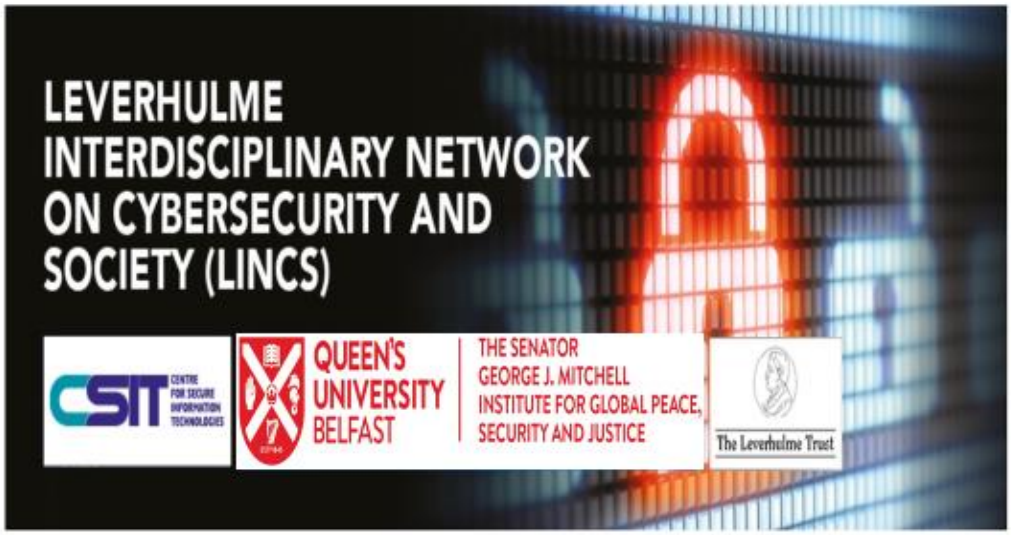
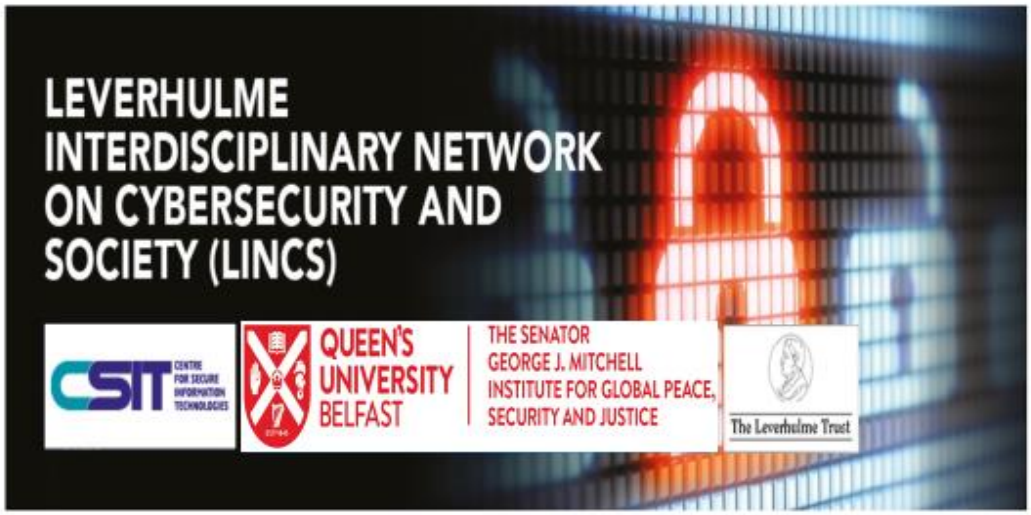
LEVERHULME INTERDISCIPLINARY NETWORK ON CYBERSECURITY AND SOCIETY (LINCS)

DOCTORAL SCHOLARSHIPS 2018





Guidance for Applicants, September 2018 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**

Projects are welcome from within these themes or other related areas of interest to the applicant. Please contact a relevant academic member of the team to discuss your idea. Professor John Morison (j.morison@qub.ac.uk) is the acting coordinator of the programme and can assist in directing inquiries.

