FGV RI
ESCOLA DE RELAÇÕES INTERNACIONAIS

Digital Threats to Democracy

Monday 1st October – Saturday 6th October 2018

Course Description

Over the course of the past decade, anxieties have proliferated concerning the decay of democratic processes around the world. An important component of this 'crisis-of-democracy' narrative has focused on the emergence of new information and communications technologies and social media platforms. With the advent of big data – encompassing the collection of vast amounts of data and facilitation of new forms of surveillance, control, discrimination and manipulation by both government and corporate actors – threats to democracy have increasingly been perceived to manifest in a digital form.

In this course, we will examine how cyberspace is transforming the democratic landscape. Tackling issues ranging from digital interference in elections, cyber surveillance programmes, encryption, online speech governance, online political micro-targeting, and autonomous weapons systems, this course invites participants to reflect on the legal and policy implications of digital threats to democracy.

LECTURER

Barrie Sander
Postdoctoral Fellow
FGV School of International Relations
Barrie.Sander@graduateinstitute.ch

LOCATION

FGV EAESP
Escola de Administração de Empresas de São Paulo
Rua Itapeva 432, São Paulo
1 – 4 October, **Room 1209**
5 – 6 October, **Room 806**

Course Objectives

By the end of this course, students will develop:

- an insight into how cyberspace is transforming the democratic landscape around the world, including critically reflecting on the notions of democratic empowerment and democratic decay;
- an in-depth understanding of how different legal paradigms – including public international law, international human rights law and data protection law – offer the conceptual tools to respond to digital threats to democracy; and
- an ability to critically discuss some of the central tensions and controversies that have arisen in legal and policy debates concerning digital threats to democracy.

NB: A legal background is NOT required for this course.

Course Duration

The course will be delivered in **English** through **30 hours** of lectures divided across **six days**. The course includes a number of **guest speaker sessions** to provide participants with an insight into how different stakeholders are tackling digital threats to democracy in practice.

Participation

Participants on the course are required to attend at least 75% of all lectures and ensure they are prepared for in-class discussions by reading **the compulsory readings**. Further readings are optional. Readings will be accessible through Dropbox. If a participant is unable to attend a particular session, she or he should notify the course convener in advance by email.

Background Reading Materials

- SINGER, P.W., & FRIEDMAN, A., *Cybersecurity and Cyberwar* (Oxford University Press, 2014)
- TSAGOURIAS, N., & BUCHAN, R. (eds.), *Research Handbook on International Law and Cyberspace* (Edward Elgar, 2015)
- O'NEIL, C., *Weapons of Math Destruction* (Broadway Books, 2016)

Syllabus Outline

DAY 1. INTRODUCTION

MONDAY 1ST OCTOBER 2018, ROOM 1209, 18.30-23.00

SESSION 1 *CYBERSPACE: FOUNDATIONAL CONCEPTS*

What is 'cyberspace'? To what extent does cyberspace constitute a unique domain of politics and power? What constitutes a 'cyberthreat'? In our opening session, we will discuss these foundational questions and map the different organisational platforms and initiatives through which States, industry actors and civil society groups have attempted to regulate and govern the various layers of cyberspace in practice.

Compulsory Reading

01. NYE JR., J.S., 'The Regime Complex for Managing Global Cyber Activities', *Global Commission on Internet Governance Paper Series No. 1 – May 2014* (2014).
02. HOLLIS, D.B., 'An e-SOS for Cyberspace', 52 *Harvard International Law Journal* (2011) 373, **at 379-391 only**.
03. THE GUARDIAN, 'Dispute along cold war lines led to collapse of UN cyberwarfare talks' (23 August 2017).

Further Reading

Cyberspace

04. CHOUCRI, N. & CLARK, D.D., 'Who Controls Cyberspace?', 69 *Bulletin of the Atomic Scientists* (2013) 21.
05. EICHENSEHR, K.E., 'The Cyber-Law of Nations', 103 *Georgetown Law Journal* (2015) 317, **at 325-346 only**.
06. HOLLIS, D.B., 'Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?', in J.D. Ohlin et al. (eds.), *Cyber War: Law and Ethics for Virtual Conflicts* (OUP, 2015) 129, **at 132-155 only**.
07. TSAGOURIAS, N., 'The Legal Status of Cyberspace', in TSAGOURIAS, N., & BUCHAN, R. (eds.), *Research Handbook on International Law and Cyberspace* (Edward Elgar, 2015) 13.

Cyberpolitics, Cyberpower & Cyberthreats

08. NYE JR., J.S., 'Cyber Power', *Harvard Belfer Center for Science and International Affairs* (2010).
09. SEGAL, A., *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (Council on Foreign Affairs, 2016), **at Chapter 2 only**.
10. WITTES, B. & BLUM, G., *The Future of Violence: Robots and Germs, Hackers and Drones, Confronting A New Age of Threat* (Basic Books, 2015).
11. KELLO, L., *The Virtual Weapon and International Order* (Yale University Press, 2017).
12. GOLDSMITH, J. & RUSSELL, S., 'Strengths Become Vulnerabilities: How a Digital World Disadvantages the United States in its International Relations', Hoover Working Group on National Security, Technology, and Law, *Aegis Series Paper No. 1806* (5 June 2018).
13. MAČAK, K., 'From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers', 30 *Leiden Journal of International Law* (2017) 877.
14. KREUZLER, L., 'Disentangling the Cyber Security Debate', *Völkerrechtsblog* (20 June 2018).

