Course Syllabus, Version 08.09.2023

GRAD-E1308: States and the Control of Cyberspace
Area of Concentration(s): Management & Organisation

General information

Course Format	Onsite
Instructor(s)	Anita Gohdes
Instructor's e-mail	
Assistant (if applicable)	Dayna Sadow
Instructor's Office Hours	Tuesdays, 15-16h To make an appointment, please email Dayna Sadow **IMPORTANT**: **Please indicate if you would like to meet online or in person!**

General Readings

The reading for every session can be overwhelming when read in one sitting. I encourage you to space out the readings over multiple days.

- Do take a look at the additional literature, especially if you're thinking about writing your final essay in this area.

There are **no** general required readings. But if you are interested in getting acquainted with the topic, these books are a useful place to start:

- Roberts, Margaret E. (2018) Censored: distraction and diversion inside China's Great Firewall. Princeton University Press.
- Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2011). Access contested: security, identity, and resistance in Asian cyberspace. MIT Press.
- Zetter, Kim (2014). Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon. Broadway books.

Podcast related to topics covered:

- BBC - The Lazarus Heist
- The Guardian Today in Focus: 5 Part Report on The Pegasus Project. (first episode here)
- Motherboard CYBER Podcast
- Moderated Content (by Evelyn Douek)
- Kill Switch (by Access Now)

- ## Session Overview

Course session times and dates can be found in the Course Plan on *MyStudies*.

Session	Session Title
1	**Introduction: Why control the Internet?**
2	**Domestic control I: Understanding government behaviour**
3	**Domestic control II: Networked authoritarianism**
4	**Domestic control III: Censorship and Distraction**
5	**Domestic control IV: Surveillance**
6	**At home and abroad: Repression and the Internet**
Mid-term Exam Week: 16. – 20.10.2023 – no class	
7	**At home and abroad: Control and Market interests**
8	**Foreign control I: Offense, defense, and the role of cyber**
9	**Foreign control II: Election interference**
10	**International control I: Weaponized Interdependence**
11	**International control II: The politics of infrastructure**
12	**International control III: The push for Cyber Sovereignty**
Final Exam Week: 11. – 15.12.2023 – no class	

- ## Course Sessions and Readings

All readings will be accessible on the Moodle course site before semester start. In the case that there is a change in readings, students will be notified by email.

Required readings are to be read and analysed thoroughly. Optional readings are intended to broaden your knowledge in the respective area and it is highly recommended to at least skim them.

Session 1: Introduction: Why control the Internet?	
Required Readings	• Eric E. Schmidt and Jared Cohen. 2014. "The Future of Internet Freedom" *The New York Times*: https://www.nytimes.com/2014/03/12/opinion/the-future-of-internet-freedom.html • Larry Diamond. Liberation technology. *Journal of Democracy*, 21(3): 69–83, 2010.

Session 2: Domestic control I: Understanding government behaviour	
Required Readings	• Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, and Janice Gross Stein (eds) *Access denied: The practice and policy of global internet filtering*. Cambridge, MA: MIT Press, 2008, chapter 1 and chapter 2. • Pick two country summaries from this report to read in preparation for class: OutRight Action International, Citizen Lab, and OONI. 2021. No Access: LGBTIQ Website Censorship in Six Countries. URL: https://citizenlab.ca/2021/08/no-access-lgbtiq-website-censorship-in-six-countries/
Optional Readings	• Wu, Tim, and Jack Goldsmith. "Who Controls the Internet–Illusions of a Borderless World." (2006). Oxford University Press, chapter 5. URL: http://cryptome.org/2013/01/aaron-swartz/Who-Controls-Net.pdf

Session 3: Domestic control II: Networked authoritarianism	
Required Readings	• Levitsky, Steven, and Lucan A. Way. "Elections without democracy: The rise of competitive authoritarianism." *Journal of democracy* 13.2. 2002.: 51-65. • Rebecca MacKinnon. “China’s" networked authoritarianism"”. *Journal of Democracy*, 22(2): 32–46, 2011. • Jaclyn A. Kerr. “Rewiring Authoritarianism: The Evolution of Internet Policy in Putin’s Russia *Working Paper,* 2016.
Optional Readings	• Seva Gunitsky. Corrupting the cyber-commons: Social media as a tool of autocratic stability. *Perspectives on Politics*, 13:42–54, 3 2015. doi: 10.1017/S1537592714003120. URL http://journals.cambridge.org/article_S1537592714003120 • Kalathil, Shanthi, and Taylor C. Boas. *Open networks, closed regimes: The impact of the Internet on authoritarian rule*. Carnegie Endowment, 2010. • Chen, Jidong, and Yiqing Xu. "Why do authoritarian regimes allow citizens to voice opinions publicly?" The Journal of Politics 79.3 (2017): 792-803.