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

LEVERHULME DOCTORAL SCHOLARSHIPS

There are 5 Leverhulme LINCS Doctoral Scholarships available in 2018, 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 (£4,195 per annum) for three years (based on 2017/18 rate – 2018/19 rate to be confirmed).
- A maintenance award at the Research Councils UK Rates (£14,553 per annum – based on 2017-18 rate) 2018/18 rate to be confirmed) 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 John Morison 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, Dr Huiyu Zhou, Dr Muiris MacCarthaigh, Dr Mike Bourne, Dr Kieran McLaughlin
Primary Location: CSIT/Mitchell Institute

Rapid developments in robotics and machine learning, which will be only accelerated by the development of big data from the internet of things, have already transformed human society. This revolution in how we live everyday will increase in reach and scope as sophisticated algorithms develop autonomously, and are deployed through robotic technology with hugely improving cognitive abilities. This raises interesting (and familiar) philosophical issues as to whether these autonomous learning machines have consciousness or other attributes of personhood. An important and practical way of unpacking such questions, and exploring others, involves focusing on the criminal responsibility and legal liability for such technologies.

As technologies of this kind advance from driverless cars to smart medical devices, from digital personal assistants to advanced autonomous advice systems, and from delivery drones to self-governing policing and weapons systems, the legal implications become 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. What is the position in routine, real-world use if a driverless car or a drone is programmed (or has programmed itself) to cause minimum damage between two humans when faced with an inescapable collision? Where should tortious liability (in the sense of compensation) lie or criminal responsibility be attributed?

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” or inappropriate application (as we might understand it from within our complex social and economic context) 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" in relation to the potential harms that it may cause? What is to be done about applications that are already in market?

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 student with background in machine learning who wishes to explore the legal and other implications of the technology

PROJECT: Robotics, Autonomous Learning and the Algorithm: Delineating Criminal Responsibility and Legal Liability in the New Machine Age
Lead Supervisor: Dr Paul Miller
Co Supervisors: Dr Paul Miller, Dr Graham Ellison
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 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. 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 Dr Graham Ellison, 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

2. THEME: Cyberspace, Privacy and Data Protection

PROJECT: Regulating the Use of Big Data: The challenge for government
Lead Supervisor: Dr Muiris MacCarthaigh
Co Supervisor: Dr Cheng Long, Professor John Morison
Primary Location: Mitchell Institute

Big data constitutes 'information that can't be processed or analysed using traditional processes or tools' (Eaton et al. 2015: 3). It can be characterized in a number of ways, for example by 5Vs: Volume, Velocity, Variety, Veracity, and Value (Kune 2011: 1). In general, big data is information that is not structured or easily interpreted by traditional databases or data models, and the majority of it is text-heavy (Arthur 2013). Conversely, multi/semi-structured data constitutes a wide variety of data which can be derived from interactions between people and machines, such as web applications or social networks. Current estimates are that 80 percent of the world's information is unstructured data, and the volume of this is growing at 15 times the rate of structured data.

The big data 'revolution' presents a number of unique challenges for government. These range from practical issues concerning the toll placed on a government's administrative hardware and software infrastructure by an ever-expanding data footprint, to the need for data management skills within government, to the economic challenge of ensuring markets based on big data work well for citizens and businesses. We may summarise the many challenges presented by big data for government as twofold: firstly, ensuring the state is in a position to make effective and meaningful use of data (primarily a technological and administrative challenge) and, secondly, discovering how best to balance the opportunities afforded by big data against the social and ethical questions its use raises.

The purpose of this PhD study will therefore be to initially explore the range of regulatory challenges faced by governments arising from big data use across economic, social and political domains, and from this develop a regulatory taxonomy. Next, the study will involve the development of a conceptual model that addresses these multiple regulatory challenges. This model will then be tested through the use of a limited number of case studies involving big data usage by citizens and firms, and in respect of both historical and real-time data use contexts.

Combined, these case studies will provide new insights as to how big data use can be regulated and in so doing the studentship will make a major contribution to both academic public administration and data analytics research. The ideal candidate will have some technological awareness including the use of big data for decision-making. A candidate with basic legal training will also be at an advantage for the project, though this is not essential.

The thesis will be supervised draw upon the disciplines of public administration, data analytics, political science and law.

