2020 Geopolitics of Cyberspace Syllabus

Pol 481 / 2240 H1S
Tuesdays 2-4pm
BA B026

Office Hours: By appointment only. Send email to r.deibert@utoronto.ca I will prioritize answering students' emails promptly.

Description:

The constantly evolving digital electronic telecommunications environment that surrounds us is having dramatic and far-reaching impacts on our lives, social relationships, and systems of political authority. While they have not eliminated the perennial quest for power, security and competitive advantage among actors on the world stage, they are profoundly changing the context and the character of these contests. Individuals, organizations, corporations and states are all seeking ways to control information and information systems to pursue political objectives in the midst of a rapidly evolving technological environment.

This course is an intensive examination of the newly evolving terrain of global digital–electronic–telecommunications through the lens of the research of the Citizen Lab. For over 15 years, the Citizen Lab (**https://citizenlab.ca/**) -- an interdisciplinary research laboratory based at the Munk School of Global Affairs and Public Policy, University of Toronto (which the instructor founded and currently directs) -- has investigated issues at the intersection of information and communication technologies, human rights, and global security. We use a "mixed methods" approach to research combining practices from political science, law, computer science, and area studies. We see ourselves as a kind of "early warning system," looking over the horizon, or peering beneath the covers of the technological systems that surround us, to expose abuses of power, violations of human rights, or other threats to privacy and security.

After setting the stage with some general readings on background and context, we turn to several modules organized as detailed examinations of the Citizen Lab's mixed methods research on information controls, including analyzing Internet censorship and surveillance, investigating targeted digital espionage, uncovering privacy and security risks of mobile applications, disinformation operations, and the role of the private sector in information controls. We conclude with an exploration of threat modeling and how each of you can increase your own digital hygiene.

The **goals** of the class are two-fold: first, we aim to familiarize you with the unique approach, methods, and outputs of the Citizen Lab. The Citizen Lab is a very unusual research organization. Our publications routinely make world news, and we have exposed the wrong-doings of very powerful states and companies. (Perhaps not surprisingly, these

efforts have had significant repercussions, which we will discuss); second, we also aim to better equip you with the tools to help you navigate this complex, evolving terrain. You do not need to be a computer scientist or software engineer to take this course, nor will you learn how to become one. But we hope that by the end of the course you will have a better understanding of how digital-electronic-telecommunications are organized and are evolving, and more importantly how they impact your life, rights, and security.

Please familiarize yourself with the work of the Lab here: **https://citizenlab.ca/**. You may also want to follow the Citizen Lab twitter account @citizenlab and my twitter account @RonDeibert. The Toronto Star recently published a detailed profile of the Citizen Lab that provides a pretty decent history and overview (unfortunately it is behind a paywall).

Class participation involves active, engaged contributions to the discussion. Each student should come to class prepared to make prepared comments about the readings. Additional points are given for contributing comments that show some degree of analytical sophistication (e.g., comparing readings to one another; contrasting assumptions made in readings with evidence and clear examples). Poor participation involves not being engaged, not communicating or preparing comments in advance (i.e., being a "spectator" in class). Do not wait for me to direct the discussion. Come willing to engage!

Here is a good resource on the topic of active reading:
http://pne.people.si.umich.edu/PDF/howtoread.pdf

Plagiarism is a serious academic offense. Familiarize yourself with what constitutes plagiarism here.

Course prerequisites

Students do not require extensive technical (e.g., computer science or engineering sciences) as a prerequisite for the course as we assume non–technical expertise. However, a basic understanding of political science, international security, and communication studies concepts will be helpful.

Assignments. There are two written assignments for this course, both of which are focused on a topic of your choosing from the list below:

1. A one page summary of the topic chosen plus a 10 page annotated bibliography of resources related to the topic. You will be evaluated on the quality of the resources you choose, as well as the annotations you write. Each annotated should comprise two to three sentences that explains the gist and provides a top-level evaluation.
2. A 20 page essay that provides a critical analysis of the topic chosen. Your paper should be written in the form of a issue-area brief. By the end of reading the paper, I should have a strong grasp of the key issues around the topic, including background, context, relevant research, dissenting points of view, and likely trajectories for the future, in terms of future research and policy. Your aim should be to "inform" rather than "persuade." You do not need a thesis or central argument for this type of paper. I am looking to be brought up to speed.