Session 4: Domestic control III: Censorship and distraction	
Required Readings	***This session focuses on China.*** • King, Gary, Jennifer Pan, and Margaret E. Roberts. "How censorship in China allows government criticism but silences collective expression." American Political Science Review 107.2 (2013): 326-343. • King, Gary, Jennifer Pan, and Margaret E. Roberts. How the Chinese government fabricates social media posts for strategic distraction, not engaged argument. *American Political Science Review*, 2017. • Pan, Jennifer. 2017. “How Market Dynamics of Domestic and Foreign Social Media Firms Shape Strategies of Internet Censorship.” Problems of Post-Communism 64(3–4): 167–88.

Optional Readings	• Liu, Jun, and Jingyi Zhao. "More than plain text: Censorship deletion in the Chinese social media." *Journal of the Association for Information Science and Technology* (2020). • Rita Liao and Catherine Shu. 2022. “Great Wall of porn obscures China protest news on Twitter”. URL: https://techcrunch.com/2022/11/28/great-wall-of-porn-obscures-china-protest-news-on-twitter/ • Xu, Xueyang, Z. Morley Mao, and J. Alex Halderman. "Internet censorship in China: Where does the filtering occur?." *International Conference on Passive and Active Network Measurement*. Springer, Berlin, Heidelberg, 2011. • Gohdes, Anita R. "Pulling the plug: Network disruptions and violence in civil conflict." *Journal of Peace Research* 52.3 (2015): 352-367. • Lorentzen, Peter. "China's strategic censorship." *American Journal of Political Science* 58.2 (2014): 402-414.

Session 5: Domestic control IV: Surveillance	
Required Readings	***This session draws on examples from Ethiopia, Zimbabwe, and Pakistan*** • **Focus on Sections I and II:** Horne, Felix, and Cynthia Wong. "They Know Everything We Do": Telecom and Internet Surveillance in Ethiopia. *Human Rights Watch*, 2014: https://www.hrw.org/sites/default/files/reports/ethiopia0314_ForUpload_0.pdf • **Scan this report:** Haroon Baloch and Amjad Qammar 2017. “Dangers of Digital Surveillance: An account on self-censorship by journalists and human rights defenders in Pakistan”, Bytes for All, Pakistan. https://bytesforall.pk/publication/dangers-digital-surveillance • The Engine Room: “Digital ID in Zimbabwe: A case study”: https://digitalid.theengineroom.org/assets/pdfs/[English]%20Zimbabwe%20Case%20Study%20-%20DigitalID%20-%20The%20Engine%20Room.pdf
Optional Readings	• Motherboard CYBER Podcast: CYBER: Iran’s AI-Powered Surveillance State: https://www.vice.com/en/article/epze9w/cyber-irans-ai-powered-surveillance-state • “Evidence of Government Surveillance in Mexico Continues to Mount” - Global Voices Advox: https://advox.globalvoices.org/2017/09/20/evidence-of-government-surveillance-in-mexico-continues-to-mount/ • Browne, Simone. 2015. Dark matters: On the surveillance of blackness. Duke University Press. **AVAILABLE IN THE LIBRARY OR HERE AS E-BOOK:** http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=1057532