Primary Academic Discipline: Public Administration

3. THEME: Debordering and Rebordering in Cyberspace: Technogical, Legal and Political Aspects

PROJECT: Algorithmic Ethics and 'Pattern-of-Life' Analysis: The Automation of Everyday Life
Lead Supervisor: Professor Debbie Lisle
Co Supervisors: Dr Kieran McLaughlin, Dr Mike Bourne
Primary Location: Mitchell Institute

Much has been written about how security technologies and algorithms govern by gathering information about the isolated characteristics of people's lives (gender, age, citizenship, religion, purchase history etc.) so as to better understand the characteristics of a whole population. This project engages with more recent arguments about how algorithms and security technologies observe distinct 'patterns-of-life' (POL) behaviours and habits which are then used as the basis for new techniques of governance and intervention. POL analysis is a form of surveillance that constructs a pattern of statistically normal behaviours against which instances of statistical deviance can be identified, tracked, and acted upon. Central to this production of norm / deviance is a pre-emptive frame: the future is made *actionable* so that (a) populations can be encouraged to avoid pre-determined deviant behaviour; and (b) suspect individuals can be identified by their 'pattern-of-life' behaviour and marked as risky *before* they have committed a crime. This project contributes to critical accounts of how the norm/deviant logics underscoring POL analysis map onto more familiar social cleavages to do with race, gender, sexuality, socio-economic position, citizenship status and difference. This PhD project focuses on two areas:

From the Battlefield to Everyday life: Much critical work on POL analysis examines its use in drone warfare: how data points from drone footage produce generalized norms of behaviour against which deviations can be identified. However, the way 'foreign' individuals and populations become suspect through POL analysis is not neutral, but instead maps norm/deviance logics onto prevailing geopolitical asymmetries. In other words, patterns of 'normal' behaviour assume particular Western liberal subjectivities, behaviours and habits, whereas deviations from that norm are attached to bodies that are culturally, ethnically and racially 'different' (Franz, 2017; Pötzsch, 2015; Shaw, 2016). Drawing on those insights, this project explores how POL analysis is now being used to shape, manage and intervene in the everyday lives of subjects, citizens and non-citizens. Certainly law enforcement agencies have been early adopters of predictive systems that can help them mobilize, direct and focus their resources to pre-emptively identified 'hotspots' of crime, and retailers have long used POL analysis to predict consumer demand, behaviour and habits (Bell, 2013; Wall, 2016). This project analyses how POL analysis is being rolled out into the sectors of society that govern our everyday lives such as education, public health and transport, and asks how its central norm / deviant logics are making themselves felt differently in different populations (e.g. citizens, non-citizens).

The Automation of Judgement: The central selling point of POL analysis is its supposed 'neutrality': by allowing algorithms to trawl the data and produce statistically proven norms, governing authorities can avoid charges of discrimination (e.g. 'We are not racist! The data told us to arrest this individual!') In this sense, POL analysis has to be understood as part of

a broader shift into algorithmic governance. However, what remains unclear in the expansion of POL analysis is the transformation in who is enacting political judgement and making decisions. Drawing on recent work in critical security studies, this project puts debates about pre-emption and POL analysis into productive conversation with debates over the ethics of automation and algorithmic governance (Amoore & Piotukh, 2016; Hall, 2018; Lisle & Bourne, 2018). Of particular concern here is the way automation claims to be objective, neutral and impartial while it simultaneously disaggregates populations through familiar categories of race, difference, gender, class and sexuality.

This project emerges from our ESRC grant 'Treating People as Objects' (2014-2016) and helps to develop our current thinking about automation, ethics, materialism and politics. The student selected for this project will become part of our reading group on 'Materiality, Objects, Politics and Space'

Primary Academic Discipline: International Relations (Critical Security Studies / Critical Border Studies)

---

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

Proposals within this general theme are welcome and may be based either within the Mitchell Institute or CSIT.

HOW TO APPLY

The deadline for applications is 5:00pm, Monday 15 January 2018.

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 **LINCS18** on your application form to indicate that you wish to be considered for a LINCS award.

Applicants should choose the option "**I wish to be considered for external funding**" and then enter **LINCS18** 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 LINCS18 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 15 January 2018

[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 John Morison** j.morison@qub.ac.uk
Training & Skills Coordinators	**Dr Philip O'Kane** p.okane@qub.ac.uk
Internationalisation Coordinator	**TBC**
Placements and Partnerships Coordinators	**CSIT: Dr Kieran McLaughlin** 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 John Morison** j.morison@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 **Prof 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