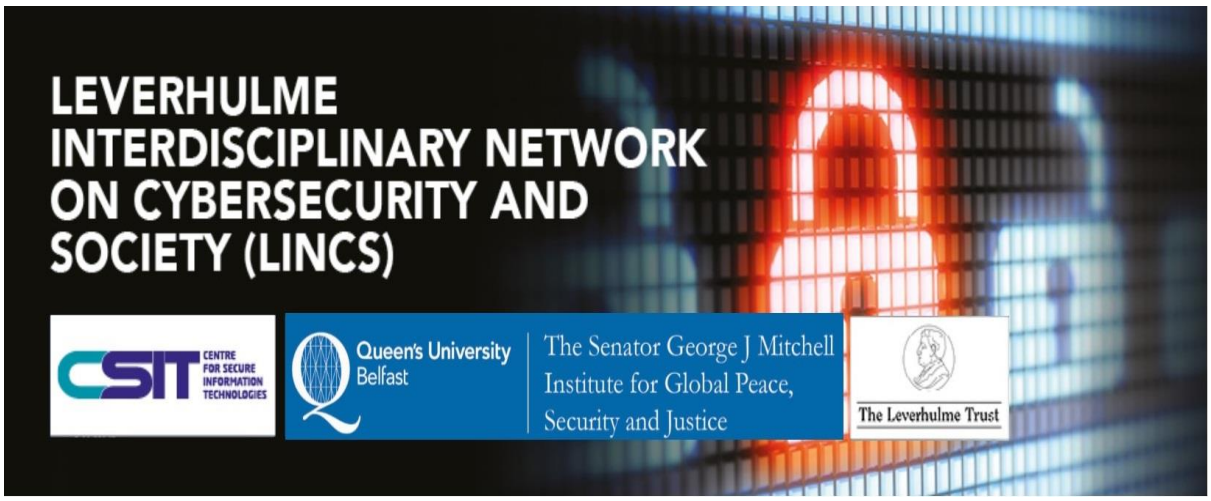
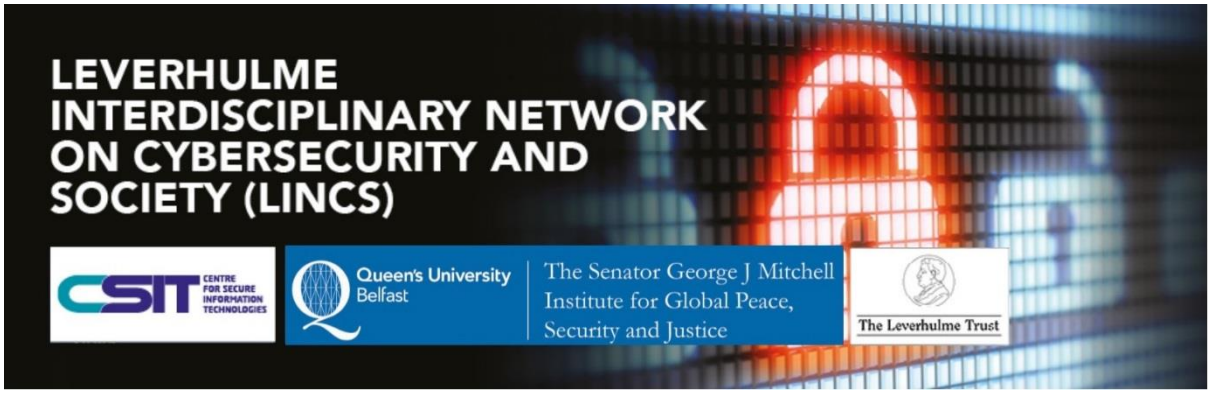
LEVERHULME INTERDISCIPLINARY NETWORK ON CYBERSECURITY AND SOCIETY (LINCS)

DOCTORAL SCHOLARSHIPS 2017





Guidance for Applicants, September 2017 entry

Contents

ABOUT THE PROGRAMME

The Leverhulme Interdisciplinary Network on Cybersecurity and Society (LINCS) at Queen's University Belfast was established in 2015, to support pioneering research at the interface between the social sciences and electronic engineering & computer science.
LINCS brings together the Senator George J. Mitchell Institute for Global Peace, Security and Justice (Mitchell Institute) and the Centre for Secure Information Technologies (CSIT) to develop a distinctive cohort of doctoral students working across the boundaries of their disciplines who will open up new avenues of enquiry centred initially on the priority themes and specific PhD projects.