Session 6: At home and abroad I: Repression and the Internet	
Required Readings	***This session draws on examples from Syria, Saudi Arabia, and China*** • Gohdes, Anita R. 2020: "Repression technology: Internet accessibility and state violence", *American Journal of Political Science.* 64: 488-503. URL: https://onlinelibrary.wiley.com/doi/abs/10.1111/ajps.12509 • Pan, Jennifer, and Alexandra A. Siegel. "How Saudi crackdowns fail to silence online dissent." American Political Science Review 114.1 (2020): 109-125. URL: https://www.cambridge.org/core/journals/american-political-science-review/article/abs/how-saudi-crackdowns-fail-to-silence-online-dissent/1BA13DF8FD5D04EC181BCD4D1055254B Podcasts: • The New York Times Daily Podcast, May 6 2019: The Chinese Surveillance State, Part 1 https://www.nytimes.com/2019/05/06/podcasts/the-daily/china-surveillance-uighurs.html • The New York Times Daily Podcast, May 2 2019: The Chinese Surveillance State, Part 2 https://www.nytimes.com/2019/05/07/podcasts/the-daily/china-uighurs-internment-camps-surveillance.html
Optional Readings	• Greitens, Sheena Chestnut, Myunghee Lee, and Emir Yazici. "Counterterrorism and Preventive Repression: China's Changing Strategy in Xinjiang." *International Security* 44.3 (2020): 9-47. • Moss, Dana M. "The ties that bind: Internet communication technologies, networked authoritarianism, and 'voice' in the Syrian diaspora." *Globalizations* 15.2 (2018): 265-282. • Xu, Xu. "To repress or to co-opt? Authoritarian control in the age of digital surveillance." *American Journal of Political Science* 65.2 (2021): 309-325. • Web of Impunity - The killings Iran's internet shutdown hid: https://iran-shutdown.amnesty.org/. Joint research by Amnesty International, the Hertie School, and Internet Outage Detection and Analysis (IODA). 2020.

Mid-term Exam Week: 16. – 20.10.2023 – no class

Session 7: At home and abroad II: Control and Market interests	
Required Readings	***This session draws on examples from various African countries*** • Mare, Admire. " State-Ordered Internet Shutdowns and Digital Authoritarianism in Zimbabwe." *International Journal of Communication* 14 (2020): 20. https://ijoc.org/index.php/ijoc/article/download/11494/3184 • Nothias, Toussaint. 2020. "Access Granted: Facebook's Free Basics in Africa." Media, Culture & Society 42(3): 329–48. URL: https://journals.sagepub.com/doi/full/10.1177/0163443719890530 • Yeboah, Kofi 2020: "Silicon Valley tech giants race to build Africa's internet infrastructure. Should Africa worry? " https://globalvoices.org/2020/06/05/silicon-valley-tech-giants-race-to-build-africas-internet-infrastructure-should-africa-worry/

Optional Readings	• Adegoke, Yinka 2020: "How Google's balloons are bringing internet to new parts of Kenya" https://qz.com/africa/1879038/how-googles-balloons-are-bringing-internet-to-new-parts-of-kenya/ • Podcast: Nanjira Sambuli -World Wide Web Foundation - The Dickens Olewe podcast: https://open.spotify.com/episode/4QTKk8mYZ3z2LtZRiES5Cj?si=QkrbHhjHRoKGLxuT_HLhZg&dl_branch=1 • Flyverbom, Mikkel, Ronald Deibert, and Dirk Matten. "The governance of digital technology, big data, and the internet: new roles and responsibilities for business." *Business & Society* 58.1 (2019): 3-19. • Brian Ekdale & Melissa Tully (2019) African Elections as a Testing Ground: Comparing Coverage of Cambridge Analytica in Nigerian and Kenyan Newspapers, African Journalism Studies, 40:4, 27-43, https://doi.org/10.1080/23743670.2019.1679208 • "Surveillance and censorship: The impact of technologies on human rights" European Parliament – Directorate General for External Policies Policy Department. Url: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/549034/EXPO_STU(2015)549034_EN.pdf

Session 8: Foreign control I: Offense, defense, and the role of cyber	
Required Readings	• Slayton, Rebecca. 2017. "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment." International Security 41(3): 72–109. • Kostyuk, Nadiya, and Aaron Brantly. 2022. "War in the Borderland through Cyberspace: Limits of Defending Ukraine through Interstate Cooperation." *Contemporary Security Policy* 43(3): 498–515. https://www.tandfonline.com/doi/full/10.1080/13523260.2022.2093587. • Burgess, Matt. 2022. "Russia Is Taking Over Ukraine's Internet." *WIRED Magazine*. https://www.wired.com/story/ukraine-russia-internet-takeover/.
Optional Readings	• F-Secure Podcast: Episode 20 | Defining Cyber Warfare, with Mikko Hypponen: https://blog.f-secure.com/podcast-cyber-warfare-mikko/ • Motherboard Cyber Podcast: Why There's No Need to Panic About a 'Cyber 9/11': https://www.vice.com/en_us/article/ywy3z7/no-need-to-panic-about-cyber-911 • Giles, Keir, and William Hagestad. "Divided by a common language: Cyber definitions in Chinese, Russian and English." *2013 5th International Conference on Cyber Conflict (CYCON 2013)*. IEEE, 2013.