Choose only **one** of the following three areas, and then drill down into a manageable topic for your two papers:

1. The control of information and communications is dynamically contested around major events, like protests, elections, and armed conflict. Pick a major event and analyze the struggles that took place around information controls leading up to, during, and after the event. Describe the key players involved, the technological environment, and the laws, policies, and practices that were implicated around the event.

2. Pick a single country and develop a profile of its information control regime. Break down the key government agencies involved in information control. Have these agencies changed over time? What are the laws, policies and regulations that have been developed in this country to control information? What is the relationship between the state and the private sector in terms of information control? Is there resistance to information controls from citizens? What shape does that resistance take? How popular is the resistance?

3. Pick a single technological platform / company and provide a profile of that company's services as they relate to basic human rights, like access to information, freedom of speech, and privacy. Does the company's services present challenges to these rights? Has the company acknowledged the need to respect human rights? How effective are those pledges? What relations does this company have with specific governments? Focus on a particular problem, event, or controversy that involves this company to make your paper topic more manageable.

Course Evaluation

First paper / 30% / Due February 4 2020
Second paper / 50% / Due March 31 2020
Participation / 20 %

Late penalty: 5% off of the assignment for each day of lateness

Plagiarism is a serious academic offense. Familiarize yourself with what constitutes plagiarism here.

Course Schedule and Readings

Session 1: Background and context (Jan 7)

Deibert, R. "Cyberspace Under Siege," Journal of Democracy (Volume 26, Number 3, July 2015) pp. 64-78, [**link**]

Deibert, R. J. (2019). "The Road to Digital Unfreedom: Three Painful Truths About Social Media," Journal of Democracy 30(1), 25-39. Johns Hopkins University Press.

Deibert, R. (2018) "Toward a Human-Centric Approach to Cybersecurity," Ethics & International Affairs 32(4).

Session 2: What constitutes cyberspace? (Jan 14)
(Asterix indicates strongly recommended resource for review)

*Biddle, S. "How to Destroy the Internet." *Gizmodo*. May 23, 2012. [link]

*McLaughlin, A., & Zuckerman, E. (2003). *Introduction to Internet Architecture and Institutions*. [link]

*The Route of a Text Message, a Love Story
https://www.vice.com/en_us/article/kzdn8n/the-route-of-a-text-message-a-love-story

"The Urban, Infrastructural Geography of 'The Cloud'" [**link**]

*"'Messages in the Deep: The Remarkable Story of the Underwater Internet," [link]

40 maps that explain the Internet [**link**]

*The Secrets of Cornwall Communications. [**link**]

*Project X. Field of Vision. [**link**]

*Ingrid Burrington, "Why Amazon's Data Centers Are Hidden in Spook Country?" Atlantic Monthly (Jan 8, 2016). [**link**]; the entire Atlantic Monthly series by Ingrid Burrington is here: [**link**]

*Citizen Lab. "The Many Identifiers in Our Pockets: A primer on mobile privacy and security," Citizen Lab Research Report No. 53, University of Toronto, May 2015. [Download PDF]

"An Analysis of Pre-installed Android Software." Julien Gamba, Mohammed Rashed, Abbas Razaghpanah, Juan Tapiador, Narseo Vallina-Rodriguez. arXiv:1905.02713 Submitted 7 May 2019. https://arxiv.org/abs/1905.02713

*Timburg, Craig (24 August 2014). "For sale: Systems that can secretly track where cellphone users go around the globe". *The Washington Post*. Retrieved 27 December 2014.

