Hertie School

Master of International Affairs/Master of Public Policy
Fall Semester 2020
Course Syllabus, Version 31.08.2020

GRAD-E1308: States and the Control of Cyberspace

Concentration: Management & Organisation

Prof. Dr. Anita Gohdes

1. General information

[…]

2. Grading and Assignments

[…]

3. General Readings

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.

4. Session Overview

Session	Session Date	Session Title
1	07.09.2020	Introduction: Why control the Internet?
2	14.09.2020	Domestic control I: Understanding government behaviour
3	21.09.2020	Domestic control II: Networked authoritarianism
4	28.09.2020	Domestic control III: Censorship and Distraction
5	05.10.2020	Domestic control IV: Surveillance
6	12.10.2020	At home and abroad: Repression and the Internet
Mid-term Exam Week: 19.10 - 23.10.2020 – no class		
7	26.10.2020	At home and abroad: The role of private companies
8	02.11.2020	Foreign control I: Cyberwar!?
9	09.11.2020	Foreign control II: A closer look at Cyberattacks: Stuxnet, Estonia 2007, Ukraine 2015
10	16.11.2020	Foreign control III: Election interference
11	23.11.2020	International control I: Cyber Sovereignty and Cybersecurity Governance
12	30.11.2020	International control II: Accountability and Transparency
Final Exam Week: 14.12 - 18.12.2020 – no class		

5. Course Sessions and Readings

Session 1: Introduction: Why control the Internet?	
Learning Objective	Why are governments interested in controlling the Internet? What's at stake?
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	
Learning Objective	What do governments want? How can we understand their behaviour? How can we evaluate their behaviour? We will look at this by examining the techniques states used to control the Internet in the early 2000s. What kind of content did states focus on back then? What does this teach us about the origins of Internet control?
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 the book to read in preparation for class: https://archive.org/details/AccessDenied_201701
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	
Learning Objective	What institutional framework motivates states to engage in 'networked authoritarianism'? What are some of the key strategies used to promote 'networked authoritarianism'? What role does social media play? *This session will focus on Russia as a case example.*
Required Readings	- Levitsky, Steven, and Lucan A. Way. "Elections without democracy: The rise of competitive authoritarianism." *Journal of democracy* 13.2. 2002.: 51-65. - 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 - Jaclyn A. Kerr. "Rewiring Authoritarianism: The Evolution of Internet Policy in Putin's Russia *Working Paper*, 2016
Optional Readings	- Rebecca MacKinnon. China's" networked authoritarianism". *Journal of Democracy*, 22(2): 32–46, 2011 - 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	
Learning Objective	What is the logic of censoring content on the Internet? What 'flavours' of censorship exist? How does censoring on the Internet work? How do citizens react to censorship? *This session will focus on China as a case example.*
Required Readings	- 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. - How China Walled Off the Internet - The New York Times: https://www.nytimes.com/interactive/2018/11/18/world/asia/china-internet.html
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). - 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.

	- Analysis how Iran's internet shutdown gagged local freedom of speech: https://medium.com/@techjournalism/how-irans-internet-block-gagged-local-online-protests-5dcf5dfaod19 - 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. - Haroon Baloch, Maria Xynou, and Arturo Filastò 2017. "Internet Censorship in Pakistan: Findings from 2014-2017", Bytes for All, Pakistan. https://bytesforall.pk/publication/internet-censorship-pakistan-findings-2014-2017

Session 5: Domestic control IV: Surveillance	
Learning Objective	Even though governments all over the world have started to use digital surveillance in their attempts to control the Internet, the specific technology used by governments varies widely with respect to its level of sophistication. We'll explore a number of examples and investigate the motivation and consequences of surveillance more broadly. For this session, please read the two papers and listen to the two podcasts listed below. *This session will look at examples from Ethiopia, Zimbabwe, and the US.*
Required Readings	- 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 - 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 - Zetter, Kim: "How Cops Can Secretly Track Your Phone - A guide to stingray surveillance technology, which may have been deployed at recent protests." https://theintercept.com/2020/07/31/protests-surveillance-stingrays-dirtboxes-phone-tracking/
Optional Readings	- [Movie]: Citizen Four: https://citizenfourfilm.com/ - Browne, Simone. 2015. Dark matters: On the surveillance of blackness. Duke University Press. - How China Is Changing Your Internet: https://www.nytimes.com/video/technology/100000004574648/china-internet-wechat.html - Susan Landau (Aug 2013), "Making sense from Snowden: What's significant in the NSA Surveillance revelations," IEEE Security & Privacy 111, no. 4. https://www.computer.org/cms/Computer.org/ComputingNow/pdfs/MakingSenseFromSnowden- IEEESecurityAndPrivacy.pdf - 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

	- Bei Qin, David Strömberg, and Yanhui Wu. Why does china allow freer social media? Protests versus surveillance and propaganda. Journal of Economic Perspectives, 31(1): 117–140, 2017 - "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/

Session 6: At home and abroad: Repression and the Internet	
Learning Objective	How does Control of the Internet affect other forms of government repression? And does digital repression 'work'? *This session will look at examples from Syria, Saudi Arabia, and China.*
Required Readings	- Gohdes, Anita R. 2020: "Repression technology: Internet accessibility and state violence", *American Journal of Political Science.* - Pan, Jennifer, and Alexandra A. Siegel. 2020: "How Saudi crackdowns fail to silence online dissent." *American Political Science Review* 114.1: 109-125. - 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. 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	- Moss, Dana M. "The ties that bind: Internet communication technologies, networked authoritarianism, and 'voice' in the Syrian diaspora." *Globalizations* 15.2 (2018): 265-282.

