

Course Title: 91195 – Forecasting and Analyzing Conflict and Instability

Term: Spring 2021

Instructor: Matteo Giglioli

Email: matteo.giglioli@unibo.it

Sessions: Thursdays, 9-11am
Fridays, 9-11am

Office hours: Thursdays, 6-7pm, by appointment

Description: This year's course will approach the topic of conflict and instability from the point of view of the functioning of our contemporary digital societies. The overarching notion which will guide us through the course is *social trust*, and specifically the systemic lack of it and the crisis of the notion itself in multiple spheres of our everyday experience. The course will trace the disruption generated by new technologies in eight politically and socially strategic ambits; in each, it will attempt to highlight how key actors either attempt to rebuild the bases for trustworthiness or tend to exploit mistrust for their own ends.

Prerequisites: This is an advanced research course. While there are no formal prerequisites, participants are expected to be acquainted with basic concepts in political science, international relations, economics, and quantitative reasoning techniques; furthermore, they should be self-starters, capable of orienting themselves quickly in large amounts of new information, and curious about the role of IT in our understanding of contemporary politics. Excellent written and spoken English is indispensable.

Readings: The material for the course is outlined below, week by week. Required readings form the basis for each week's lectures; thus, it is advisable to read them before class. Suggested further readings are presented as a guide for those interested in exploring a particular topic in greater depth.

Assessment: *Non-attendees* will sit an oral examination. The examination will cover all material included in the required reading for the course. The examination will be offered at various different dates within the official exam periods, as is customary. *Attendees* will need to declare their intention to follow the course by the end of the second session (i.e., by the end of week one). They will be required to attend all lectures. The maximum number of sessions that may be missed (barring documented emergencies) in order to maintain attendee status is 2. Attendee performance will be assessed on the basis of a final research paper. The final research paper will be an original, 5000-word-long essay. Its aim will be to apply the general knowledge gained in the course to an empirical case-study. The topic of the research paper must be approved by the instructor before the Easter break. The research paper will be due

exactly one week after the final session of the course. No extensions will be offered. Style, formatting, and submission details to follow.

COURSE CALENDAR

		Thursdays	Fridays
<i>Week 1</i> Trust as a social-science problem	Feb. 25 & 26	Course introduction	Crises of democracy, neoliberalism, the global order, and community
Deadline to confirm attendee status			
<i>Week 2</i> Surveillance & archives	Mar. 4 & 5	Search and access to the digital archive	Data science and information overload
<i>Week 3</i> Information & the public sphere	Mar. 11 & 12	Misinformation and fake news	Generic trust in the public sphere
<i>Week 4</i> Organizational behavior & relations	Mar. 18 & 19	Leaks & whistleblowers, industrial espionage	Legitimacy and institutional reputations
<i>Week 5</i> Domestic politics	Mar. 25 & 26	Online populism, mobilization, astroturfing	Election management
Deadline to confirm paper topic			
<i>Week 6</i> Comparative policymaking	Apr. 8 & 9	Digital policy regulatory fora, regulatory capture	Tech company nationality
<i>Week 7</i> IR & power politics	Apr. 15 & 16	Information warfare	State-sponsored hacking, hacking as a power resource
<i>Week 8</i> Online sociability	Apr. 22 & 23	Digital charismatic communities, belief entrepreneurship	Digital discrimination (domestic and international)
<i>Week 9</i> Political economy & visibility	Apr. 29 & 30	Anonymity, visibility, wealth (financial flows)	Gig economy careers, platform monopolies and exploitation
<i>Week 10</i> Present & future challenges	May 6 & 7	Civic responsibility	Course roundup
			Final paper due May 14, 7pm

READINGS

Week 1: Trust as a social-science problem

Required readings

None

Suggested readings

- Schneier, B., 2012. Liars and outliers: enabling the trust that society needs to thrive. Wiley, Indianapolis.
- Zuckerman, E., 2021. Mistrust: why losing faith in institutions provides the tools to transform them. W.W. Norton & Co., New York.