Session 10: Foreign control II: Election interference	
Required Readings	***<u>This session draws on examples from the US and various European elections</u>*** • Brattberg, Erik, and Tim Maurer. Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks. Vol. 23. Carnegie Endowment for International Peace, 2018. URL • Benkler, Yochai, Robert Faris, and Hal Roberts. Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics. Oxford University Press, 2018., chapter 8. • Francois, Camille, and Herb Lin. 2021. "The Strategic Surprise of Russian Information Operations on Social Media in 2016 in the United States: Mapping a Blind Spot." *Journal of Cyber Policy* 6(1): 9–30. https://www.tandfonline.com/doi/full/10.1080/23738871.2021.1950196 (September 6, 2021).
Optional Readings	• Lutscher, Philipp M., et al. "At home and abroad: The use of denial-of-service attacks during elections in nondemocratic regimes." *Journal of Conflict Resolution* 64.2-3 (2020): 373-401. • Chinese Cyber-Operatives Boosted Taiwan's Insurgent Candidate – Foreign Policy: https://foreignpolicy.com/2019/06/26/chinese-cyber-operatives-boosted-taiwans-insurgent-candidate/ • Methods of Foreign Electoral Interference - EU vs DISINFORMATION: https://euvsdisinfo.eu/methods-of-foreign-electoral-interference/ • How Russia Hacks Elections in the US and Around the World: https://www.wired.com/story/russia-election-hacking-playbook/

Session 10: International Control I II: Weaponizing Interdependence	
Required Readings	• Farrell, Henry, and Abraham L. Newman. "Weaponized interdependence: How global economic networks shape state coercion." *International Security* 44.1 (2019): 42-79. • Farrell, Henry, and Abraham Newman. "Weaponized Globalization: Huawei and the Emerging Battle over 5G Networks." *Global Asia* 14.3 (2019): 8-12.

Session 11: International control II: The politics of infrastructure	
Required Readings	• Laura DeNardis *The Internet in everything: Freedom and security in a world with no off switch*. Yale University Press, 2020, chapter 8. • **<u>Chapter TBD!!</u>** Musiani, Francesca, Derrick L. Cogburn, Laura DeNardis, and Nanette S. Levinson. 2016. The Turn to Infrastructure in Internet Governance. New York: Palgrave Macmillan. • Geuns, Suzanne van, and Corinne Cath-Speth. 2020. "How Hate Speech Reveals the Invisible Politics of Internet Infrastructure." Brookings. https://www.brookings.edu/techstream/how-hate-speech-reveals-the-invisible-politics-of-internet-infrastructure
Optional Readings	• Bruce Schneier. *Data and Goliath: The hidden battles to collect your data and control your world*. WW Norton & Company, 2015, chapters 12+13.

Session 12: International control III: The push for Cyber Sovereignty	
Required Readings	• Glen, Carol M. "Internet governance: territorializing cyberspace?." *Politics & Policy* 42.5 (2014): 635-657. • Yeli, Hao. "A three-perspective theory of cyber sovereignty." Prism 7.2 (2017): 108-115. • **TBD**
Optional Readings	• Shen, Yi. "Cyber sovereignty and the governance of global cyberspace." *Chinese Political Science Review* 1.1 (2016): 81-93. • Governing Cyberspace: State Control vs. The Multistakeholder Model: URL: https://www.belfercenter.org/publication/governing-cyberspace-state-control-vs-multistakeholder-model • Shen, Hong. "China and global internet governance: toward an alternative analytical framework." Chinese Journal of Communication 9.3 (2016): 304-324. • Stevens, Tim. 2015a*. "BRICS Set Out Vision for International Information Security." Thesigers. July 1. Available online at http://thesigers.com/analysis/2015/7/3/brics-set-out-vision-for-international-information-security*