LINCS opens up new avenues of enquiry on Cybersecurity through 4 priority research areas:

1. **Cybersecurity: Technology and Ethics**
2. **Cyberspace, Privacy and Data Protection**
3. **Debordering and Rebordering in Cyberspace: Technological, Legal and Political Aspects**
4. **Borders, Security Technologies, Data Gathering and Data Sharing**

The LINCS project runs from 2015 to 2021, funding a total of 30 Doctoral Scholarships.

LEVERHULME DOCTORAL SCHOLARSHIPS

There are 7 Leverhulme LINCS Doctoral Scholarships available in 2017, to outstanding eligible candidates, for full-time study over 3 years. Full details on the research projects are provided in the next section - Available Scholarships.

The Scholarship covers

- Full tuition fees at Standard UK Rates (£4,121 per annum) for three years (based on 2016/17 rate – 2017/18 rate to be confirmed).
- A maintenance award at the Research Councils UK Rates (£14,296 for 2016/17) for three years
- Research Training and Expenses £1,000 per annum for three years.

ELIGIBILITY CRITERIA

- Applicants must hold a minimum 2nd Class Upper Degree (2:1) or equivalent qualification in a relevant Technology, Social Science or Humanities Based subject.
- Applicants must be a UK or EU citizen.
- Applications from non-UK or non-EU citizens may be accepted on an exceptional basis but additional funding to cover International student fees is not available and must be secured by the applicant prior to starting.
- Applicants must be proficient in both writing and speaking in English.
- Successful applicants must be prepared to live and work in Northern Ireland for the duration of their studies.
- Interested candidates must consult the main topic contact at the earliest possible opportunity to discuss their research plans and application, or Professor Cathal McCall in relation to an Open Proposal.

AVAILABLE SCHOLARSHIPS

1. THEME - Cybersecurity: Technology and Ethics

PROJECT: Robotics, Autonomous Learning and the Algorithm: Delineating Criminal Responsibility and Legal Liability in the New Machine Age
Lead Supervisor: Prof John Morison
Co Supervisors: Dr Paul Miller, Prof Weiru Liu, Dr Debbie Lisle, Dr Muiris MacCarthaigh, Dr Mike Bourne, Dr Danny Crookes
Primary Location: CSIT/Mitchell Institute

Rapid developments in technologies around robotics and machine learning are being accelerated by the development of autonomous learning drawing on big data and the internet of things. This throws up a series of radical challenges for the legal system around the attribution of criminal responsibility and legal liability in the context of a range of new challenges from driverless cars to smart medical devices; digital personal assistants to advanced autonomous advice systems; and from delivery drones to self-governing policing and weapons systems. The legal implications are becoming increasingly complex. The applications that make up a "smart" home or office may fail. As things stand now the supplier is probably liable for any damage caused. But we are on the threshold of a more complex world where existing understandings provided by product liability law, legal notions of consent and criminal responsibility may be tested to destruction. As applications become more complex and more embedded within our social and economic systems the potential for negative interactions multiply. What if a malfunction in the sense of a "fault" develops as a result of a device's autonomous learning? Software used in financial markets to buy and sell in response to complex, self-generated algorithms can make decisions with major implications but these may be blind to non-technical factors such as their impact in relation to gender, class or ethnicity. Or they may contain or produce misstatements which, if they were from a human source, might be regarded as negligent, reckless or deliberate. Similar concerns and others manifest themselves immediately in relation to policing and defence applications. What is the initial programmer's responsibility? When, within the development of a self-learning machine, should the designer "pull the plug"? What is to be done about applications that are already in market? A researcher with a background in *either* law *or* technology would be well placed to explore these important issues.

This fits in well with existing LINCS studentships – Harkens, Gilbert etc - which generally are exploring the adequacy of the legal paradigm within this wider context as well as a number of Law School PhDs – Cobbe, McCusker – which are developing theoretical aspects of similar questions. It also contributes generally towards the algorithmic governance research application which is currently in preparation.