Cyber Governance and Cyber Norms

15. FINNEMORE, M. & HOLLIS, D.B., 'Constructing Norms for Global Cybersecurity', 110 *American Journal of International Law* (2016) 425.
16. EICHENSEHR, K.E., 'Digital Switzerlands', 167 *University of Pennsylvania Law Review* (*forthcoming*, 2019).
17. HUANG, Z., & MAČÁK, K., 'Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches', 16 *Chinese Journal of International Law* (2017) 271.
18. SCHMITT, M.N. & VIHUL, L., 'The Nature of International Law Cyber Norms', *NATO CCD COE Tallinn Paper No. 5* (2014).
19. LESSIG, L., *Code: Version 2.0* (Basic Books, 2006), **at 120-137 only**.
20. SANDER, B., 'Cyber Insecurity and the Politics of International Law', 6 *ESIL Reflections* (2017).

SESSIONS 2-3 DIGITAL THREATS TO DEMOCRACY: FOUNDATIONAL CONCEPTS

What is 'democracy'? What are 'digital threats to democracy'? Over the course of two sessions, we will critically examine the concept of democracy and how cyberspace may be utilised as a medium for both democratic empowerment and democratic backsliding. These sessions will introduce a range of a case studies and set the conceptual foundations for the remainder of the course.

Compulsory Reading

01. OWEN, T., 'Ungoverned Space: How Surveillance Capitalism and AI Undermine Democracy', *Centre for International Governance Innovation* (20 March 2018).
02. DEIBERT, R., 'Cyberspace Under Siege', 26 *Journal of Democracy* (2015) 64.
03. TENOVE, C., 'Digital Threats to Democratic Elections: How Foreign Actors Use Digital Techniques to Undermine Democracy', *Centre for the Study of Democratic Institutions* (January, 2018), **at 8-49 only**.

Further Reading

Democracy & Democratic Backsliding

04. BERMEO, N., 'On Democratic Backsliding', 27 *Journal of Democracy* (2016) 5.
05. HUQ, A., & GINSBURG, T., 'How to Lose a Constitutional Democracy', 65 *UCLA Law Review* (2018) 78.
06. DALY, T., 'Democratic Decay in 2016', in International IDEA, *Annual Review of Constitution-Building Processes: 2016* (International IDEA, 2017) 7.
07. SCHEPELLE, K.L., 'Autocratic Legalism', 85 *University of Chicago Law Review* (2018) 545.
08. FOA, R.S., & MOUNK, Y., 'The Danger of Deconsolidation: The Democratic Disconnect', 27 *Journal of Democracy* (2016) 5.
09. NORRIS, P., 'Is Western Democracy Backsliding? Diagnosing the Risks', *Harvard Kennedy School, Faculty Research Working Paper Series* (March 2017).
10. BALKIN, J.M., 'Constitutional Crisis and Constitutional Rot', 77 *Maryland Law Review* (2017) 147.
11. FREEDOM HOUSE, *Democracy in Crisis: Freedom in the World 2018* (Freedom House, 2018).
12. V-DEM INSTITUTE, *Democracy for All? V-DEM Annual Democracy Report 2018* (V-Dem Institute, 2018).
13. PURDY, J., 'Normcore', *Dissent* (Summer 2018).

Cyberspace & Democracy

14. FREEDOM HOUSE, *Manipulating Social Media to Undermine Democracy: Freedom on the Net 2017* (Freedom House, 2017),
15. LAIDLAW, E.B., *Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility* (Cambridge University Press, 2015), at **Chapter 1 only**.
16. PALFREY, J., 'Four Phases of Internet Regulation', 77 *Social Research* (2010) 981.
17. MOUNK, Y., 'Can Democracy Survive Social Media?', *New York Review of Books* (30 April 2018).
18. JOSEPH, S., 'Social Media, Political Change, and Human Rights', 35 *Boston College International & Comparative Law Review* (2012) 145.
19. GOLDSMITH, J., 'The Failure of Internet Freedom', *Emerging Threats* (2018).
20. KAYE, D., 'The Limits of Supply-Side Internet Freedom', *Emerging Threats* (2018).
21. LIN, H. & KERR, J., 'On Cyber-Enabled Information/Influence Warfare and Manipulation', *SSRN* (2017).
22. GUNITSKY, S., 'Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability', 13 *American Political Science Association* (2015) 42.
23. BRADSHAW, S., & HOWARD, P.N., 'Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation', *Computational Propaganda Project* (2018).
24. ARNAUDO, D., 'Computational Propaganda in Brazil: Social Bots During Elections', *Working Paper No. 2017.8,* Computational Propaganda Project, University of Oxford (2017).
25. GHOSH, D. & SCOTT, B., '#DigitalDeceit: The Technologies Behind Precision Propaganda on the Internet', New America & Harvard Kennedy School (January 2018).
26. MARWICK, A., & LEWIS, R., *Media Manipulation and Disinformation Online* (Data & Society Research Institute, 2017).
27. DUBOIS, E. & BLANK, G., 'The Echo Chamber is Overstated: The Moderating Effect of Political Interest and Diverse Media', *Information, Communication & Society* (2018) 729.
28. ZUIDERVEEN BORGESIUS, F.J. et al., 'Should We Worry About Filter Bubbles?', *Internet Policy Review* (2016).
29. RUNCIMAN, D., *How Democracy Ends* (Profile Books, 2018), **at Chapter 3 only**.
30. BARTLETT, J., *The People Vs Tech: How Internet is Killing Democracy (And How We Can Save It)* (Dutton, 2018).

