SECURITY, SURVEILLANCE, FREEDOM, AND HUMAN RIGHTS IN A DIGITAL AGE

Professor: Didier Bigo
Academic year 2018/2019: Common core curriculum – Spring semester

COURSE DESCRIPTION

This common course will combine various approaches and scholarship in critical security, surveillance, freedom and human rights studies with specific reference to the intersection of these issues in the digital sphere. This course will draw from a variety of digital data and primary sources, combining political theoretical knowledge with an understanding of what is at stake in the ‘digital’ and data politics. The aim is to develop a reflexive understanding of the main categories of security, surveillance and human rights, such as deconstructing the claims that so-called ‘fake news’ is novel. This reflection will be led by academics, high level practitioners who are faced with these issues and students themselves who will participate in three debates on central cases and work on research papers. Throughout the course, central concepts and political stakes will be theorised and historicised, and hypotheses will be formulated. Students will then analyse themselves various cases, connecting them to the hypotheses and central theoretical concepts at stake in these discussions. Several experts will be invited to give lectures on central issues, and students are invited to engage and lead an interactive discussion. This course will rely on an interactive form of teaching, encouraging students to participate in debates, providing an array of video sources and discussing central issues with guest speakers.

OVERVIEW OVER SESSIONS

Session 1: Introduction to the course - The Internet: Where is the world, where is the globe?

Presentation of the course: Aims, assessment and interactive format

● Where suitable, guest speakers will give a 20-30 minute lecture during the second half of the session, followed by a 30 minute debate with students
The course will be interactive and students will be invited to participate in three debates. At the end of each debate, all students will vote for the most convincing argument. The debates will not be assessed, but good interactive participation is expected.

Being online/offline: Where is the world, where is the globe?
- The novelty of digitisation of data, the ideology of the interconnected world, imagining life without the Internet, back to the past?
- The origins of telecommunications, telegraphs, internet cables, uses of SIGINT, ‘the Internet’ as such, smart phones, social networks, digital intimacies, friends 2.0
- Impact of the online world on security, surveillance, human rights and freedom

Background reading:
- Routledge Handbook of Internet Politics https://books.google.co.uk/books?id=GJdfuGSa1xUC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Readings
Session 2: (In)security and the digital I: Cases of cyber warfare – myth, realities, and a political imagination

Many debates exist around the effectiveness of the distinction between cyberspace and territorial space. Can cyber affect territory, and the other way round? Is cyber a tool for technological war or a radically new type of war? Are cyber attacks and defenses a form of war, or not? What is the meaning of war in a digital age? Could you do war only via manipulation of the web or by accident? This second session will be led by student debates around cases commonly referred to as “cyberwars”.

Cyber wars: First student debate on three cases: US/Iran, Baltic States and Y2K. Are these instances cases of cyberwar?

- Students will divide themselves into three groups (email choice to TA, discuss through email or google docs), choosing one of the cases. In each group, two representatives will be identified to present the debate and argue for or against the proposition that the case is a “cyberwar”. At the end of each debate, all students will vote for the most convincing position.
- Recovering various possible stories to narrate these instances & assessing to what extent ‘the cyber’ constitutes a new way to conduct war or whether there are new forms of war in the revolution of military affairs – the Internet as a part of the military political imagination?
- Deconstructing the polemics around cyberwars

Readings/Resources:

Session 3: (In)security and the digital II: Thinking military activities today through war studies and strategic studies

This session will Interrogate the concepts of ‘cyber’ and ‘war’ as part of a new agenda by historicising the transformation of war and technologies. How is the current technology different, and how is its use novel?

- Traditional analysis of war (Westphalian state model and realist IR tradition) and its construction after the World Wars, in which war figures as external to the nation; Nationalism and survival of the nation; the state as a shadow actor embodying the nation; countering this narrative by a description of the state as a field of power configurations
- The war matrix and Michel Foucault, reversing Clausewitz’s ‘war is the continuation of politics by other means’, viewing politics as a continuation/attenuation of war; wars and struggles as invasions and their internal dimension (e.g. civil wars)
- The war, peace and security nexus: analysing military interventions in the name of peace, flows of changes and regulations, the smooth governance of changes; ‘cyber’ as a deterritorialised place and subsequently reterritorialized in networks of enemies
Military doctrine is a system of knowledge the contemporary "spirit of war" is characterized by the organizing concepts of "culture" and "network"—seeing like a military in the twenty-first century is seeing a world of networks. Cyber is only its prolongation.

the notion of the ‘enemy within’ and its relation to terrorism (which will be explored in Session 4).