Primary Academic Discipline: This would suit EITHER

1. a law (or possibly social science) graduate who wishes to apply existing legal background to new technical area OR EQUALLY
2. A computer science graduate with background in machine learning who wishes to explore the legal and other implications of the technology

PROJECT: A Safety Inspired Approach to Solving the IoT Cyber Security Dilemma
Lead Supervisor: Dr Kieran McLaughlin
Co Supervisor: Dr Mike Bourne
Primary Location: CSIT

By 2020 there may be 50 billion globally connected devices. Driving this growth is the emergence of Internet-of-Things (IoT) devices: low cost sensors, body worn devices, household appliances, vehicles, etc. Poor cybersecurity in IoT devices such as webcams has already resulted in huge IoT powered botnets generating DDoS traffic at *terabit* rates. However, future attacks may go beyond the *cyber* domain into the *physical* domain. Tumble driers and fridges regularly cause fires in homes – what if these devices were internet-connected but with such poor cybersecurity that physical faults or vulnerabilities could be triggered? Who is responsible? Who should be *legally* responsible? With seemingly no incentive for anyone to take responsibility for the IoT cybersecurity challenge, is it time for government to intervene to ensure the protection of citizens?

Government has previously legislated to ensure effective safety measures are developed and adopted by industry to meet certain targets. Legislation defines legal requirements for water quality. Regulations define exhaust emission standards for vehicles, and there are requirements for safety features such as daytime running lights. In such cases, the government does not prescribe technical mechanisms that should be adopted to meet legal requirements. The design and technical workings are developed by the relevant service provider or manufacturer. Government does not specify how to manufacture daytime running lights.

This PhD will examine what is feasible, via legislation and regulation, to ensure the security problems posed by IoT devices are addressed.

- What are the technical challenges in IoT cybersecurity?
- Stakeholders include devices owners, ISPs, manufacturers and retailers. What are their legal rights and responsibilities regarding possible legislative solutions? Who is responsible?
- What are the parallels between legislation for health and safety and for IoT device cybersecurity? How might similar approaches be applied to IoT?
- Increasingly ISPs must retain data, reveal file-sharers' IP addresses, filter certain websites, etc. Is there a technical role for ISPs to mitigate IoT exploitation?

Primary Academic Discipline: Computer Science

PROJECT: First Person Tracking and Retrieval using Second and Third Person Video
Lead Supervisor: Dr Paul Miller
Co Supervisors: Prof Brice Dickson
Primary Location: CSIT

The domestic market for overt use of police Body-Worn Video (BWV) is potentially very large. Public Order deployments of police generally include both Forward Intelligence Teams

and Evidence Gathering Teams, who are overtly collecting video footage of subjects using BWV (this is also known as second person video). One of the issues is how to exploit the data in order to provide enhanced situation awareness, both to officers on the ground and back at command and control centres. The research question addressed by this work is: Can data analytics for BWV networks be used in to recognise and track persons of interest during a public order incident? Specifically, given a third person video from a CCTV camera, the system will retrieve all second person video of those individuals in the third person video, acquired by police officers during the public order incident. Conversely, given a second person video containing an individual's signature, the system, will retrieve third person video containing that individual. This will build on previous work that we have performed in this area for static mounted CCTV sensor networks. Specifically, we will address the novel challenges posed by BWV such as camera jitter, moving background and reduced resolution. In this work we will employ a 3-D multi-target tracking algorithm developed for tracking subjects in conventional CCTV systems where the camera angle is acute. This is known as third person video. We will develop a technique for matching a set of egocentric videos with an acute-view video. Following this, we will then associate each egocentric video with a viewer in the acute-view. In the second stage we propose the use of bipartite graph matching between each egocentric video and each viewer in the acute-view. In the third and final stage, those viewers not associated with an egocentric video, will be associated by performing person re-identification between their signatures in the ego-centric video and the acute video.