DAY 2. STATE RESPONSIBILITY FOR CYBER ELECTION MEDDLING (1)

TUESDAY 2ND OCTOBER 2018, ROOM 1209, 18.30-23.00

SESSION 1 *THE FRAMEWORK OF STATE RESPONSIBILITY & BREACH*

In what circumstances can States be held internationally legally responsible for meddling in the electoral processes of other States? This question will form the focus of the second and third days of the course. In this session, we will discuss how the international law of State responsibility applies in the cyber context. Relying on a number of contemporary case studies, the session will examine a range of international legal obligations – including the principle of State sovereignty, the principle of non-intervention, individual human rights, and the principle of self-determination – that may be breached as a result of inter-State cyber election meddling campaigns.

Compulsory Reading

01. HOLLIS, D.B., 'The Influence of War: The War for Influence', 32 *Temple Journal of International & Comparative Law* (2018) 31.
02. International Law Commission (ILC) Articles on Responsibility of States for Internationally Wrongful Acts, Annex to UN General Assembly Resolution 56/83 (2001), U.N. Doc. A/RES/56/83, 12 December 2001, **at Articles 1-3, 12-15 and 55-59 only**.

Further Reading

03. SCHMITT, M.N. (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP, 2017), **at 79-87 (*internationally wrongful acts*), 11-27 (*sovereignty*), 168-174 (*espionage per se*), and 312-325 (*non-intervention*) only**.
04. OHLIN, J.D., 'Did Russian Cyber Interference in the 2016 Election Violate International Law?' 95 *Texas Law Review* (2017) 1579.
05. KILOVATY, I., 'Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information', 9 *Harvard National Security Journal* (2018) 146.
06. SCHMITT, M.N., '"Virtual Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law', *Chicago Journal of International Law* (2018, *forthcoming*).
07. BRATTBERG, E. & MAURER, T., 'Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks', *Carnegie Endowment for International Peace* (May 2018).
08. FRIED, D. & POLYAKOVA, A., *Democratic Defence Against Disinformation* (Atlantic Council, February 2018).
09. EICHENSEHR, K.E., 'Political Parties as Critical Infrastructure?', *Just Security* (22 June 2017).
10. DEEKS, A. et al., 'Addressing Russian Influence: What Can We Learn From US Cold War Counter-Propaganda Efforts?', *Lawfare* (25 October 2017).
11. BUCHAN, R., 'The International Legal Regulation of State-Sponsored Cyber Espionage', in OSULA, A-M. & ROGIAS, H. (eds.), *International Cyber Norms* (NATO CCD COE Publications, 2016) 65.
12. CHARLESWORTH, H., 'International Legal Encounters with Democracy', 8 *Global Policy* (2017) 34.
13. EFRONY, D., & SHANY, Y., 'A Rule Book on The Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice', *SSRN* (2018).
14. HELMUS, T.C. et al., *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe* (RAND Corporation, 2018).
15. GILES, K., *Russia's "New" Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power* (Chatham House, 2016).
16. NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE, *Social Media as a Tool of Hybrid Warfare* (NATO StratCom COE, 2016).

SESSION 2 *ATTRIBUTION & THE PRINCIPLE OF DUE DILIGENCE*

In what circumstances are cyber operations attributable to State actors? Tackling this question, this session will discuss the different modes by which conduct may be attributed to a State under the law of State responsibility, as well as the legal and technical challenges of attribution in the cyber context. The session will also examine how reliance on the principle of due diligence may help alleviate such challenges.

Compulsory Reading

01. ANTONOPOULOS, C., 'State Responsibility in Cyberspace', in TSAGOURIAS, N., & BUCHAN, R. (eds.), *Research Handbook on International Law and Cyberspace* (Edward Elgar, 2015) 55.
02. EICHENSEHR, K., 'Cyber Attribution Problems – Not Just Who, But What', *Just Security* (11 December 2014).
03. International Law Commission (ILC) Articles on Responsibility of States for Internationally Wrongful Acts, Annex to UN General Assembly Resolution 56/83 (2001), U.N. Doc. A/RES/56/83, 12 December 2001, **at Articles 4-11 and 16-19 only**.

