:

- Electronic Frontier Foundation, "Surveillance Self-Defense: Your Security Plan" [https://ssd.eff.org/en/playlist/activist-or-protester#your-security-plan] - **know the definitions of underlined terms.**
- Le Blond et al. "A look at targeted attacks through the lense of an NGO" [www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-blond.pdf]
- Citizen Lab. "Bittersweet: Supporters of Mexico's soda tax targeted with NSO exploit links" [https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/]
- Silver & Elgin. "Torture in Bahrain Becomes Routine With Help From Nokia Siemens" [https://web.archive.org/web/20111006185329/http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html]
- **(Explore)** MSFT's STRIDE and related blog posts. [https://cloudblogs.microsoft.com/microsoftsecure/2007/09/11/stride-chart/]
- **(Optional)** Joseph Cox. "I Gave a Bounty Hunter $300. Then He Located Our Phone" [https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile]
- **(Optional)** Stephen Arnold. "Telestrategies - An Interview with Dr. Jerry Lucas" [http://www.arnoldit.com/search-wizards-speak/telestrategies-2.html]
- **(Optional)** Alex Gaynor. "What happens when you type google.com into your browser's address box and press enter?" [https://github.com/alex/what-happens-when]

Assignments Due:

- *2/1 6:00PM*: Partner Communications Instructions (for Review) *[Team]*

Tuesday 1/29:

- Threat Modeling

- Partner Communication Workshop

Thursday 1/31:

- Bill Marczak, “Digital Surveillance of PVOs - The Threat Landscape”

Week 3: Information Collection

Read:

- Amnesty International. “Digitally dissecting atrocities – Amnesty International’s open source investigations.” [https://www.amnesty.org/en/latest/news/2018/09/digitally-dissecting-atrocities-amnesty-internationals-open-source-investigations/]
- Protective Intelligence. “Part I: An Introduction To OSINT Research For Protective Intelligence Professionals” [https://www.protectiveintelligence.com/blog/osint-intro-for-protective-intelligence-pt1]
- Protective Intelligence. “Part 2: An Introduction To OSINT Research For Protective Intelligence Professionals” [https://www.protectiveintelligence.com/blog/osint-intro-for-protective-intelligence-pt2]
- Ian Barwise. “Open-Source Intelligence (OSINT) Reconnaissance” [https://medium.com/@z3roTrust/open-source-intelligence-osint-reconnaissance-75edd7f7dada]
- **(Explore)** OSINT Framework [https://osintframework.com/]
- **(Explore)** Bellingcat Online Investigation Toolkit [https://docs.google.com/document/d/1BfLPJpRtyq4RFtHJoNpvWQjmGnyVkfE2HYoICKOGguA/edit]

Assignments Due:

- *2/8 6:00PM:* Collaborative Plan *[Team]*

Swapped - Tuesday 2/5:

- Open Source Research Methods, Safety, and Tools

Thursday 2/7:

- Félim McMahon, Technology Director, Human Rights Center "Deploying Security Controls in a High-Risk Environment"

Week 4: Risk Assessment for Cybersecurity

Read:

- *Example Risk Assessment shared via email.*
- SAFETAG Guide. Read to Section 4.4, skim rest. [https://safetag.org/guide/ read to Section 4.4]
- Julian Cohen. "Playbook Based Testing." [https://medium.com/@HockeyInJune/playbook-based-testing-5df4b656113a]
- NIST SP 800-37 "Risk Management Framework for Information Systems and Organizations." Chapter 2 only. [https://csrc.nist.gov/CSRC/media/Publications/sp/800-37/rev-2/draft/documents/sp800-37r2-draft-ipd.pdf or Shutdown Mirror]
- **(Explore)** About PESTLE. [http://guides.ucf.edu/industryanalysis/PESTLE]
- **(Skim)** NIST SP 800-39 "Managing Information Security Risk." Chapter 2 only. [https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf or Shutdown Mirror]
- **(Skim)** NISTIR 8062 "An Introduction to Privacy Engineering and Risk Management in Federal Systems." [https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf or Shutdown Mirror]