The Security Innovation and Demonstration Centre (SIDC) recently hosted a workshop on Body-Worn Video and the Digital Criminal Justice System. Dr Chris Rampton, who is Director SIDC, is a member of the CSIT advisory board and has expressed an interest in this work. This project will partner another LINCS project supervised by Professor Brice Dickenson entitled "The Use and Potential of Body-Worn Cameras for Policing Purposes", which will focus on examining and evaluating practice to date in a range of jurisdictions and making an assessment in particular of the technical as well as the human rights challenges which the use of such technology entails.

Primary Academic Discipline: Computer Science

PROJECT: Deeply Ethical: Unlearning Multiple Tasks
Lead Supervisor: Dr Paul Miller
Co Supervisors: Dr Jesus Martinez del Rincon and Dr Tom Walker
Primary Location: CSIT

The research question this proposal tries to answer is: Can we design machine learning algorithms that are ethical? The ethics of machine learning is not so much about the algorithms, as the fact that there might be a bias in the dataset. For example, one might be training a neural network to verify a person, however, in doing so the system might inadvertently learn about their gender, or even race. Previously, we have developed a deep learning Siamese convolutional neural network for person re-identification. During training the network is also tasked with learning other attributes about the person, such as gender, hair colour, clothing style etc. The learning of the multiple tasks is achieved by having cost functions for each task which promote good performance on the task. Therefore, we propose to modify this multi-task approach in which we modify the cost function to ensure it

does not promote the learning of other attributes. We will specifically explore the use of other cost functions such as Fisher ratio, KL divergence, entropy etc, to generate features that are not useful for the other tasks. Another name for this could be multi-task unlearning. Furthermore, we will investigate whether the multi-task unlearning detrimentally affects the efficiency of the single task learning for which we are trying to design the network.

Primary Academic Discipline: Computer Science

PROJECT: Programming Security Ethics in Cyber-Physical Systems
Lead Supervisor: Dr Mike Bourne
Co Supervisors: Dr Kieran McLaughlin and Dr Tom Walker
Primary Location: Mitchell Institute

This cross-disciplinary project explores the possibilities, challenges, and politics of programming security ethics. Particular formations of security practice emerge around novel technologies at all stages from inception through development to commercialisation and use. Thus, security is built in and through new technologies. This project seeks to explore how ethics can also be built-in. Recent developments in the practice and politics of security technology development (e.g. Privacy by Design (PBD); requirements for addressing ethical and societal impacts in European projects, etc.) require deeper engagement with the possibilities, challenges and limits of building ethical principles into security technologies.

The project focuses on the intersections of cyber-physical systems, prominent in the 2016-21 UK Cyber-Security Strategy (e.g. Critical Infrastructure Protection; Internet of Things), that raise issues in understanding security that neither cyber-security nor traditional physical security frameworks are well suited to tackle. Building on recent developments in International Security studies that are attentive to either cyber security or the materialities of security (e.g. CIP) and their intersections (e.g. smart cities), this project explores the politics of technology, and the political actions and effects of technology, in relation to how particular forms of ethics and security (and security ethics) can become scripted in social and political relations. It addresses the following questions:

1) What understandings of security are being built into emerging technologies?
2) What ethical issues surround these practices?
3) How are security and ethics programmed or scripted in the development of cyber-physical security technologies?
4) How do those involved in developing cyber-physical systems engage security ethics?
5) What are the possibilities and limits of extending PBD-type approaches to wider social and ethical concerns?
6) How do such approaches settle what is ‘ethical’ or cut off the process of ethical contestation?

Primary Academic Discipline: Politics/Security Studies

PROJECT: Social Media, protest and human rights
Lead Supervisor: Dr Neil Jarman
Co Supervisors: Prof Hastings Donnan and Professor Sakir Sezer
Primary Location: Mitchell Institute

Social justice activists have been early adapters and improvisers of new technologies and social media and have often applied these to circumvent controls and restrictions by the state. From the early use of SMS messages to organise flash mobs in 2003, the first so-called Twitter revolutions in Iran and Moldova in 2009, the use of Facebook in Egypt and the Arab Spring of 2011 and the adoption of Firechat by Hong Kong protesters in 2014, activists have adapted new technologies in imaginative and unforeseen ways.