"The Messenger Shoots Back:Network Operator Based IMSI Catcher Detection." (2016). Adrian Dabrowski and Georg Petzl and Edgar R. Weippl, 19th International Symposium on Research in

Attacks, Intrusions and Defenses (RAID 2016).
https://publications.sba-research.org/publications/providerICdetection.pdf

*Stuart A. Thompson and Charlie Warzel, "Twelve Million Phones, One Dataset, Zero Privacy," New York Times, December 19, 2019.
https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html

Video Essay, "All That Is Solid Melts Into Data"
http://www.boundary2.org/2016/11/all-that-is-solid/

Session 3: Measuring Internet Filtering, Throttling, Blocking, and Other Forms of Network Interference (Jan 21)

Bill Marczak (Lead), Nicholas Weaver (Lead), Jakub Dalek, Roya Ensafi, David Fifield, Sarah McKune, Arn Rey, John Scott-Railton, Ronald Deibert, Vern Paxson, "**China's Great Cannon**," Citizen Lab Research Brief No. 52, April 2015. [**Download PDF**]

Jakub Dalek, Lex Gill, Bill Marczak, Sarah McKune, Naser Noor, Joshua Oliver, Jon Penney, Adam Senft, and Ron Deibert. "**Planet Netsweeper**," Citizen Lab Research Brief No. 108, April 2018.

Bill Marczak, Jakub Dalek, Sarah McKune, Adam Senft, John Scott-Railton, and Ron Deibert. "**Bad Traffic: Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?**," Citizen Lab Research Brief No. 107, March 2018.

Suggested Readings

Bennett Haselton, "Smartfilter: Miscategorization and Filtering in Saudi Arabia and UAE," Citizen Lab Research Report No. 27, University of Toronto, November 2013. [Download PDF]

Deibert, R. , Oliver, J. and Senft, A. (2019). "Censors Get Smart: Evidence from Psiphon in Iran," Review of Policy Research.

Miles Kenyon, Adam Senft, and Ronald Deibert, "Identities in the crosshairs—censoring LGBTQ internet content around the world," *OpenGlobalRights*, November 27, 2018.

A DEEP DIVE INTO INTERNET CENSORSHIP IN RUSSIA. Authors: Reethika Ramesh (reethika@umich.edu), Leonid Evdokimov (leon@darkk.net.ru), Roya Ensafi (ensafi@umich.edu). https://censoredplanet.org/russia

Session 4: Measuring Information Controls on China-based Social Media Apps (Jan 28)

Jeffrey Knockel and Ruohan Xiong. "(Can't) Picture This 2: An Analysis of WeChat's Realtime Image Filtering in Chats," Citizen Lab Research Report No. 122, University of Toronto, July 2019.

Jeffrey Knockel, Lotus Ruan, and Masashi Crete-Nishihata, Citizen Lab, Munk School of Global Affairs, University of Toronto, "Measuring Decentralization of Chinese Keyword Censorship via Mobile Games." FOCI 2017.
https://www.usenix.org/conference/foci17/workshop-program/presentation/knockel

Adam Senft, Jason Q. Ng, Jeffrey Knockel, and Masashi Crete-Nishihata. "Every Rose Has Its Thorn: Censorship and Surveillance on Social Video Platforms in China," Citizen Lab Research Report No. 59, University of Toronto, August 2015. Also:
https://www.usenix.org/conference/foci15/workshop-program/presentation/knockel

Suggested Readings

Masashi Crete-Nishihata, Jeffrey Knockel, Ruohan Xiong. "Censored Commemoration: Chinese Live Streaming Platform YY Focuses Censorship on June 4 Memorials and Activism in Hong Kong," Citizen Lab Research Report No. 119, University of Toronto, June 2019.

Lotus Ruan, Jeffrey Knockel, Jason Q. Ng, and Masashi Crete-Nishihata. One App, Two Systems: "One App, Two Systems: How WeChat uses one censorship policy in China and another internationally," Citizen Lab Research Report No. 84, University of Toronto, November 2016.

Jeffrey Knockel, Lotus Ruan, Masashi Crete-Nishihata, and Ron Deibert. "(Can't) Picture This: An Analysis of Image Filtering on WeChat Moments," Citizen Lab Research Report No. 112, University of Toronto, August 2018.