Further Reading

General

04. MAURER, T., *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge University Press, 2018).

Attribution

05. SCHMITT, M.N. (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP, 2017), **at 87-104 only**.
06. MAČÁK, K., 'Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors', 21 *Journal of Conflict & Security Law* (2016) 405.
07. CHIRCOP, L., 'A Due Diligence Standard of Attribution in Cyberspace', 67 *International & Comparative Law Quarterly* (2018) 643.
08. MICROSOFT, *An Attribution Organization to Strengthen Trust Online* (2017).
09. SCHMITT, M.N., & VIHUL, L., 'Proxy Wars in Cyberspace: The Evolving International Law of Attribution', 1 *Fletcher Security Review* (2014) 54.
10. BANKS, W., 'State Responsibility and Attribution of Cyber Intrusions After *Tallinn 2.0*', 95 *Texas Law Review* (2016-2017) 1487.

Due Diligence

11. SCHMITT, M.N. (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP, 2017), **at 30-50 only**.
12. BUCHAN, R., 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm', 21 *Journal of Conflict & Security Law* (2016) 429.
13. LIU, I.Y., 'State Responsibility and Cyberattacks: Defining Due Diligence Obligations', 4 *Indonesian Journal of International & Comparative Law* (2017) 191.
14. SCHMITT, M.N., 'In Defence of Due Diligence in Cyberspace', 125 *Yale Law Journal Forum* (2015) 68.
15. BANNELIER, K. & CHRISTAKIS, T., *Cyber-Attacks Prevention-Reactions: The Role of States and Private Actors* (Les Chahiers de al Revue Defence Nationale, 2017), **at 12-26 only**.
16. COZIGIOU, I., 'Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations', 32 *International Review of Law, Computers & Technology* (2018) 37.

SESSION 3 *INTRODUCTION TO DIGITAL VERIFICATION TECHNIQUES*

How can we spot online disinformation? Stepping back from the framework of State responsibility, this session will introduce some of the tools utilised to verify online content. Verification is an evolving process and the end product is rarely definitive. In this session, we will examine what questions to ask of online content for the purpose of verification and which tools can help answer those questions.

DAY 3. STATE RESPONSIBILITY FOR CYBER ELECTION MEDDLING (2)

WEDNESDAY 3RD OCTOBER 2018, ROOM 1209, 18.30-23.00

SESSION 1 RESPONDING TO CYBER ELECTION MEDDLING CAMPAIGNS

What options are available to States to respond to cyber election meddling campaigns? In this session, we will examine a range of response options, including retorsion and countermeasures. The session will also identify the obligations of States for international legally wrongful acts under the law of State responsibility.

Compulsory Reading

01. HINKLE, K.C., 'Countermeasures in the Cyber Context: One More Thing To Worry About', 37 *Yale Journal of International Law Online* (2011) 11.
02. GOLDSMITH, J., 'Contrarian Thoughts on Russia and the Presidential Election', *Lawfare* (10 January 2017).
03. International Law Commission (ILC) Articles on Responsibility of States for Internationally Wrongful Acts, Annex to UN General Assembly Resolution 56/83 (2001), U.N. Doc. A/RES/56/83, 12 December 2001, **at Articles 20-27, 28-39, and 49-54 only.**

Further Reading

General

04. HENRIKSEN, A., 'Lawful State Responses to Low-Level Cyber Attacks', 84 *Nordic Journal of International Law* (2015) 323.
05. SCHMITT, M.N., 'International Law and Cyber Attacks: Sony v. North Korea', *Just Security* (17 December 2014).
06. SCHMITT, M.N. (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP, 2017), **at 111-134 (*countermeasures*), 135-142 (*necessity*) and 142-152 (*remedies*) only**.

Countermeasures

07. SCHMITT, M.N., '"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law', 54 *Virginia Journal of International Law* (2014) 697.
08. JENSON, E.T., & WATTS, S., 'A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?', 95 *Texas Law Review* (2017) 1555.
09. HATHAWAY, O.A., 'The Drawbacks and Dangers of Active Defense', in BRANGETTO, P. et al. (eds.), *6th International Conference on Cyber Conflict* (NATO CCD COE Publications, 2014) 39.
10. BANNELIER, K. & CHRISTAKIS, T., *Cyber-Attacks Prevention-Reactions: The Role of States and Private Actors* (Les Chahiers de al Revue Defence Nationale, 2017), **at 28-80 only**.
11. MESSERSCHMIDT, J.E., 'Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm', 52 *Columbia Journal of Transnational Law* (2013) 275.
12. CORN, G. & JENSEN, E., 'The Use of Force and Cyber Countermeasures', *SSRN* (2018).

Beyond State Responsibility

13. CROOTOF, R., 'International Cybertorts: Expanding State Accountability in Cyberspace', 103 *Cornell Law Review* (2018) 565.
14. WALTON, B.A., 'Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law', 126 *Yale Law Journal* (2017) 1460.
15. TSAGOURIAS, N., 'Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts', 21 *Journal of Conflict & Security Law* (2016) 455.
16. EICHENSEHR, K.E., 'Public-Private Cybersecurity', 95 *Texas Law Review* (2017) 467.