Week 2: Surveillance & archives

Required readings

- Couldry, N., Mejias, U.A., 2019. The costs of connection: how data is colonizing human life and appropriating it for capitalism, culture and economic life. Stanford University Press, Stanford, California, pp. 3-68.
- Henschke, A., 2017. Ethics in an age of surveillance: personal information and virtual identities. Cambridge University Press, New York, pp. 28-55, 89-125, 185-198.
- Lyon, D., 2011 (Ed.). Theorizing surveillance: the panopticon and beyond. Routledge, New York, pp. 69-94, 247-269, 270-295.

Suggested readings

- Bauman, Z., Lyon, D., 2013. Liquid Surveillance: A Conversation. Wiley, Oxford.
- Lyon, D., 2018. The culture of surveillance: watching as a way of life. Polity, Cambridge, UK.
- O'Neil, C., 2016. Weapons of math destruction: how big data increases inequality and threatens democracy. Crown, New York.
- Smith, R.E., 2019. Rage Inside the Machine: The Prejudice of Algorithms, and How to Stop the Internet Making Bigots of Us All. Bloomsbury Publishing Plc, London.

Week 3: Information & the public sphere

Required readings

- Bronner, G., 2015. Belief and misbelief asymmetry on the internet. ISTE Ltd/John Wiley and Sons, London, pp. 1-59.
- Howard, P.N., 2020. Lie machines: how to save democracy from troll armies, deceitful robots, junk news operations, and political operatives. Yale University Press, New Haven, pp. 1-81.
- Muirhead, R., Rosenblum, N.L., 2019. A lot of people are saying: the new conspiracism and the assault on democracy. Princeton University Press, Princeton, New Jersey, pp. 17-78.

Suggested readings

- Pomerantsev, P., 2019. This is not propaganda: adventures in the war against reality. PublicAffairs, New York.

Week 4: Organizational behavior & relations

Required readings

- Sagar, R., 2013. Secrets and leaks: the dilemma of state secrecy. Princeton University Press, Princeton, N.J., pp. 16-50, 103-180.

Scott, C.R., 2013. Anonymous agencies, backstreet businesses, and covert collectives: rethinking organizations in the 21st century. Stanford Business Books, an imprint of Stanford University Press, Stanford, California, pp. 1-24, 81-105, 160-196.

Suggested readings

Angwin, J., 2015. Dragnet nation: a quest for privacy, security, and freedom in a world of relentless surveillance, Times Books/Henry Holt & co., New York.

Coleman, E.G., 2014. Hacker, hoaxer, whistleblower, spy: the many faces of Anonymous. Verso, London; New York.

Eubanks, V., 2019. Automating inequality: how high-tech tools profile, police, and punish the poor. St. Martin's Press, New York.

Week 5: Domestic politics

Required readings

Benkler, Y., Faris, R., Roberts, H., 2018. Network propaganda: manipulation, disinformation, and radicalization in American politics. Oxford University Press, New York, pp. 3-99.

Jamieson, K.H., 2018. Cyberwar: how Russian hackers and trolls helped elect a president—what we don't, can't, and do know. Oxford University Press, New York, pp. 21-63.

Persily, N., Tucker, J.A. (Eds.), 2020. Social media and democracy: the state of the field, prospects for reform. Cambridge University Press, Cambridge, pp. 34-55, 286-312.

Woolley, S., Howard, P.N. (Eds.), 2019. Computational propaganda: political parties, politicians, and political manipulation on social media. Oxford University Press, New York, pp. 3-18.

Suggested readings

Howard, P.N., Hussain, M.M., 2013. Democracy's fourth wave? digital media and the Arab Spring. Oxford University Press, Oxford.

Sauter, M., 2014. The coming swarm: DDoS actions, hacktivism, and civil disobedience on the Internet. Bloomsbury, New York.

Tufekci, Z., 2017. Twitter and tear gas: the power and fragility of networked protest. Yale University Press, New Haven; London.

Week 6: Comparative policymaking

Required readings

Farrell, H., Newman, A., 2019. Of privacy and power: the transatlantic struggle over freedom and security. Princeton University Press, Princeton, New Jersey, pp. 39-124.

Murphy, M.H., 2019. Surveillance and the law: language, power, and privacy. Routledge, New York, pp. 1-73.