Session 5: Targeted Espionage I (Feb 4)
FIRST ASSIGNMENT DUE

Missing Link: Tibetan Groups Targeted with 1-Click Mobile Exploits
By Bill Marczak, Adam Hulcoop, Etienne Maynier, Bahr Abdul Razzak, Masashi Crete-Nishihata, John Scott-Railton, and Ron Deibert September 24, 2019

Masashi Crete-Nishihata, Jakub Dalek, Etienne Maynier, and John Scott-Railton. "Spying on a Budget: Inside a Phishing Operation with Targets in the Tibetan Community," Citizen Lab Research Report No. 104, University of Toronto, January 2018.

John Scott-Railton, Ramy Raoof, Bill Marczak, and Etienne Maynier. "Nile Phish: Large-Scale Phishing Campaign Targeting Egyptian Civil Society," Citizen Lab Research Report No. 88, University of Toronto, February 2017.

John Scott-Railton, Bahr Abdulrazzak, Adam Hucloop, Matt Brooks, and Katie Kleemola. "Group5: Syria and the Iranian Connection," Citizen Lab Research Report No. 76, University of Toronto, August 2016.

John Scott-Railton and Katie Kleemola. "London Calling: Two-Factor Authentication Phishing from Iran," Citizen Lab Research Report No. 61, University of Toronto, August 2015.

Session 6: Targeted Espionage II (Commercial Spyware) (Feb 11)

Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert. **Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries**.

Bill Marczak, John Scott-Railton, Adam Senft , Bahr Abdul Razzak, and Ron Deibert. "The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil," Citizen Lab Research Report No. 115, University of Toronto, October 2018.

John Scott-Railton, Bill Marczak, Siena Anstis, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert. "Reckless VII: Wife of Journalist Slain in Cartel-Linked Killing Targeted with NSO Group's Spyware," Citizen Lab Research Report No. 117, University of Toronto, March 2019.

Suggested Readings and other material

Bill Marczak, Geoffrey Alexander, Sarah McKune, John Scott-Railton, and Ron Deibert. "**Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware,**" Citizen Lab Research Brief No. 102, December 2017.

Ronald Deibert, "Evidence that Ethiopia is Spying on Journalists Shows Commercial Spyware is out of Control," *Wired*, December 6, 2017.

60 Minutes. CEO of Israeli spyware-maker NSO on fighting terror, Khashoggi murder, and Saudi Arabia.

Session 7: Regulating "Dual-Use" Technologies (Feb 25)

David Kaye. "Surveillance and human rights – Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression." (May 28, 2019). *Human Rights Council.* A/HRC/41/35. Available here.

Siena Anstis, Ronald J. Deibert, John Scott-Railton, “A Proposed Response to the Commercial Surveillance Emergency,” Lawfare, July 19, 2019. https://www.lawfareblog.com/proposed-response-commercial-surveillance-emergency

Penney, J., McKune, S., Gill, L., and Deibert, R. “Advancing human-rights-by-design in the dual-use technology industry,” Journal of International Affairs 71.2 (2018): 103-110.

Suggested Readings and other material

Sven Herpig. “A Framework for Government Hacking in Criminal Investigations.” (October 2018). *Stiftung Neue Verantwortung.* Available here.

Siena Anstis, Sharly Chan, Adam Senft, and Ron Deibert. “Annotated Bibliography, Dual Use Technologies: Network Traffic Management and Device Intrusion for Targeted Monitoring.” (September 2019). *Citizen Lab.* Available here.

