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.

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)
- 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


03. THE GUARDIAN, ‘Dispute along cold war lines led to collapse of UN cyberwarfare talks’ (23 August 2017).

Further Reading

Cyberspace


Cyberpolitics, Cyberpower & Cyberthreats


Cyber Governance and Cyber Norms


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


Further Reading

Democracy & Democratic Backsliding


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


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.


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).


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


Further Reading

General


Attribution


08. MICROSOFT, An Attribution Organization to Strengthen Trust Online (2017).


Due Diligence


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


02. GOLDSMITH, J., ‘Contrarian Thoughts on Russia and the Presidential Election’, Lawfare (10 January 2017).


Further Reading

General


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


Beyond State Responsibility


**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
03. ASHER-SCHAPIRO, A., ‘YouTube and Facebook are Removing Evidence of Atrocities, Jeopardizing Cases Against War Criminals’, The Intercept (2 November 2017).

Further Reading
12. ARTICLE 19, ‘Self-Regulation and ‘Hate Speech’ on Social Media Platforms’ (Article 19, 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=VUae3XgLZVU
   b. PRIVACY INTERNATIONAL, ‘Big Data’, accessible online here: https://www.youtube.com/watch?v=HOoKh:noYkU


03. PRIVACY INTERNATIONAL, ‘Cambridge Analytica Explained: Data and Elections’ (13 April 2017).


Further Reading

05. PRIVACY INTERNATIONAL, The Keys to Data Protection (Privacy International, August 2018).


17. INFORMATION COMMISSIONER’S OFFICE, Big Data, Artificial Intelligence, Machine Learning and Data Protection (ICO, 2017).

19. VAIDHYANATHAN, S., *Anti-Social Media: How Facebook Disconnects Us and Undermines Democracy* (Oxford University Press, 2018), **at Chapter 6 only**.


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

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


02. THE GUARDIAN, ‘Brazilian President: US surveillance a “breach of international law”’ (24 September 2013).


Further Reading


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

03. LONG, C., 'Why WhatsApp is Brazil’s Go-To Political Weapon’, The Brazilian Report (13 April 2018).

Further Reading

12. LANDAU, S., Listening In: Cybersecurity in an Insecure Age (Yale University Press, 2017), at Chapters 4 and 5 only.
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


Further Reading


07. BRUNDAGE, M. et al., The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation (February 2018).