Yeung, K., Lodge, M. (Eds.), 2019. Algorithmic regulation. Oxford University Press, New York, pp. 203-223, 248-262.

Suggested readings

Deibert, R. (Ed.), 2008. Access denied: the practice and policy of global Internet filtering. MIT Press, Cambridge, Mass.

Deibert, R. (Ed.), 2010. Access controlled: the shaping of power, rights, and rule in cyberspace. MIT Press, Cambridge, Mass.

Deibert, R. (Ed.), 2012. Access contested: security, identity, and resistance in Asian cyberspace. MIT Press, Cambridge, MA.

El-Ariss, T., 2019. Leaks, hacks, and scandals: Arab culture in the digital age, Translation/transnation. Princeton University Press, Princeton, NJ.

Griffiths, J., 2019. Great Firewall of China: how to build and control an alternate vision of the internet. ZED Books LTD, London.

Week 7: IR & power politics

Required readings

- Buchanan, B., 2017. The cybersecurity dilemma: hacking, trust and fear between nations. Oxford University Press, Oxford, pp. 15-73.
- Lindsay, J.R., Cheung, T.M., Reveron, D.S. (Eds.), 2015. China and cybersecurity: espionage, strategy, and politics in the digital domain. Oxford University Press, New York, pp. 51-86, 138-162, 333-354.
- Maurer, T., 2018. Cyber mercenaries: the state, hackers, and power. Cambridge University Press, Cambridge, pp. 3-28, 123-150.
- Perkovich, G., Levite, A. (Eds.), 2017. Understanding cyber conflict: 14 analogies. Georgetown University Press, Washington, DC, pp. 231-247.

Suggested readings

- Buchanan, B., 2020. The hacker and the state: cyber-attacks and the new normal of geopolitics. Harvard University Press, Cambridge, Massachusetts.
- Greenberg, A., 2019. Sandworm: a new era of cyberwar and the hunt for the Kremlin's most dangerous hackers. Doubleday, New York.
- Levine, Y., 2018. Surveillance valley: the secret military history of the Internet. PublicAffairs, New York.

Week 8: Online sociability

Required readings

- Han, B.-C., 2015. The transparency society. Stanford Briefs, an imprint of Stanford University Press, Stanford, California, pp. 1-8, 15-20, 34-49.
- Marwick, A.E., 2013. Status update: celebrity, publicity, and branding in the social media age. Yale University Press, New Haven, pp. 73-244.

Suggested readings

- Guo, S. 2021. The evolution of the Chinese Internet: creative visibility in the digital public. Stanford University Press, Stanford, California.
- Phillips, W., 2015. This is why we can't have nice things: mapping the relationship between online trolling and mainstream culture. The MIT Press, Cambridge, Massachusetts.
- Quinn, Z., 2017. Crash override: how Gamergate (nearly) destroyed my life, and how we can win the fight against online hate. PublicAffairs, New York.

Week 9: Political economy & visibility

Required readings

- Brunton, F., 2019. Digital cash: the unknown history of the anarchists, utopians, and technologists who created cryptocurrency. Princeton University Press, Princeton, NJ, pp. 62-205.
- Mejias, U.A., 2013. Off the network: disrupting the digital world. University of Minnesota Press, Minneapolis, pp. 81-141.

Suggested readings

- Odell, J., 2019. How to do nothing: resisting the attention economy. Melville House, Brooklyn, NY.
- Turow, J., 2017. The aisles have eyes: how retailers track your shopping, strip your privacy, and define your power. Yale University Press, New Haven.

- Wu, T., 2016. The attention merchants: the epic scramble to get inside our heads. Alfred A. Knopf, New York.
- Zuboff, S., 2018. The age of surveillance capitalism: the fight for a human future at the new frontier of power. PublicAffairs, New York.

Week 10: Present & future challenges

Required readings

None

Suggested readings

- Doctorow, C., 2014. Information Doesn't Want to Be Free: Laws for the Internet Age. McSweeney's, New York.
- Webb, M., 2020. Coding democracy: how hackers are disrupting power, surveillance, and authoritarianism. MIT Press, Cambridge, Massachusetts.