While the importance of social media has been widely recognised in some jurisdictions, with Hillary Clinton, for example, describing it as 'the public square of the 21st Century', the state has often struggled to develop a consistent response to such activism, and too often resorted to surveillance of activists and legal restraints. There is a growing recognition that the use of social media and related activities falls within established legal and rights frameworks, but the changes have been occurring so fast that they have also outstripped a clear application of our contemporary understanding of human rights for the new forms of social activism.

The research studentship will investigate these changes from an interdisciplinary perspective to investigate how social media has been utilised in relation to public protests and forms of freedom of assembly. The key Research Question to be investigated are:

1. How has social media has been used over the past decade in relation to protests and freedom of assembly in physical space?
2. What are the key human rights issues impacted by social media use in protests?
3. What technological developments that have taken place in the past decade in relation to social media platforms used in public protests?
4. How has the state responded to the use of social media in protests through forms of surveillance, technology, and legal?

The proposed project will link with Jarman's ongoing work on freedom of assembly and his work with the OSCE/ODIHR, which has identified a lack of clarity in relation to the use of social media within a human rights framework.

Jarman will be able to facilitate contacts with key organisations such as the OSCE/ODIHR; Article 19; Electronic Frontier Foundation; and the UN Special Rapporteur on Freedom of Assembly; and with civil society organisations involved with protests in a variety of different countries.

Primary Academic Discipline: Anthropology

PROJECT: Human pose estimation for real scenarios. Dealing with multiple people and interaction
Lead Supervisor: Dr Jesus Martinez del Rincon
Co Supervisors: Dr Paul Miller and Dr Debbie Lisle
Primary Location: CSIT

Human pose recovery is one of the most challenging research areas in computer vision. Successful estimations of the human pose provide information and simplify further tasks such as activity recognition or behaviour analysis, and therefore, it can benefit a wide range of industrial sectors such as video surveillance, physical security or sport performance enhancement.

Constant steps forward have been made in this field, solving the problem for a single person performing a simple and repetitive activity in heavily constrained scenarios. However, pose recovery of complex actions in an unconstrained environment still remains a challenging problem. Even more if we consider that interaction scenarios are of particular interest, where the actions of one of the subjects condition the others, e.g. martial arts, boxing, football in the sports domain, fighting, theft, exchanging luggage in the surveillance domain and dancing in the arts domain. To our knowledge, no research has been done for simultaneously recovering the pose of multiple people on video footage.

The aim of this project is to produce a system that tracks the articulated motion of a group of human beings that interact with each other in the scene. The system should be able to work in real life scenarios, such as sport analysis and video surveillance, combining information from multiple cameras. The project will incorporate and combine techniques from different field of expertise, such as activity recognition, action modelling, pose estimation and human tracking.

Objectives:

- To design experiments where interacting subjects condition each other actions
- To construct an activity datasets that realistically contain interactive activities
- To model the space of interactive activities by combining non-linear dimensionality reduction methods with advanced Markovian approaches
- To assess the adequacy of the interactive models to detect abnormal or antisocial interactions
- To develop pose estimation algorithms capable of consider occlusions and interactions between multiple people and its impact in the individual pose estimation, as well as developing strategies to tackle their inherent problems.
- To validate the above approach, by implementing a system that tracks the 3D pose of small groups of interacting people from video footage on a general purpose scenario

Primary Academic Discipline: Computer Science

---

2. THEME: Cyberspace, Privacy and Data Protection

PROJECT: Preventing and detecting blackmail resulting from the use of webcams
Lead Supervisor: Professor Brice Dickson
Co Supervisors: Dr John Topping and Dr Paul Miller
Primary Location: Mitchell Institute

This research programme will explore the phenomenon of 'webcam blackmail'. This occurs when victims are induced into recording intimate acts in front of cameras on computers and smartphones. The footage is then used by criminals to extort money in return for not publicly releasing the videos. Victims often pay large sums to blackmailers and are unwilling to tell the police what has happened. Criminals tend to target vulnerable individuals, especially teenagers. Sadly, several victims have committed suicide or otherwise self-harmed.

As well as seeking to assess the nature of the problem (including its extent and the profile of victims) the research will explore technical and legal measures which might be taken to reduce the prevalence of the crime. It will research techniques which may prevent such recordings being made in the first place, examine law enforcement measures which could limit the release of such footage, and consider technological and legal steps which affect the ability of policing agencies to identify the perpetrators.