17. GOLDSMITH, J., 'Uncomfortable Questions in the Wake of Russia Indictment 2.0 and Trump's Press Conference With Putin', *Lawfare*, 16 July 2018.
18. INDICTMENT, *United States of America v. Internet Research Agency LLC et al.*, No. 1:18-cr-00032, 2018 WL 914777, D.D.C. (16 February 2018).
19. INDICTMENT, *United States of America v. Viktor Borisovich Netysksho et al.*, No. 1:18-cr-00215-ABJ, D.D.C. (13 July 2018).
20. WEEDON J., et al., *Information Operations and Facebook* (Facebook 2017).
21. LIN, H., 'Developing Responses to Cyber-Enabled Information Warfare Operations' (6 September 2018).
22. STAMOS, A., 'How the U.S. Has Failed to Protect the 2018 Election – and Four Ways to Protect 2020', *Lawfare* (22 August 2018).

SESSION 2 ***CYBER ELECTION MEDDLING CRISIS SIMULATION***

Drawing together the themes discussed during the past two days, this session will engage participants in an interactive simulation designed to generate discussion concerning how the law of State responsibility applies to a concrete cyber election meddling crisis situation.

SESSION 3 ***GUEST SPEAKER: MONICA ROSINA (FACEBOOK)***

DAY 4. CYBER CONTENT DILEMMAS

THURSDAY 4TH OCTOBER 2018, ROOM 1209, 18.30-23.00

SESSIONS 1-2 *PLATFORM RESPONSIBILITY FOR ONLINE CONTENT: THE DILEMMAS OF HATE SPEECH, TERRORIST PROPAGANDA & "FAKE NEWS" CAMPAIGNS*

As social media platforms have proliferated around the world, digital speech increasingly flows through an elaborate privately-owned infrastructure. Today, our practical ability to communicate is subject to the decisions of private platform owners, who govern the digital spaces in which people interact with each other. States, understanding this, have developed new techniques for speech regulation which include targeting the owners of private platforms in an effort to coerce them into regulating speech on their behalf. Over the course of two sessions, we will examine how online content is governed in practice – examining the particular challenges posed by hate speech, terrorist propaganda and "fake news" campaigns.

Compulsory Reading

01. KELLER, D., 'Internet Platforms: Observations on Speech, Danger, and Money', Hoover Working Group on National Security, Technology, and Law, *Aegis Series Paper No. 1808* (13 June 2018).
02. UN SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF THE RIGHT TO FREEDOM OF OPINION AND EXPRESSION, 'Report', U.N.Doc. A/HRC/38/35 (6 April 2018).
03. ASHER-SCHAPIRO, A., 'YouTube and Facebook are Removing Evidence of Atrocities, Jeopardizing Cases Against War Criminals', *The Intercept* (2 November 2017).

Further Reading

04. BALKIN, J.M., 'Free Speech is a Triangle', *Columbia Law Review* (2018, *forthcoming*).
05. KLONICK, K., 'The New Governors: The People, Rules, and Processes Governing Online Speech', 131 *Harvard Law Review* (2018) 1598.
06. WARDLE, C. & DERAKHSHAN, H., 'Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making', Council of Europe Report DGI (2017)09 (27 September 2017).
07. SYED, N., 'Real Talk About Fake News: Towards a Better Theory for Platform Governance', *Yale Law Journal Forum* (2017) 337.
08. WU, T., 'Is the First Amendment Obsolete?', *Knight First Amendment Institute* (2017).
09. MARDA, V. & MILAN, S., *Wisdom of the Crowd: Multistakeholder Perspectives on the Fake News Debate*, (Internet Policy Observatory, 2018).
10. CITRON, D.K., 'Extremist Speech, Compelled Conformity and Censorship Creep', 93 *Notre Dame Law Review* (2018) 1035.
11. LIEBERMAN, A.V., 'Terrorism, the Internet, and Propaganda: A Deadly Combination', 9 *Journal of National Security Law & Policy* (2017) 95.
12. ARTICLE 19, 'Self-Regulation and 'Hate Speech' on Social Media Platforms' (Article 19, 2018).
13. EUROPEAN COMMISSION, 'Code of Conduct on Countering Illegal Hate Speech Online' (2016).
14. EUROPEAN COMMISSION, 'Communication: Tackling Illegal Content Online, Towards an Enhanced Responsibility of Online Platforms', COM(2017) 555 final (28 September 2017).
15. JØRGENSEN, R.F., 'Human Rights and Private Actors in the Online Domain', in LAND, M.K. and ARONSON, J.D., *New Technologies for Human Rights Law and Practice* (Cambridge University Press, 2018) 243.
16. ARTICLE 19, 'Side-stepping Rights: Regulating Speech By Contract' (Article 19, 2018).
17. JOSEPH, S., 'The Human Rights Responsibilities of Media and Social Media Businesses', in FARRIOR, S. (ed.), *Human Rights and Non-State Actors* (Edward Elgar, *forthcoming*).
18. MANILA PRINCIPLES ON INTERMEDIARY LIABILITY, *Best Practices Guidelines for Limiting Intermediary Liability for Content to Promote Freedom of Expression and Innovation* (24 March 2015).