Reading:

- Olsson, Christian. « Military interventions and the concept of the political: Bringing the political back into the interactions between external forces and local societies ». In Terror, Insecurity and Liberty, 156–187. Routledge, 2014.
- Rigouste, Mathieu. L’ennemi intérieur : La généalogie coloniale et militaire de l’ordre sécuritaire dans la France contemporaine. Editions La Découverte, 2009
Session 4: (In)security and the digital IV: Cyber crime

This session will explore various cases of cyber-crime, such as ransomware, everyday crimes on the Internet (identity theft, cyberstalking, harassment, copyright infringements, etc.)

- Specific agencies tackling these issues: e.g. US cybercrime units (such as the FBI cyber division), ENISA (The European Union Agency for Network and Information Security), Europol, ANSI cybersecurity portal
- Reporting Crime - Trends on crime: history of violent crime, crime against persons and property
- Theories of crime and their application to “cyber” crime
- Predicting cyber-crime with Artificial Intelligence: The case of predpol - a utopia in the making? A money making activity? New astrologists?
- The notion of the politics of unease and ‘cyber’ in practice: What does this approach offer? How is anonymity here constituted as irresponsibility, giving opportunities for petty crime?
- Literature on critical criminology and police studies, critical digital studies, critical security studies

Guest lecture around Predictive Policing

Readings

- ‘This is How Easy It Is To Get Hacked’ via VICE on HBO, 28 March 2018
  https://www.youtube.com/watch?v=G2_5rPbUDNA
- FireEye Cyber Threat Map: https://www.fireeye.com/cyber-map/threat-map.html
Session 5 : (In)security and the digital III: Preventing cyber war crime and terrorism, a cyber security success or a politics of fear and unease?

This session will deconstruct the notion of “cyber terrorism”, where terrorism becomes increasingly mobilised as a fusion of war and crimes. We will also focus on ‘the war on terror’ and its legacy, shaping the notion of cyber terrorism.

- Links to the ‘enemy within’ and the politics of fear: fear of foreigners, fear of majorities to become minorities at home, deconstructing a particular form of populism around the fears of the future; genesis of the notion of the ‘enemy within’
- What precisely is done in the name of countering cyberterrorist attacks? What are the narratives of justification of today’s policies which enable military operations, CIA operations, drone killings and cyber activities?
- Prevention and prediction of interventions abroad, connecting the figures of the enemies both abroad and within; criminal justice applied ‘inside’ and military operations against the same figure outside, enabling the killings of suspected terrorists
- Critical security studies as an alternative to think about security and insecurity, the external and the internal. Surveillance studies, a way to combine critical security studies and critical technology studies.

Readings:

COURSE OUTLINE

- Denning, Dorothy E. "Cyberterrorism: Testimony before the special oversight panel on terrorism committee on armed services US House of Representatives." Focus on Terrorism 9 (2000).
https://books.google.co.uk/books?hl=en&lr=&id=dyEZhA3ptyAC&oi=fnd&pg=PR7&dq
Session 6: Surveillance I: The case of Cambridge Analytica—Data capitalism, digital surveillance, junk news and its political impact

Analysis of Cambridge Analytica case: Second Student Debate

- The second student debate will divide students in three groups: Group A assessing to what extent the Cambridge Analytica case can be seen as a form of data capitalism (one for yes, one for no); Group B assessing to what extent it can be seen as a part of the development of digital surveillance (one for yes, one for no); Group C assessing to what extent it can be seen as junk news and its political impact (one for yes, one for no). Two representatives per group will present the debate and students will vote for the most convincing arguments.

- The rest of the session will assess the relations between these three dimensions: Cambridge Analytica and its links to data brokers and GAFAM (the five most popular US tech stocks: Google, Apple, Facebook, Amazon and Microsoft): How has this form of data capitalism shaped a new economy? What is the importance of ‘political opinion’ in framing votes and giving rise to political surveillance? What are the intersections between commercial and political surveillance?