The research will also consider the legal liability of internet service providers and social media companies in this context and investigate how victims might obtain remedies from the perpetrators and/or from those who have facilitated or benefited from the crime. Legal principles drawn from domestic and international laws on confidentiality, data protection, intellectual property, human rights, child protection, criminal justice and enforcement of judgments will be researched to suggest

The research will be explicitly inter-disciplinary in that the researcher will be expected to have and to develop some technical awareness of how webcams may be controlled but also to have a knowledge of basic legal principles and of how they can be deployed to ensure that people are protected against harmful behaviour. how they can be moulded in ways which allow webcam blackmail to be dealt with more effectively.

The key research questions will include:
1. How extensive is the phenomenon of webcam blackmail?
2. How can technology reduce the occurrence of this crime and improve detection rates?
3. What steps can the law take in this context?

Primary Academic Discipline: Criminology

PROJECT: Social Media as 'Intelligence' – Policing Through Public Data
Lead Supervisor: Dr Huiyu Zhou
Co Supervisors: Dr Michelle Butler and Dr Paul Miller
Primary Location: CSIT

Email clients and web browsers are two types of communication tools commonly used in our society. Comparing these tools, email is continuously monitored and secure, whilst social media is full of conversations that may be public and potentially become "dangerous". Evidence shows that accidental disclosure on social media is one of the major risks to business corporations. This could be anything from **financial information** through to the **private experiences** of authors.

In this research project, we intend to develop an automated software tool that allows us to continuously monitor one or several social media websites (e.g. Bloomberg and Twitter) for understanding the financial implications of messages left on social media. To do so, we will extract keywords from these on-line messages using an established WordNet library. Then, machine learning techniques, such as deep learning, will be developed to detect and remove those **inside threats**.

One of the main research challenges in this study is whether or not financial inference buried in social media messages can be identified using the methods described above. On the other hand, sentiment analysis with information theory will be investigated to quantify the relationship between social media messages and corporations' finance. The objectives of our study can be summarised as follows:

(1) To create a training database using individuals' comments shown on social media (e.g. Twitter).
(2) To develop a novel framework using machine learning techniques to establish the relationship between social media messages and corporations' finance.
(3) To develop sentimental analysis techniques with information theory to measure the relationship described in (2).
(4) To evaluate the proposed system using online social media messages.

Dr H Zhou (Primary Supervisor of this proposal) has been working with Dr Dong Li from Hong Kong Baptist University on information diffusion for one year, who is sponsored by the Hong Kong Scholar Program of China (No. ALGA4131016116). In the information diffusion project [1], we simulate and predict temporal dynamics of the information diffusion process, which helps us deeply understand social media dynamics. This has laid a solid foundation for the project proposed in this new proposal.

[1] D. Li, S. Zhang, H. Zhou, X. Sun, S. Li and X. Li, "Modeling information diffusion over social networks for temporal dynamic prediction", IEEE Trans. On Knowledge and Data Engineering, under review.

Primary Academic Discipline: Computer Science

PROJECT: Extending state capacity through algorithmic governance: How can machine learning extend the state's predictive capability?
Lead Supervisor: Dr Muiris MacCarthaigh
Co Supervisor: Dr Paul Miller
Primary Location: Mitchell Institute

Algorithmic governance is an emerging concept in the political sciences that denotes the increased prevalence of sophisticated algorithms used to arrive at and make decisions on key questions of public policy. With machine learning causing ever more data to be generated and gathered by public bodies, and more connections and relations being mapped and manipulated, algorithmic governance poses very significant questions for how we understand the role of national public administration systems in the modern age. Such questions that go beyond those of 'digital-era governance' identified by Dunleavy et al (2006) which pointed to the increased use of online public services and virtual modes of citizen-state engagement. Instead, more new concerns have emerged with automated decision-making including unconscious bias in the design of systems used for the public service delivery and the effects of data-driven assessments of public service performance.