Session 8: Disinformation Ops (March 3)

Leber, A., & Abrahams, A. (n.d.). A Storm of Tweets: Social Media Manipulation During the Gulf Crisis. Review of Middle East Studies, 1-18. doi:10.1017/rms.2019.45 https://www.cambridge.org/core/journals/review-of-middle-east-studies/article/storm-of-tweets-social-media-manipulation-during-the-gulf-crisis/56F18499A63115DF038BF3157578DCF2

Adam Hulcoop, John Scott-Railton, Peter Tanchak, Matt Brooks, and Ron Deibert. “**Tainted Leaks: Disinformation and Phishing with a Russian Nexus**,” Citizen Lab Research Brief No. 92, May 2017

Gabrielle Lim, Etienne Maynier, John Scott-Railton, Alberto Fittarelli, Ned Moran, and Ron Deibert. “Burned After Reading: Endless Mayfly’s Ephemeral Disinformation Campaign,” Citizen Lab Research Report No. 118, University of Toronto, May 2019.

Session 9: Stalkerware (March 10)

Cynthia Khoo, Kate Robertson, and Ron Deibert. “Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications,” Citizen Lab Research Report No. 121, University of Toronto, June 2019.

Christopher Parsons, Adam Molnar, Jakub Dalek, Jeffrey Knockel, Miles Kenyon, Bennett Haselton, Cynthia Khoo, and Ron Deibert. “The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry,” Citizen Lab Research Report No. 120, University of Toronto, June 2019.

Session 10: Transparency and Accountability (March 17)

Andrew Hilts, Christopher Parsons, and Masashi Crete-Nishihata. "Approaching Access: A Look at Consumer Personal Data Requests in Canada," Citizen Lab Research Report No. 106, University of Toronto, February 2018.

Petra Molnar and Lex Gill. "Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System," Citizen Lab and International Human Rights Program (Faculty of Law, University of Toronto) Research Report No. 114, University of Toronto, September 2018.

Access My Info (Canada): https://accessmyinfo.ca/#home

Suggested Readings and other material

Ronald Deibert, "Clicking I Accept Doesn't Mean You Surrender Right To Know How A Company Uses your Data," *CBC*, June 29, 2016.

Parsons, Christopher; and Molnar, Adam. (2017). "Government Surveillance Accountability: The Failures of Contemporary Canadian Interception Reports," Canadian Journal of Law and Technology. Available at: https://ojs.library.dal.ca/CJLT/article/view/9007

Parsons, Christopher. (2017). "The (In)effectiveness of Voluntarily Produced Transparency Reports," Business & Society. Available at: https://journals.sagepub.com/doi/10.1177/0007650317717957

Session 11: Threat Modeling / Security Planner / Protect the Net (March 24)

Security Planner: https//securityplanner.org/ Take a tour through Security Planner and come to class prepared to discuss threat modeling based on the resources at EFF.

How do you protect yourself against digital threats? How do you even know what those threats are in the first place, and which are most relevant to you? During this class, Matthew Braga will join us to talk about common digital threats you might face today, and steps that you can take to protect yourselves online. Matthew is the project manager of Security Planner, an accessible online resource for digital security advice created by the Citizen Lab. We'll cover some basic security hygiene that everyone should and can do (if you're not already!). We'll also discuss threat modelling — what it is, and when/how/why to do it — with lots of time for questions. Students will be encouraged to try and follow some of Security Planner's recommendations for themselves.

Here are some helpful resources you may wish to consult ahead of time (and keep handy for future reference):
- Security Planner
- EFF's guide to creating a security plan
- The Vice guide to not getting hacked
- A long list of up-to-date digital security resources

And here are some recent stories to get you thinking about some novel/recent threats, and how they may (or may not) apply to you:

- NYT: Hackers Hit Twitter C.E.O. Jack Dorsey in a 'SIM Swap.' You're at Risk, Too.
- Wired: Facebook Removes Accounts With AI-Generated Profile Photos
- Motherboard: We Tested Ring's Security. It's Awful
- NYT: It Seemed Like a Popular Chat App. It's Secretly a Spy Tool.
- Citizen Lab: The Predator in Your Pocket
- Bloomberg: Silicon Valley Is Listening to Your Most Intimate Moments
- Wired: How Apple and Amazon Security Flaws Led to My Epic Hacking (an old one, but some of this is still relevant today)

Session 12: Paper Discussions (March 31)
FINAL PAPER DUE