19. THE SANTA CLARA PRINCIPLES ON TRANSPARENCY AND ACCOUNTABILITY IN CONTENT MODERATION (2018).
20. UN SPECIAL RAPPORTEURS, 'Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda', FOM.GAL/3/17 (3 March 2017).
21. EUROPEAN COMMISSION, 'A Multi-Dimensional Approach to Disinformation', Report of the Independent High Level Group on Fake News and Online Disinformation (March 2018).
22. EUROPEAN COMMISSION, 'Communication: Tackling Online Disinformation: a European Approach', COM(2018) 236 FINAL (26 April 2018).
23. ALEMANNO, A., 'Editorial: How to Counter Fake News? A Taxonomy of Anti-Fake News Approaches', 9 *European Journal of Risk Regulation* (2018) 1.
24. SABEEL RAHMAN, K., 'The New Utilities: Private Power, Social Infrastructure, and the Revival of the Public Utility Concept', 39 *Cardozo Law Review* (2018) 101.
25. GILLESPIE, T., 'Improving Moderation' (2018).
26. WARNER, M.R., 'Potential Policy Proposals for Regulation of Social Media and Technology Firms', *Draft White Paper* (2018).
27. HOUSE OF COMMONS DIGITAL, CULTURE, MEDIA AND SPORT COMMITTEE, 'Disinformation and 'Fake News': Interim Report', *Fifth Report of Session 2017-19* (29 July 2018).
28. VARIOUS, 'Symposium: Information Platforms and the Law', *2 Georgetown Law Technology Review* (2018) 191.
29. BELLI, L. & ZINGALES, N. (eds.), *Platform Regulations: How Platforms are Regulated and How They Regulate Us*, Official Outcome of the UN IGF Dynamic Coalition on Platform Responsibility (UN Internet Governance Forum, 2017).
30. GILLESPIE, T., *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions that Shape Social Media* (Yale University Press, 2018).

SESSION 3 ***GUEST SPEAKER: FRANCISCO BRITO CRUZ (INTERNETLAB)***

DAY 5. DATA PROTECTION

FRIDAY 5TH OCTOBER 2018, ROOM 806, 18.30-23.00

SESSION 1 *ONLINE POLITICAL MICROTARGETING AND DATA PROTECTION*

In an era of big data, concerns about the protection of personal data have become ever more pressing. In this session, we will examine the increasingly prevalent practice of online political microtargeting – the combination of data-driven voter research with personalised political advertising. Examining the recent events surrounding Cambridge Analytica and Facebook as a case study, the session will discuss whether political microtargeting constitutes a threat to democracy as well as the extent to which the European Union's new General Data Protection Regulation (GDPR) may serve to limit such practices.

Compulsory Reading

01. Watch these three short videos:
    a. PRIVACY INTERNATIONAL, 'What Is Data Protection?', accessible online here: https://www.youtube.com/watch?v=VUae3XgIZVU
    b. PRIVACY INTERNATIONAL, 'Big Data', accessible online here: https://www.youtube.com/watch?v=HOoKhnvoYkU
02. ZUIDERVEEN BORGESIUS, F. et al., 'Online Political Microtargeting: Promises and Threats for Democracy', 14 *Utrecht Law Review* (2018) 82.
03. PRIVACY INTERNATIONAL, 'Cambridge Analytica Explained: Data and Elections' (13 April 2017).
04. BALKIN, J., 'Three Questions: Prof. Jack Balkin on Facebook and the Risks of 'Data Capitalism'', *Yale Insights* (8 May 2018).

Further Reading

05. PRIVACY INTERNATIONAL, *The Keys to Data Protection* (Privacy International, August 2018).
06. EU AGENCY FOR FUNDAMENTAL RIGHTS, *Handbook on European Data Protection Law* (2018).
07. VAN DER SLOOT, B. & ZUIDERVEEN BORGESIUS, F., 'The EU General Data Protection Regulation: A New Global Standard for Information Privacy', *SSRN* (2018).
08. ZARSKY, T.Z., 'Incompatible: The GDPR in Age of Big Data', 47 *Seton Hall Law Review* (2017) 995.
09. WACHTER, S. & MITTELSTADT, B., 'A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI', *Columbia Business Law Review* (*forthcoming*).
10. VAN DER SLOOT, B. & VAN SCHENDEL, S., 'Ten Questions for Future Regulation of Big Data: A Comparative and Empirical Legal Study', 7 *JIPITEC* (2016) 110.
11. BENNETT, C.J., 'Voter Databases, Micro-Targeting, and Data Protection Law: Can Political Parties Campaign in Europe as they do in North America?', 6 *International Data Privacy Law* (2016) 261.
12. ZARSKY, T.Z., 'The Privacy-Innovation Conundrum', 19 *Lewis & Clark Law Review* (2015) 115.
13. CHESTER, J. & MONTGOMERY, K.C., 'The Role of Digital Marketing in Political Campaigns', 6 *Internet Policy Review* (2017).
14. EUROPEAN DATA PROTECTION SUPERVISOR, 'Opinion 3/2018: EDPS Opinion on Online Manipulation and Personal Data' (19 March 2018).
15. INFORMATION COMMISSIONER'S OFFICE, *Democracy Disrupted? Personal Information and Political Influence* (ICO, 2018).
16. BARTLETT, J. et al., *The Future of Political Campaigning* (Demos, 2018).
17. INFORMATION COMMISSIONER'S OFFICE, *Big Data, Artificial Intelligence, Machine Learning and Data Protection* (ICO, 2017).
18. LANCHESTER, J., 'You Are The Product', *London Review of Books* (17 August 2017).