Notwithstanding these concerns, however, algorithmic governance and machine learning also offer great potential in terms of extending state capacity. We may consider state capacity as, essentially, encompassing what the state is able to get done through its public administration, i.e. delivery of public services, regulating activity by state and non-state actors, and providing economic incentives to the market. Of concern to this PhD project, however, is the relatively unexplored field of how algorithmic governance and machine learning can help the state's capacity to *predict* service needs and to prepare for them. This study of what we term predicative capability is concerned with forecasting and intelligence that inform policy-making on what kinds of future demands and challenges are likely to emerge. To make sense of the massive quantity of information, predictive capability requires decision-making about what to know and how to find the necessary information. The project will explore this by considering two policy arenas – health and security services.

Working with the cross-disciplinary supervisory team, the successful applicant will be first required to develop a taxonomy of state capacity and the extent to which algorithmic control could be (and has been) applied to key components of this capacity (such as policy competence and organisational performance). Then, adopting an inductive approach based on a number of thematic case studies, the studentship explore the use of algorithmic governance and machine learning in a series of contexts including, at least, the following:

Health services – The focus here is on the use of machine learning to help radiotherapy planning treatment.

Security services – The focus here is on the use of machine learning to predict anti-social behaviour.

Combined, these case studies will provide new insights as to how machine learning extends the state's predictive capability and in so doing the studentship will make a major contribution to both academic public administration and cybersecurity research. The ideal candidate will have sufficient technological awareness to understand machine learning - based algorithmic decision making applications and the use of big data for decision-making.

A candidate with awareness of privacy law will also be at an advantage for the project, though this is not essential.

Refs
Dunleavy et al. 2006. *Digital-Era Governance: IT Corporations, the State and E-Government*. Oxford: Oxford University Press.

Primary Academic Discipline: Public Administration

---

3. THEME - Debordering and Rebordering in Cyberspace: Technological, Legal and Political Aspect

PROJECT: Emerging Cyber Bordering Technologies
Lead Supervisor: Professor Sakir Sezer
Co Supervisor: Dr Cathal McCall
Primary Location: CSIT

This PhD will combine research on the technological development of cyberborders with the efforts of state governments to defend and penetrate them.

Firewalls, network-based application and user detection technologies, as well as URL black and white lists present essential technological tools for building borders in cyberspace and preventing cross-border access to web-content. However, new technologies, based on well-established Virtual Private Networks (VPNs), and new VPN service providers (CyberGhost, Spotflux, Private Internet Access, Hotspot Shield, ProXPN, etc.) have evolved, providing encrypted anonymous tunnels, capable of penetrating virtual borders and providing anonymous access and hosting of unrestricted content via a country specific proxy server.

Defending cyberspace borders for the protection of critical infrastructure, key resources and sensitive information is a key concern for governments. Yet, as the Edward Snowden case revealed, state governments are also deeply implicated in acts of penetrating cyberspace borders for the purpose of information-gathering on friend and foe alike. Similarly, international corporations have a vital interest in securing internal networks, as well as a research and development compulsion to penetrate the cyberborders of competitors in the name of innovation.

This PhD will have 4 key stages:

- At the outset, the research will chart the development and management of cyberspace borders by selected states in the contexts of technology and government policy;
- It will then examine the evolution of VPNs and service providers in the context of the provision of encrypted anonymous tunnels that penetrate cyberborders;
- It will consider the political implications of a policy of cyberborder penetration by governments for the purposes of espionage.

- Finally, it will assess the prospects for integrated cyberborder management systems between 'friendly' states.

Primary Academic Discipline: Computer Science

---

4. THEME: Borders, Security Technologies, Data Gathering and Data Sharing

PROJECT: Social Media as 'Intelligence' – Policing Through Public Data
Lead Supervisor: Dr John Topping
Co Supervisors: Prof Brice Dickson, Dr Paul Miller
Primary Location: Mitchell Institute

The wide array of current social media platforms represents a significant source of information for police organisations to use in the management and prediction of crime, crisis and security. With over 1.7 billion Facebook users and 200m regular Twitter users producing 500m Tweets per day, the digitisation of human behaviour, sentiment and action represents an enormous pool of data through which more informed and intelligence-led forms of policing may be considered.

Beyond 'traditional' forms of policing, social media and website-based information can further provide police with the capacity to understand and monitor individual/group behaviours, communications and interactions. Yet how that information can or should be used by police services in the UK remains far from clear-cut.