Assignments Due:

- *By end of week (2/15)*: First Call with Partner *[Team]*
- *2/15 6:00PM*: OSINT Assignment *[Team]*

Tuesday 2/12:

Contextual Factors and Frameworks

- SAFETAG

- PESTLE-M
- PMESII

Thursday 2/14:

- Bounding Risk Assessments

Week 5: Changing Security Behaviors

Read:

- Engine Room. “Ties That Bind: Organisational Security for Civil Society” - read Full Report. [https://www.theengineroom.org/civil-society-digital-security-new-research/]
- APF et al. “Improving SSL Warnings: Comprehension and Adherence” [https://dl.acm.org/citation.cfm?id=2702442]
- Abu-Salma et al. “Obstacles to the Adoption of Secure Communication Tools” [https://ieeexplore.ieee.org/abstract/document/7958575/]
- **(Watch)** Rachel Tobac. “How I would Hack You: Social Engineering Step-by-Step” [https://www.youtube.com/watch?v=L5J2PgGOLtE]
- **(Optional)** Scott, James C. “Seeing Like a State” - Chapter 9 [https://libcom.org/files/Seeing%20Like%20a%20State%20-%20James%20C.%20Scott.pdf]

Assignments Due:

- *By end of week (2/22)*: 1st Contextual Research Briefs *[Individual]*

Tuesday 2/19:

- Steve Weber, “Changing Behaviors within PVOs”

Thursday 2/21:

- Phishing for Context

Week 6: Establishing Baseline Digital Security (Part 1)

Read:

- Bill Marczak and John Scott-Railton. "Keep Calm and (Don't) Enable Macros: A New Threat Actor Targets UAE Dissidents" [https://citizenlab.ca/2016/05/stealth-falcon/]
- Micah Lee. "It's Impossible To Prove Your Laptop Hasn't Been Hacked. I Spent Two Years Finding Out." [https://theintercept.com/2018/04/28/computer-malware-tampering/]
- Arthur Turner. "Consulting Is More Than Giving Advice." [https://hbr.org/1982/09/consulting-is-more-than-giving-advice]

Assignments Due:

- *3/1 6:00PM*: Draft Work Plan (to Teaching Team) *[Team]*
- *3/3 11:59PM*: Phishing Email Template *[Individual]*

Tuesday 2/26:

- Managing an Effective Consulting Relationship
- Designing your Work Plan

Thursday 2/28:

- Bill Marczak, "Technical Investigations and Techniques"

Week 7: Establishing Baseline Digital Security (Part 2)

Read:

- IFTF "State-Sponsored Trolling: How Governments Are Deploying Disinformation as Part of Broader Digital Harassment Campaigns". Read pages 3 to 21 & 45 to 51. [http://www.iftf.org/statesponsoredtrolling]
- InterAction "Disinformation Toolkit." [https://staging.interaction.org/documents/disinformation-toolkit/]

- Emma L. Backe. “Left to their Own Devices: Gender, Cyberviolence, and the Internet” [https://thenewinquiry.com/blog/left-to-their-own-devices-gender-cyberviolence-and-the-internet/]
- Reply All podcast. “#112 The Prophet” Listen to or read transcript. [https://www.gimletmedia.com/reply-all/112-the-prophet]
- **(Explore)** Mitre’s ATT&CK Wiki. [https://attack.mitre.org/wiki/Main_Page]

Assignments Due:

- *3/5 11:59PM*: Phishing Email Template *[Individual]*
- *By end of week (3/8)*: Work Plan Call with Partner *[Team]*
- *3/8 6:00PM*: Final Work Plan Approved by Partner *[Team]*

Tuesday 3/5:

- Adversary Persona and Threat Scenario Development (Nick Merrill’s Security Game)

Thursday 3/7:

- Leigh Honeywell, Founder/CEO, Tall Poppy “Online Harassment and Trolling”

Week 8: Digital Security Training (Part 1)

Read:

- Weidinger et al. “How To Give A Digital Security Training” [https://medium.com/@geminiimatt/how-to-give-a-digital-security-training-4c83af667d40]
- EFF. “Am I the Right Person?” [https://sec.eff.org/articles/right-person-to-train]
- EFF. “How to Teach Adults” [https://sec.eff.org/articles/how-to-teach-adults]
- **(Explore)** Citizen Lab’s Security Planner. [https://securityplanner.org/]
- **(Explore)** The rest of EFF’s Security Education Companion. [https://sec.eff.org/]

- **(Explore)** Mitre's Common Vulnerabilities and Exposures search. [https://cve.mitre.org/cve/]

Assignments Due:

- *By end of week (3/15)*: 2nd Contextual Research Briefs *[Individual]*

Tuesday 3/12:

- Adult Education for Security
- Studying and Evaluating Security Tools (Yubikey), Indiana University

Thursday 3/14:

- Eva Galperin, Director of Cybersecurity, EFF - "Being a good security educator"

Week 9: Digital Security Training (Part 2)

Assignments Due:

- *3/21 11:59PM* : Team Evaluation 1 *[Individual]*

Tuesday 3/19:

- Community Clinic with the School of Journalism **(School of Journalism Library, Lunch will be provided)**

Thursday 3/21:

- Community Clinic Discussion
- Third-Party Tool Evaluation

Week 10 - "Spring Break":

- Tuesday 3/26: *No Class*
- Thursday 3/28: *No Class*

Week 11:

- Tuesday 4/2: Clinic Core Hours / Team Check-in

"Clinic Core Hours" refers to the required student attendance of official class meeting hours between 12PM and 2PM that will be reserved for instruction specific to partner needs, feedback and guidance from the teaching team, and ad-hoc lectures. Every Tuesday (starting on April 2nd), each team will have a 30-minute check-in with the teaching team. Each team member will provide a ~5 minute update on the progress of their assigned partner work.

- Thursday 4/4: Clinic Core Hours

Week 12:

- Tuesday 4/9: Clinic Core Hours / Team Check-in
- Thursday 4/11: Clinic Core Hours

Week 13:

- Tuesday 4/16: Clinic Core Hours / Team Check-in
- Thursday 4/18: Clinic Core Hours

Week 14:

- Tuesday 4/23: Clinic Core Hours / Team Check-in
- Thursday 4/25: Clinic Core Hours

Week 15:

Assignments Due:

- *4/30 11:59PM:* Final Partner Report (for Teaching Team Review) *[Team]*
- Tuesday 4/30: Clinic Core Hours
- Thursday 5/2: Clinic Core Hours / Final Report Feedback

Week 16 (RRR): Wrap-up & Project Presentations

Assignments Due:

- *5/10 6:00PM:* Final Partner Report (to Partner) *[Team]*
- *5/8 11:59PM*: Project Presentations *[Team]*
- *5/12 11:59PM*: Final Individual Write-up *[Individual]*
- *5/12 11:59PM:* Team Evaluation 2 *[Individual]*

Tuesday 5/7 - Course Wrap-up:

Feedback on deliverables, submit all final deliverables.

Thursday 5/9 - Project Presentations:

An overview of partner work, findings, recommendations delivered to CLTC and stakeholders.

Course policies

Workload.

This is a 4-unit class. Coursework will primarily focus on partner-facing projects while weekly lectures will be used to inform and engage with students' hands-on experiences. Students are expected to work an average of 12 hours per week on this course, however the distribution of this workload may fluctuate based on the availability and needs of the partner.

Evaluation.

Assignments will largely be evaluated on the following rubric that emphasizes (1) sound rationale in assessments, recommendations, and reflections, (2) "partner-ready" work products which reflect professional quality, and (3) completing the instructions of the assignment or the requirements agreed upon work plan with the partner.

