# Fall 2018

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

**Fall 2018.**

**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. The Center for Long-Term Cybersecurity's Citizen Clinic provides students with real-world experience to develop and implement sound cybersecurity practices needed to protect these politically-vulnerable organizations and persons around the world. Students will learn about both the theory and practice of baseline digital security, the intricacies of protection for largely under-resourced organizations, and effective risk management in complex political, sociological, legal, and ethical contexts. Working with civil society organizations as clients, students will learn how to assess vulnerabilities and develop, recommend, and implement mitigations for security risks despite having little or no prior background in the client's mission or context. The emphasis is on pragmatic, workable solutions that take into account the way client organizations operate.

Coursework will focus on client-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 client.

**Schedule.**

Typically, Wednesday class meetings in the first half of the semester will be lecture/discussion-centered, while Monday meetings will be more technical &

project-oriented. In the second half of the semester, these class times will be reserved for work with the teaching team, guest speakers, and discussions tailored to the specific needs of your client.

*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 0: Introduction

**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/]
- Sean Brooks "Defending Politically Vulnerable Organizations Online" [https://cltc.berkeley.edu/wp-content/uploads/2018/07/CLTC_Defending_PVOs.pdf]

**Assignments Due:**

- *8/22 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 August 27th.

**Wednesday 8/22 [South Hall Room 107] :**

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

## Week 1: What is Public-Interest Cybersecurity?

**Read:**

- Jorge Luis Sierra "Digital and Mobile Security for Mexican Journalists and Bloggers" [https://ijnet.org/en/content/digital-and-mobile-security-mexican-journalists-and-bloggers]

- Netgain “Digital Security and Grantcraft Guide” [fordfoundation.org/media/3334/digital-security-grantcraft-guide-v10-final-22317.pdf]
- Citizen Lab’s “About Us” Paper. [https://citizenlab.ca/wp-content/uploads/2018/05/18033-Citizen-Lab-booklet-p-E.pdf]
- Tactical Tech's Annual Report [https://tacticaltech.org/media/news/annual-report-2017.pdf]

**Assignments Due:**

- *8/27 in-class*: Code of Conduct Signed *[Individual]*
- *8/31 6:00PM:* Secure Communications Established (with Reflection) *[Individual]*

**Monday 8/27 Lab:**

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.

**Wednesday 8/29 Lecture:**

- Sean B & Steve T: “The need for public interest cybersecurity”

## Week 2: Threat Landscape (Technical Theory Base)

**Read:**

- Citizen Lab. “Bittersweet: Supporters of Mexico’s soda tax targeted with NSO exploit links” [https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/]

- 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]
- 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]
- Stephen Arnold. “Telestrategies - An Interview with Dr. Jerry Lucas” [http://www.arnoldit.com/search-wizards-speak/telestrategies-2.html]
- **(Optional)** Reply All podcast. “#112 The Prophet” Listen to or read transcript. [https://www.gimletmedia.com/reply-all/112-the-prophet]
- **(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:**

- *9/7 6:00PM:* Collaborative Plan *[Team]*
- *9/9 11:59PM:* 9/12 11:59PM: Secure-a-Friend Reflection *[Individual]*

**Monday 9/3:** *Academic and Administrative Holiday (Labor Day)*

**Wednesday 9/5 Lecture:**

- Bill Marczak “The vulnerabilities of cyberspace”

## Week 3: Challenges to Securing Politically-Vulnerable Organizations

**Read:**

- CIPESA. “Safeguarding Civil Society: Assessing Internet Freedom and the Digital Resilience of Civil Society in East Africa” - Read each chapter, but for one country only. [https://cipesa.org/?wpfb_dl=237]
- Abu-Salma et al. “Obstacles to the Adoption of Secure Communication Tools” [https://ieeexplore.ieee.org/abstract/document/7958575/]