While commercial bodies offer a host of potential analytical solutions, such as sentiment analysis, influencer identification, real-time monitoring and community/demographic analysis, 'in-house' social media data capture and analysis by police services remains in its infancy. In this regard, a number of under-developed avenues of inquiry exist for police organisations, including issues of police IT infrastructure, analytical tools and skills, along with what can usefully be 'mined' from social media to inform police decision-making and operations.

Additionally, legal limits and oversight regimes related to the use of social media and internet data by police services remains uncertain. From general principles of privacy, confidentially and discrimination/profiling, or the more specific frames of the Data Protection Act 1998 and the Regulation of Investigatory Powers Act 2000 (RIPA), the relationship between technical capacity and legal limits of this 'new watching' is still evolving.

Overall, the proposed PhD seeks to examine technical, analytical issues related to information which can be extracted from social media and website sources by police organisations, and examine those within the legal and oversight boundaries of the United Kingdom.

Key Research Questions:

What types of information produced on social media are of value to police organisations?

What technical and computing solutions are required to extract data of value to police?

To what extent do legal parameters shape police capacities to engage with, and utilise social media data for policing purposes?

Primary Academic Discipline: Criminology

HOW TO APPLY

The deadline for applications is 5:00pm, Monday 16 January 2017.

ONLINE APPLICATION FORM

If you meet the eligibility criteria and wish to apply for any of these posts, you will need to complete an on-line application via the Queen's University Applications Portal.

You must include the code **LINCS17** on your application form to indicate that you wish to be considered for a LINCS award.

Applicants should chose the option "**I wish to be considered for external funding**" and then enter **LINCS17** in the free text box which follows.

COMPLETING YOUR APPLICATION

- All applicants must provide an up-to-date CV; this should be uploaded to the Admissions Portal as a separate document.[1]
- All applicants are required to provide a **100-400** word statement detailing how their PhD will address the interdisciplinary aspects of the LINCS programme.
- Applicants wishing to propose an interdisciplinary PhD topic of their own, that aligns with one or more of the LINCS priority themes, **must upload a 400 word research proposal** that describes the topic as a separate document. [2] This research proposal must **clearly identify** a potential supervisory team and which of the themes it relates to.
- Applicants must provide the name of an Academic Referee in support. **Failure to provide a referee will result in the application being rejected.**
- **Please note, failure to include the reference LINCS17 in the free text box may result in your application not being allocated or considered for funding.**

The deadline for applications is 5:00pm, Monday 16 January 2017

[1] Please note that **only one document can be uploaded**, you must combine your CV and Research Proposal into one document (word or PDF).
[2] As above note.

PROGRAMME CONTACTS

Programme Coordinator	**Prof Cathal McCall** c.mccall@qub.ac.uk
Training & Skills Coordinators	**CSIT: Dr Philip O'Kane** p.okane@qub.ac.uk **AHSS: Prof Brice Dickson** b.dickson@qub.ac.uk
Internationalisation Coordinator	**Prof Weiru Liu** w.liu@qub.ac.uk
Placements and Partnerships Coordinators	**CSIT: Dr Kieran McLoughlin** kieran.mclaughlin@qub.ac.uk **AHSS: Dr Muiris MacCarthaigh** m.maccarthaigh@qub.ac.uk
Pastoral Support Coordinator	**Prof John Morison** j.morison@qub.ac.uk
Programme Reporting Coordinator	**Prof Cathal McCall** c.mccall@qub.ac.uk
Supervisory Teams Coordinators (Theme)	Cybersecurity: Technology and Ethics **Prof Sakir Sezer** sakir.sezer@qub.ac.uk Cyberspace, Privacy and Data Protection **Dr Tom Walker** tom.walker@qub.ac.uk Debordering and Rebordering in Cyberspace: Technological, Legal and Political Aspects **Dr Debbie Lisle** d.lisle@qub.ac.uk Borders, Security Technologies, Data Gathering and Data Sharing **Prof Hastings Donnan** h.donnan@qub.ac.uk
Research Ethics Officer	**Dr Tom Walker** tom.walker@qub.ac.uk
Programme Administrator	**Ms Valerie Miller** v.miller@qub.ac.uk