19. VAIDHYANATHAN, S., *Anti-Social Media: How Facebook Disconnects Us and Undermines Democracy* (Oxford University Press, 2018), **at Chapter 6 only**.
20. BALKIN, J.M., 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation', 51 *UC Davis Law Review* (2018) 1149.
21. O'NEIL, C., *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Crown, 2016), **at Chapter 10 only**.
22. PASQUALE, F., *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press, 2015), **at Chapters 1-3 only**.

SESSION 2 ***GUEST SPEAKER: MARCEL LEONARDI (FGV)***

SESSION 3 ***GUEST SPEAKER: RAFAEL ZANATTA (INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR, IDEC)***

DAY 6. CYBER SURVEILLANCE & FUTURE DIGITAL THREATS

SATURDAY 6TH OCTOBER 2018, ROOM 806, 08.30-17.00

SESSIONS 1-2 CYBER SURVEILLANCE

The emergence of cyberspace has led to a dramatic expansion of not only the possibilities for communication, but also the opportunities for far-reaching governmental surveillance programmes. The vast magnitude of data collection through cyber surveillance programmes achieved global recognition when in 2013 Edward Snowden disclosed details about the covert surveillance practices of the UK and US intelligence agencies, as well as their partners. How do such practices impact on the democratic culture of society? What are the legal limits of such practices? After discussing how human rights apply in the cyber context, this session will examine the compatibility of modern forms of communications surveillance with international human rights law, focusing in particular on the right to privacy.

Compulsory Reading

01. THE GUARDIAN, 'Edward Snowden's "open letter to the Brazilian people" – in full' (17 December 2013).
02. THE GUARDIAN, 'Brazilian President: US surveillance a "breach of international law"' (24 September 2013).
03. BRUNNER, L., 'Digital Communications and the Evolving Right to Privacy', in LAND, M.K. and ARONSON, J.D., *New Technologies for Human Rights Law and Practice* (Cambridge University Press, 2018) 217.

Further Reading

04. LUBIN, A., 'A New Era of Mass Surveillance is Emerging Across Europe', *Just Security* (9 January 2017).
05. RONA, G. & AARONS, L., 'State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace', 8 *Journal of National Security Law & Policy* (2016) 503.
06. FIDLER, D.P., 'Cyberspace and Human Rights', in TSAGOURIAS, N., & BUCHAN, R. (eds.), Research Handbook on International Law and Cyberspace (Edward Elgar, 2015) 94.
07. WATT, E., 'The Right to Privacy and the Future of Mass Surveillance', 21 *International Journal of Human Rights* (2017) 773.
08. KOSTA, E., 'Surveilling Masses and Unveiling Human Rights: Uneasy Choices for the Strasbourg Court', Inaugural Address, Tilburg University (15 December 2017).
09. NYST, C. & FALCHETTA, T., 'The Right to Privacy in the Digital Age', 9 *Journal of Human Rights Practice* (2017) 104.
10. LUBIN, A., 'Legitimizing Foreign Mass Surveillance in the European Court of Human Rights', *Just Security* (2 August 2018).
11. BERNAL, P., 'Data Gathering, Surveillance and Human Rights: Recasting the Debate', 2 *Journal of Cyber Policy* (2016) 243.
12. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU: Volume II: Field Perspectives and Legal Update* (European Union Agency for Fundamental Rights, 2017).
13. SEGAL, A., *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (Council on Foreign Affairs, 2016), **at Chapter 5 only**.
14. DEEKS, A., 'An International Legal Framework for Surveillance', 55 *Virginia Journal of International Law* (2015) 291.
15. LUBIN, A., '"*We Only Spy on Foreigners*": The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance', 18 *Chicago Journal of International Law* (2018) 502.
16. MILANOVIC, M., 'Human Rights Treaties and Foreign Surveillance', 56 *Harvard International Law Journal* (2015) 81.

17. NG, V., & MURRAY, D., 'Extraterritorial Human Rights Obligations in the Context of State Surveillance Activities?', *HRC Essex* (2 August 2016).
18. SHANY, Y., 'Cyberspace: The Final Frontier of Extra-Territoriality in Human Rights Law', *Hebrew University of Jerusalem Cyber Security Research Center Cyber Law Program* (29 September 2017).
19. OFFICE OF THE UN HIGH COMMISSIONER FOR HUMAN RIGHTS, 'The Right to Privacy in the Digital Age', A/HRC/27/37 (30 June 2014).
20. PRIVACY INTERNATIONAL, *Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards* (April 2018).

