Global Cybersecurity

Description

This course plots the emergence of cybersecurity as a critical political issue around the world. Technological progress, accompanied by globalisation, has transformed the ways in which economic life is conducted. The increasing importance of information systems in conducting everyday activities - affecting supply chains, administration, and potentially resulting in the automation of large economic sectors - continues to expose increasing numbers of vulnerabilities to different state and non-state actors. Surveillance has been enabled, to a greater extent than previously believed possible, and the use of 'big data' to store multiple points of referenced data has extended the potential for invasive techniques. The development of remotely controlled and semi-autonomous weapon systems has also opened up further, important questions regarding the nature of state power and security in a networked society, which will be investigated by the course. The course aims to give students the ability to understand, assess and review the effectiveness of various cybersecurity strategies, including examination of those societies which have overtly restricted internet access. Additionally, social networks have impacted the way in which state propaganda is being disseminated. These questions are explored in a way to encourage understanding of the way politics and society is evolving. Students are encouraged to incorporate these approaches into theories relating to international relations and comparative politics.

Learning Objectives

- Examine society's increasing dependencies upon technological infrastructures and associated vulnerabilities;

- Establish a clear historical view of how cybersecurity has emerged as a crucial factor in questions of domestic and international politics, and develop awareness of the implications of this;

- Explore the emergence of information systems underpinning methods of waging warfare, subterfuge and espionage;

- Examine the impact of the mobile web, Internet of Things and social networks upon surveillance, state power and political activity;

- Consider cybersecurity within different models and frameworks of international relations and conflict resolution, incorporating critical perspectives;

Required Materials

Lessons

Definitions of cyberspace and historical conceptions of security

a) What is cyberspace? Understanding technology as understanding the world

b) What is security? Technical, sociological, psychological and international definitions

c) Cybersecurity and technological development

d) Cybersecurity and comparative / non-comparative politics

e) definitions of the ‘other’ and suspicion

f) historical basis: spying, examples

Critical infrastructure vulnerabilities

a) film of incident/s

b) slide show of Telco and related hacks

c) how dependent are we? As individuals.

d) Supply chains and companies

e) market volatility and information

Exploits, hacks and consequences

a) impact on municipalities

b) EMC scenario

c) 1998 report

d) which institutions are most vulnerable? why? What kind of vulnerabilities would exist?

e) mitigating attacks

Weaponisation of networks and systems

a) What is ‘war’? Conflict and technology, esp broadcasting

b) examples of codebreaking

c) Encryption and the Cold War

d) Backdoors and insecure technology

Hacker culture and tech utopia/dystopia

a) the emergence of silicon valley

b) the first online communities

c) tech utopias vs dystopias incl. IBM.

d) automation and AI- Hacktivism and whistleblowing

Social movements online

f) public service and the national interest, theories of the ‘military-industrial complex’

g) social movement theory and strategies of activism

h) theories of hierarchy and oligarchy

Policing the web - Western strategies for security and insecurity

a) preventing anonymity

b) tapping cables

c) equipment and infrastructure

d) imbalance between embedded state power - to what extent in the 1990s was the US running the web - and counter-reaction

e) Full-spectrum dominance and PNAC - role of ideology

Strategies of hybrid warfare - the use of different channels and media by different actors

a) What is propaganda? How reliable is the news you listen to?

b) What is fake news? Historical role of misinformation

c) emergence of 24-hour news culture - but whose news?

d) commercial imperatives vs state broadcasting

The rise of social networks and the fall of privacy - advertising and commodification

a) ‘Here comes everybody’

b) ‘free’ services

c) the rise of Adwords and Facebook

d) big data and data mining, the role of metadata

e) the surveillance state and society. What of democracy?

The development of the mobile web - apps, gadgets and monitoring

a) cellphone design and security

b) the emergence of smart phones and mobile data

c) designing apps for reward

d) implications of phones for tracking and monitoring

e) convergence

Internet of Killing Things: drones, artificial intelligence and robot soldiers

a) principles of the 'internet of things'

b) development of sensors and automation

c) the evolution of drone technology

d) assassination by drone and international law

Theories of 'securitization' - perspectives on violence and security as a political phenomena

a) Theories of social and political change

b) geography of cyberspace - gated communities and walls

c) military-industrial complex and security apparatchiks

d) military doctrine and the role of cyberdefence

e) the challenge of retaliation

States and online power

a) Social contract

b) algorithmic computational way of seeing relationships eg solution-ism

c) accountability and openness

d) contrast between low-tech, crumbling public infrastructure and high-tech (public squalor, private affluence)

Liberal models of primacy and system change

a) theories of development (Roslow)

b) Whig approach based on progress, developmental economics

c) Castells and conflict theory - cyberspace as competitive domain for different interest groups

d) conflict analysis: Harvard, human needs, conflict transformation

e) wheel, tree, mapping. escalation, perspective, needs-fears, multi-causal

Ethics and cyberspace, cyberwar and cyberpeace

a) Is the logic of computational thinking peaceful? Dominance of commerce/power, too powerful

b) does the medium dominate the message, and how?

c) public policy and an environment ‘for the cause of security’

d) adapting to a changing world - resource wars and competition