General Grading Rubric

Component	**0 points**	**5 points**	**10 points**
Rationale	Does not meet partner needs, introduces serious harms to partner, shows limited or inappropriate consideration for context	Addresses most of partner needs, some oversight of potential harms to partner, mostly appropriate for given context.	All partner needs are met, feasible & effective rationale that addresses all major threats, appropriate for given context.
Professionalism	Hard to understand, full of jargon, serious writing/format errors present, tone / design unsuitable for its audience	Writing is mostly understandable; minor writing/ format errors (typos), mostly appropriate tone / design	"partner-ready," clear and concise writing, almost no writing/formatting errors, appropriate tone & design for its audience
Requirements	Some requirements in assignment or work plan not met; no insights or connections to readings/lectures; for group work: no evidence of group work	Most requirements met, some evidence for connections with readings/lectures; for group work: some evidence of group work	All requirements met, with clear, thoughtful insights and multiple cited connections to relevant readings/ lectures; for group work: full evidence of strong, equitable collaboration

Note: Students taking the course for P/NP or S/U are expected to participate in classes and complete all work to the same level of quality as students taking the course for a letter grade.

Assignments.

1. Partner Deliverables - 60%

The largest portion of graded evaluation will be based upon your team's work and support for its assigned partner. These deliverables may include assessments, recommendations, and guides, each tailored towards the partner's needs. Each team will also deliver a final report summarizing work performed with their partner.

2. Individual Assignments - 10%

A small number of individual assignments will be given, mostly within the first half of the course.

3. Final Individual Write-Up - 10%

We want students to be able to discuss and share their experience in the course with others, including future employers. We also want our partners to remain confidential and protected. This being said, each student will submit a write-up of work performed and takeaways with sensitive information removed. The teaching team will review to ensure your experience is captured in an effective & safe manner.

4. Participation - 10%

You are expected to attend each official class meeting and contribute substantially to class discussions. While you may not be able to attend every team meeting and partner engagement outside of normal class hours, you are expected to attend and contribute to your team's effort as often as possible. Absences from class meetings (including Clinic Core Hours) should be excused by the teaching team in advance. Not showing up to team check-ins every Thursday after Spring Break will also negatively impact this grade. **As a rule, two people from your team must attend any partner meeting or call.**

5. Team Evaluations - 10%

If there are difficulties with any team member, discuss the matter within your team and seek resolution. If you cannot resolve the problem, immediately contact any faculty member, so that we can make an appointment to discuss the situation individually or with the entire group as needed. Throughout the course, you will submit confidential evaluation forms which ask you to evaluate the contributions of each team member including yourself. Your final course

grade will be adjusted, higher or lower, if you are contributing more or less than those within your group.

Late assignments.

As we want to respect the time of our partners and ensure a high level of quality control (the teaching team will review deliverables before it reaches the partner), we expect students to adhere to timelines and due dates. **Each day an assignment is late will result in a letter grade deduction.** Recognizing that emergencies arise and partners may require schedule adjustments, exceptions will be made on a case-by-case basis.

Code of Conduct.

Each student enrolled in the course must agree in writing to the Citizen Clinic's Code of Conduct (to be distributed) for maintaining a safe and secure learning experience and partner relationship. This Code of Conduct will be respected by all students, the teaching team, and CLTC staff and it is the responsibility of all personnel to report possible violations of the Code of Conduct to the teaching team.

Additionally, we expect all students to abide by the Berkeley Student Code of Conduct (see https://sa.berkeley.edu/student-code-of-conduct) and act with honesty, integrity, and respect for others. (See also https://diversity.berkeley.edu/principles-community). The consequences for failing to act within these standards may include failing an assignment, a referral to the Center for Student Conduct and Community Standards, a failed grade in the course, and even immediate expulsion. A note on plagiarism: even in the scope of providing a partners with a walkthrough for securing a certain account or system, you are expected not to copy material from another guide, website, article or book (word-for-word or paraphrased) without citing the source - it's a small community and we should give credit where it is due. Other examples of unacceptable conduct include turning in deliverables created by students not currently in the course, work found on the Internet, or created by a commercial service.

Disability Accommodation.

If you need disability-related accommodations in this class, if you have emergency medical information you wish to share with us, or if you need special arrangements in case the building must be evacuated, please inform us as soon as possible.

Last update: March 30, 2020