Reading:

Session 7: Surveillance III: intelligence and surveillance: the diagonal of power

This session will build on the empirical analysis of the previous sessions and draw out more...
COURSE OUTLINE

theoretical questions around the connection between security, intelligence and surveillance. We will compare and contrast security studies and surveillance studies, as well as their different approaches to the same research questions and objects. The two fields of studies bear different assumptions about the state, violence, democracy and policing which will be analysed in this session. They also disagree on the links between capitalism and neoliberal influences on intelligence and tools of surveillance, as well as the role of internet providers

- Origins of surveillance studies: sociology of state making, sociology of policing, political surveillance by undercover activities, practices of identification
- Epistemological questions about state and protection of populations: How far do you embrace “your” population? - Knowledge, statistics, probability, great number and governmentality
- The hybridisation of state intelligence: Public and private collaboration and fights. Is it possible to oppose state political surveillance and private commercial surveillance?
- The CIA open venture: an arms industry transposed into the digital and its export strategies; France and Germany in Libya and Syria
- GAFAM: Internet providers as intermediaries and private actors complying to state legislations with reticence or powerful non-elected politicians shaping the future and restructuring politics and the role of politicians as well as elections
- The boundaries patrolled by “data brokers”: the wild wild west or the place for the construction of transnational meta capital (electronic money, electronic state and international organisations…)

Readings:

Session 8: Surveillance III: Practices of five eyes & Snowden disclosures of NSA shared secrets

This session will focus on the Snowden disclosures and an international political sociology of the practices of the “five eyes”.

- The five eyes plus: what are the bases of solidarity between intelligence services: cultural (the anglo world), material (geopolitics of cables), know-how and dispositions
- National security in a transnational world and a digital age
- What is left of national if we have shared secrets and transnational guilds
- Data politics: data interception, raw data, the social construction of data intelligence
- Interrogating the infrastructure of data collection, storage, sharing, alteration and destruction
- Data mining, data extraction from data analytics, predictive software and speculation
- Surveillance “tools”: relations with intelligence black boxing, technology of control, and the Internet? Mass surveillance and targeted surveillance by intelligence services
- The social use of large scale surveillance; What for? Politics of needs or bureaucratics precautionary logics?
- The Snowden paradox? Reinforcement of some intelligence services tools and power? Taming the US surveillance, used to reinforce other secret services in order to fill the gap? Introducing publicity
into secrecy: the legalisation of intelligence bodies and the end of immunity. Accountability even for secret activities

Readings:

- James Bamford- The Shadow Factory _ The Ultra-Secret NSA from 9_11 to the Eavesdropping on America-Doubleday (2008),
- Greenwald, Glenn, Ewen MacAskill, Laura Poitras, Spencer Ackerman, and Dominic Rushe. "Microsoft handed the NSA access to encrypted messages." the Guardian 12 (2013).
- The guardian (2013) 'NSA files decoded: What the revelations mean for you' via https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

This session will analyse the Snowden controversy and its impact on international human rights law cases. We will host a third Student Debate on the Snowden legacy: Reinforcement of technology of intelligence? Safeguarding privacy and democracy. What are the arguments of the Courts and the philosophers?

- In line with the previous sessions, the third student debate will divide students into three groups:
  - Group A will analyse discuss the way domestic surveillance is performed and how different courts and especially the ECtHR and CJEU examine the limits of state surveillance. They can begin the debate with the Tele2/Watson case but also the EU-Canada PNR case;
  - Group B will discuss how foreign intelligence, external surveillance beyond the jurisdiction of the state are or not under constraints. They may begin with the Big Brother Watch case as well as the CJEU Schrems cases;
  - Group C will examine the question of biometrics identification and anonymity. Do biometrics have the capacity to de-anonymize data? They may begin with the Digital Rights Ireland case.

Each group has to discuss the central implications of the Courts on these subjects, including philosophical, ethical and legal backgrounds, as well as the relations between a permanent state of exception and the democratic mechanisms of representative democracies (and their uneasy relation with democratic principles). What are the effects of rulings with regards to sovereignty and democracy? What do the rulings mean in terms of privacy and human rights for all internet users, and what do they do for better regulations of the activities of intelligence services?

For each debate, we will have this time, not two but three representatives of each group as they will present the debate along 3 positions: one in favour of government positions, another one in favour of...
privacy and friends of claimants, and a third one on the position of the court itself.