- Whitten & Tygar. “Why Johnny Can’t Encrypt” [https://people.eecs.berkeley.edu/~tygar/papers/Why_Johnny_Cant_Encrypt/OReilly.pdf]
- Scott, James C. “Seeing Like a State” - Chapter 9 [https://libcom.org/files/Seeing%20Like%20a%20State%20-%20James%20C.%20Scott.pdf]

**Assignments Due:**

- *9/10 11:59PM*: Client Communications Instructions (for Review) *[Team]*
- *9/12 11:59PM:* (Moved from Week 2) Secure-a-Friend Reflection *[Individual]*
- *9/20 (Target)*: Communication Established with Client *[Team]*
- *9/16 11:59PM:* Personal Threat Model *[Individual]* TBD

**Monday 9/10: Lab:**

- Threat modelling.
- Establishing communications with clients.
- Conducting interviews.

**Wednesday 9/12 Lecture:**

- Steve Weber “Changing behaviors within PVOs”

## Week 4: Contextual Assessments for Cybersecurity

**Read:**

- SAFETAG Guide. Read pages 1 - 31, skim rest. [github.com/SAFETAG/SAFETAG/files/1278308/SAFETAG-FullGuide_Sep2017.pdf]
- NIST SP 800-39 “Managing Information Security Risk.” Chapter 2 only. [https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf]
- 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]

- NISTIR 8062 “An Introduction to Privacy Engineering and Risk Management in Federal Systems.” [https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf]
- Fong, Rowland, Trush. “A CRIMSon Tide of Data: An Assessment of Potential Privacy Problems of the Consolidate Records Information Management System” [http://people.ischool.berkeley.edu/~strush/CRIMS_FongRowlandTrush_Feb2018.pdf]
- About PESTLE. [http://guides.ucf.edu/industryanalysis/PESTLE]

**Assignments Due:**

- *9/20 (Target) Continued*: Communication Established with Client *[Team]*

**Monday 9/17: Lab**

- Open Source Research methods and tools.
- Environmental factors frameworks (PESTLE-M, PMESII).

**Wednesday 9/19 Lecture:**

- Sean Brooks: “Bounding risk assessments”

## Week 5: Conducting Technical Assessments

**Read:**

- 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/]
- Explore Mitre’s PRE-ATT&CK Wiki. [https://attack.mitre.org/pre-attack/index.php/Main_Page]
- Explore Mitre’s ATT&CK Wiki. [https://attack.mitre.org/wiki/Main_Page]

- Use Mitre's Common Vulnerabilities and Exposures search. [https://cve.mitre.org/cve/].

*Additional readings as specified by guest*

**Assignments Due:**

- *9/24 2:00PM*: 1st Contextual Research Briefs *[Individual]*
- *9/26 2:00PM*: Threat Model Reflection *[Individual - Mini Assignment]*
- *9/26 11:59PM*: Initial Work Plan (for Teaching Team Review) *[Team]*
- *9/28 6:00PM*: Work Plan To Client *[Team]*

**Monday 9/24 Lab:**

- Conducting interviews.
- Surveys / Device inventories.

**Wednesday 9/26 Lecture:**

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

## Week 6: Establishing Baseline Digital Security (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]
- Musiani & Ermoshina. "What is a Good Secure Messaging Tool? The EFF Secure Messaging Scorecard and the Shaping of Digital (Usable) Security" [https://www.westminsterpapers.org/articles/10.16997/wpcc.265/]
- Use Citizen Lab's Security Planner. [https://securityplanner.org/]
- Explore EFF's Surveillance Self-Defense guide. [https://ssd.eff.org/]

*Additional readings as specified by guest.*

**Assignments Due:**

- *10/1 2:00PM* 2nd Contextual Research Briefs *[Individual]*

**Monday 10/1: Lab**

- Technical assessments.
- Tool Evaluation.