SESSION 3 ***GUEST SPEAKERS: LOUISE MARIE HUREL & LUISA LOBATO, IGARAPÉ INSTITUTE***

SESSION 4 ***ENCRYPTION & ONLINE ANONYMITY***

Individuals have become increasingly concerned with seeking to protect their online security through encryption – the scrambling of data so only intended recipients may access it – and other anonymising tools designed to disguise their online identity and digital footprint. In this session, we will examine the tensions that have arisen over the regulation of encryption and other anonymising tools, including the human rights implications of different regulatory approaches.

Compulsory Reading

01. AMNESTY INTERNATIONAL, *Encryption: A Matter of Human Rights* (Amnesty International, 2016).
02. PRIVACY INTERNATIONAL, 'The Battle for Encryption in Brazil', *Medium* (16 November 2016).
03. LONG, C., 'Why WhatsApp is Brazil's Go-To Political Weapon', *The Brazilian Report* (13 April 2018).

Further Reading

04. KERR, O.S. & SCHNEIER, B., 'Encryption Workaronds', 106 *Georgetown Law Journal* (2018) 989.
05. GILL L. et al., 'Shining A Light on the Encryption Debate: A Canadian Field Guide', *Joint Research Publication by the Citizen Lab and the Canadian Internet Policy & Public Interest Clinic* (May 2018).
06. UN SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF THE RIGHT TO FREEDOM OF OPINION AND EXPRESSION, 'Report', U.N.Doc. A/HRC/29/32 (22 May 2015).
07. UN SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF THE RIGHT TO FREEDOM OF OPINION AND EXPRESSION, 'Encryption and Anonymity Follow-up Report', Research Paper 1/2018 (June 2018).
08. THE NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, MEDICINE, *Decrypting the Encryption Debate: A Framework for Decision Makers* (The National Academies Press, 2018).
09. SCHULZ, W. & VAN HOBOKEN, J., 'Human Rights and Encryption' (UNESCO, 2016).
10. EASTWEST INSTITUTE, *Encryption Policy in Democratic Regimes: Finding Convergent Paths and Balanced Solutions* (EastWest Institute, 2018).
11. LIN, H., 'The East West Institute's New Report on Encryption: A Review', *Lawfare*, 23 February 2018.
12. LANDAU, S., *Listening In: Cybersecurity in an Insecure Age* (Yale University Press, 2017), at **Chapters 4 and 5 only**.
13. DEEKS, A., 'The International Legal Dynamics of Encryption', *Hoover Series Paper No. 1609* (2016).
14. ZINGALES, N., 'Virtues and Perils of Anonymity: Should Intermediaries Bear the Burden?', *Tilberg University Discussion Paper* (July 2014).

15. SPANO, R., 'Intermediary Liability for Online User Comments under the European Convention on Human Rights', 17 *Human Rights Law Review* (2017) 665.

SESSION 5 *FUTURE DIGITAL THREATS TO DEMOCRACY*

Reflecting on the pace of technological change in recent years, our final session will examine a number of emergent threats to democracy, including the use of autonomous weapons systems in domestic law enforcement practices and the rise of digital impersonation media known as Deep Fakes.

Compulsory Reading

01. HEYNS, C., 'Human Rights and the Use of Autonomous Weapons Systems (AWS) During Domestic Law Enforcement', 38 *Human Rights Quarterly* (2016) 350.
02. CHESNEY, R. & CITRON, D., 'Deep Fakes: A Looming Crisis for National Security, Democracy and Privacy?', *Lawfare*, 21 February 2018.
03. Watch this video: 'Jack Balkin on robots, algorithms, and big data', accessible online here: https://law.yale.edu/yls-today/yale-law-school-videos/jack-balkin-robots-algorithms-and-big-data

Further Reading

04. CHESNEY, R. & CITRON, D., 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security', *SSRN* (2018).
05. BALKIN, J.M., 'The Three Laws of Robotics in the Age of Big Data', 78 *Ohio State Law Journal* (2017) 1217.
06. PIRACES, E., 'The Future of Human Rights Technology: A Practitioner's View', in LAND, M.K. and ARONSON, J.D., *New Technologies for Human Rights Law and Practice* (Cambridge University Press, 2018) 289.
07. BRUNDAGE, M. et al., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation* (February 2018).
08. BENVENISTI, E., 'Upholding Democracy Amid the Challenges of New Technology: What Role for the Law of Global Governance?', 29 *European Journal of International Law* (2018) 9.
09. BERKMAN CENTER FOR INTERNET & SOCIETY, 'Don't Panic: Making Progress on the "Going Dark" Debate' (1 February 2016).
10. RISSE, M., 'Human Rights and Artificial Intelligence: An Urgently Needed Agenda', *Harvard Kennedy School: Faculty Research Working Paper Series* (May 2018).
11. EUROPEAN COMMISSION, 'Report from the High-Level Hearing: A European Union Strategy for Artificial Intelligence' (27 March 2018).
12. EUROPEAN COMMISSION, 'Communication: Artificial Intelligence for Europe', COM(2018) 237 final (25 April 2018).
13. GOOSE, S., 'The Growing International Movement Against Killer Robots', *Harvard International Review*, 5 January 2017.
14. SCHARRE, P., *Army of None: Autonomous Weapons and the Future of War* (W.W. Norton & Company, 2018).