● This will be followed by a general discussion and a vote between the three positions after a debate.

Readings:

● The specific legal database and comments on the different cases prepared by the researchers of UTIC and QMUL will be accessible to students.


Session 10: Human Rights II: Democratic Oversight and privacy as forms of resistance against surveillance and the revival of democracy?

This section will analyse how democratic oversight and privacy can be established and guaranteed.
COURSE OUTLINE

- Are we sleepwalking into a society of surveillance? Are we slowly turning into a society of exhibition? Does the pleasure of social communication trump privacy?
- Friends 2.0: Who are our friends on social media and offline? What guides our relations, trust or privacy, individual rights or collective rights?
- Framing privacy rights: Who owns data? Those who construct datasets for their own purposes, the persons from which data has been built (with or without agreement).
- Examining international legal struggles at the Transatlantic scale: Privacy in the US and in Europe; the GDPR in Europe and the European Courts. US answers by the executive branch and the courts.
- Reorganising the ownership of the Internet. California rules?
- Navi Pillay and the UN project of "Privacy in a digital age": the human rights of Internet users: deconstructing the difference of protection between foreigners and citizens on the web; putting the reason of state and spying under control?
- Democratic Oversight over the tools and practices of intelligence services? Democracies at their limits

Guest lecture around Transatlantic debates on privacy and oversight.

Readings:

- Born, Hans, and Ian Leigh. Legal Standards and Best Practice for Oversight of Intelligence Agencies. Oslo, 2005.
Session 11: Human Rights III: Techno-science as forms of resistance against the development of data suspects
The critique of legal forms of resistance: always too late. A maginot line? In a technological society, can surveillance only be blocked by counter-surveillance measures?

- Cryptology: from war secrets to garage games
- Encryption as a counter-surveillance measure? Counter-surveillance and sousveillance
- The Thor project and Pretty Easy Privacy: Slowing down interception of data and identification - localisation processes.
- The old synopticon revived - Surveillance of the powerful
- Gulliver and lilliputians: how to limit or to control the technologisation of surveillance and its scale and speed
- The mobilisation of decrypting algorithms: breaking the malicious codes of surveillance by companies and states
- The anonymous: Hackers for freedom or criminals of a new kind? The celebrity problem of anonymity.
- Demonopolisation of intelligence forms of know-how
- A critical theory of algorithms: a series of rules, a computational process? Unpacking the concept of algorithm into specific material instances to critically engage with computation

Readings:

Session 12: Artificial intelligence: Enhanced humanity or humans as “errors”. Utopian and Dystopian futures.

The future fights: Adding artificial intelligence into computational processes?

- The Californian utopia: enhanced humanity or humanity “plus”, cyborgs as our future
- Humans are already cyborgs: medicine, nanobots
- Artificial intelligence and inclusion of neurons in mechanical systems
- Budgets for these projects
- Avoiding human face-to-face relations?
- Science fiction movies about mass surveillance, techno totalitarianism, the cyborg culture
- A critical theory of media and film studies: Taking fiction seriously as a cultural phenomenon
- Popular culture and “Do It Yourself Surveillance”, Artistic practices: the pleasure to obey or a way to fight (through uses of irony) the massive film industry
- Realist Fictions: refusing to play the science fiction and eroticisation of secret services
- Critique of James Bond: secret agents and women roles
- John le Carré: shaping popular culture; the french series: “Le bureau des légendes”
- Surveillance for data intelligence:
  - Killing abroad? Techno-spying?
  - Preventive counter-terrorism and infiltration operations
  - Fictionalisation of practices.

Guest speakers: around le bureau des légendes from DGSE, from the series producer, from critical media studies

Readings

- https://www.youtube.com/watch?v=VLN400CGEh8
- ‘PredPol – The Science Behind Predicting Crime’ via PredPol, 10 April 2015
https://www.youtube.com/watch?v=FC-OHhTG2sk
COURSE OUTLINE

- Sadin, Éric. La vie algorithmique. Critique de la raison numérique. Échappée (L'), 2015.

Bibliography

Readings specifically on anonymity
- Philippe Aigrain, « Le droit à l'anonymat et au chiffrement », in : Médiapart, (fév. 2015)