**Wednesday 10/3 Guest Lecture:**

- Bill Marczak “Technical investigations and techniques”

## Week 7: Establishing Baseline Digital Security (Part 2)

**Read:**

*Additional readings as specified by guest*

**Assignments Due:**

- *10/14 11:59PM*: Phishing Templates *[Individual]*
- *TBD:* Home Router Assessment *[Individual]*
- *TBD:* Community Clinic Reflection *[Individual]*

**Monday 10/8 Lab:**

Recommendations

- Guides: Password manager, device security.
- Phishing training.
- (Potential move) Community Clinic: *an event for assessing & securing local high-risk organization members*

**Wednesday 10/10 Lecture:**

- Félim McMahon, Technology Director, Human Rights Center “Deploying security controls in high-risk environments”

## Week 8:

**Monday 10/15:** Clinic Core Hours

*"Clinic Core Hours" refers to the required student attendance of official class meeting hours between 2PM and 4PM that will be reserved for instruction specific to client needs, feedback and guidance from the teaching team, and potential guest lectures.*

**Wednesday 10/17:** Clinic Core Hours

## Week 9:

**Assignments Due:**

- *10/29 11:59PM:* Community Clinic Reflection *[Individual]*

**Monday 10/22**: Clinic Core Hours

**Wednesday 10/24**: Clinic Core Hours

**Thursday 10/25, 4:50 - 7:00PM:** Digital Security Crash Course, **UC Berkeley, South Hall Room 210**

## Week 10:

**Assignments Due:**

- *10/31 11:59PM:* Team Midterm Progress Report *[Team]*
- *10/31 11:59PM:* Team Evaluation 1 *[Individual]*

**Monday 10/29:** Clinic Core Hours

**Wednesday 10/31:** Clinic Core Hours

## Week 11:

**Monday 11/5:** Clinic Core Hours

**Wednesday 11/7:** Clinic Core Hours

## Week 12:

**Monday 11/12:** *Academic and Administrative Holiday (Labor Day)*

**Wednesday 11/14:** Clinic Core Hours

## Week 13: Thanksgiving Week

**Monday 11/19:** Clinic Core Hours

**Wednesday 11/21:** *Academic and Administrative Holiday (Thanksgiving Eve)*

## Week 14:

**Assignments Due:**

- *11/28 11:59PM:* **Final Client Report (for Teaching Team Review)** *[Team]*

**Monday 11/26:** Clinic Core Hours

**Wednesday 11/28:** Clinic Core Hours

## Week 15 (RRR): Wrap-up & Project Presentations

**Assignments Due:**

- *12/3 6:00PM:* Final Client Report (to Client) *[Team]*
- *12/4 11:59PM*: Project Presentations *[Team]*
- *12/9 11:59PM:* Final Individual Write-up *[Individual]*
- *12/9 11:59PM:* Team Evaluation 2 *[Individual]*

**Monday 12/3 - Course Wrap-up:**

*Feedback on deliverables, submit all final deliverables, turn-in all equipment.*

**Wednesday 12/5 - Project Presentations:**

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

## Course policies

**Workload.**

This is a 4-unit class. Coursework will primarily focus on client-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 client.

**Evaluation.**

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

**General Grading Rubric**

| *Component* | **0 points** | **5 points** | **10 points** |
|---|---|---|---|
| Rationale | Does not meet client needs, introduces serious harms to client, shows limited or inappropriate consideration for context | Addresses most of client needs, some oversight of potential harms to client, mostly appropriate for given context. | All client 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 | Writing is mostly understandable; minor writing/ format errors (typos) | "Client-ready," clear and concise writing, almost no writing/ formatting errors |
| 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. Client Deliverables - 50%**

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

**2. Individual Assignments - 20%**

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 clients 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 client engagement outside of normal class hours, you are expected to attend and contribute to your team's effort as often as possible.

**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 clients and ensure a high level of quality control (the teaching team will review deliverables before it reaches the client), 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 clients 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 client 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 client 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 26, 2020