Mid-term Exam Week: 19 – 23.10.2020 – no class

Session 7: At home and abroad: The role of private companies	
Learning Objective	What role do private companies play in providing and controlling Internet access? How do they interact with state actors? What policy responses are trying to address these tensions? *This session will look at examples from Zimbabwe, Kenya, and other African countries.*
Required Readings	- 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 - 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/ - 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: - Motherboard Cyber Podcast: The Politician Fighting The Spyware Industry: https://www.vice.com/en_us/article/8xzk4x/the-politician-fighting-the-spyware-industry
Optional Readings	- What is the Wassenaar Arrangement? URL: https://www.wassenaar.org/the-wassenaar-arrangement/ - The Wassenaar Arrangement Control Lists, Category 5: https://www.wassenaar.org/app/uploads/2019/consolidated/WA-DOC-18-PUB-001-Public-Docs-Vol-II-2018-List-of-DU-Goods-and-Technologies-and-Munitions-List-Dec-18.pdf - Citizen Lab *Planet blue coat: Mapping global censorship and surveillance tools*., 2013. URL https://citizenlab.ca/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/ - 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. - Zittrain, Jonathan, and John Palfrey. "Reluctant gatekeepers: Corporate ethics on a filtered Internet." *Access Denied: The Practice and Policy of Global Internet Filtering* (2008): chapter 5. - "Here Are All the Sketchy Government Agencies Buying Hacking Team's Spy Tech", Motherboard. URL: https://www.vice.com/en_us/article/nzeg5x/here-are-all-the-sketchy-government-agencies-buying-hacking-teams-spy-tech - "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: Cyberwar!?	
Learning Objective	What do we mean when we talk about cyberattacks and cyber warfare? What are the key advantages and challenges for governments contemplating the use of cyberattacks? And should we trust the cyber hype?
Required Readings	- Rid, Thomas. "Cyber war will not take place." *Journal of strategic studies* 35.1 (2012): 5-32 - Stone, John. "Cyber war will take place!." *Journal of Strategic Studies* 36.1 (2013): 101-108. Podcast: - F-Secure Podcast: Episode 20 | Defining Cyber Warfare, with Mikko Hypponen: https://blog.f-secure.com/podcast-cyber-warfare-mikko/
Optional Readings	- 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 - Sanger, David E. (2019) *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. Broadway Books. - 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 9: Foreign control II: Case studies	
Learning Objective	We will discuss three important incidences of cyberattacks: *Stuxnet, the 2007 cyberattacks on Estonia, the 2015 cyberattack on the Ukrainian power grid.*
Required Readings	- Zetter, Kim (2014). *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon*. Broadway books, chapter 4 - Ottis, Rain. "Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective." Proceedings of the 7th European Conference on Information Warfare. 2008. URL: http://tiny.cc/kzfm9y - Analysis of the Cyber Attack on the Ukrainian Power Grid: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf Podcast: - Motherboard Cyber Podcast: How to track malware: https://play.acast.com/s/cyber/howtotrackmalware
Optional Readings	- [Movie]: Zero Days (a movie about Stuxnet): http://www.zerodaysfilm.com/ - Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid

Session 10: Foreign control III: Election interference	
Learning Objective	What means do governments use to interfere in foreign countries' electoral politics? Do these means work? What can be done about it? *This session includes examples from European countries, the US, and a cross-national comparative analysis.*
Required Readings	- 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. https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435 - Benkler, Yochai, Robert Faris, and Hal Roberts. Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics. Oxford University Press, 2018., chapter 8. - 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.
Optional Readings	- 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 11: International control I: Cyber Sovereignty and cyber governance	
Learning Objective	We will explore the concept of cyber sovereignty and look at how cyber governance occurs via domestic and international policies, and why this field of Internet governance is becoming more and more politicized.
Required Readings	- Glen, Carol M. "Internet governance: territorializing cyberspace?." *Politics & Policy* 42.5 (2014): 635-657. - Shen, Yi. "Cyber sovereignty and the governance of global cyberspace." *Chinese Political Science Review* 1.1 (2016): 81-93. - Beginner's guide to ICANN: https://www.icann.org/en/system/files/files/participating-08nov13-en.pdf Podcast: - Himal Southasian Podcast Channel: Interview with Anita Gurumurthy on data and surveillance capitalism https://www.himalmag.com/himal-interviews-between-big-data-and-big-brother-2020/
Optional Readings	- Governing Cyberspace: State Control vs. The Multistakeholder Model: URL: https://www.belfercenter.org/publication/governing-cyberspace-state-control-vs-multistakeholder-model

	- Baezner, Marie; Robin, Patrice (2018). Cyber sovereignty and Data sovereignty, Version 2, Cyberdefense Trend Analysis, Center for Security Studies (CSS), ETH Zürich. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/20180907_MB_TA_Cyber%20sovereignty_V2_rev.pdf - Mueller, M. L. (2011). China and global Internet governance: A tiger by the tail. *Access contested: Security, identity, and resistance in Asian cyberspace*, 177-194. - Shen, Hong. "China and global internet governance: toward an alternative analytical framework." Chinese Journal of Communication 9.3 (2016): 304-324. - *Stevens, Tim. 2012.* "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace." Contemporary Security Policy 33 (1): 148-170. Accessed on January 30, 2017. Available online at http://www.tandfonline.com/doi/abs/10.1080/13523260.2012.659597

Session 12: International control II: Cybersecurity Governance, Accountability and Transparency	
Learning Objective	How can we design rules, standards, and policies that promote accountability and transparency in cyberspace?
Required Readings	- TBD - Bruce Schneier. *Data and Goliath: The hidden battles to collect your data and control your world*. WW Norton & Company, 2015, chapter 12+13. - TBD
Optional Readings	- TBD

Final Exam Week: 14 - 18.12.2020 – no class