LEVERHULME INTERDISCIPLINARY NETWORK ON CYBERSECURITY AND SOCIETY (LINCS)

DOCTORAL SCHOLARSHIPS 2020

Guidance for Applicants, September 2020 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 Cathal McCall (c.mccall@qub.ac.uk) is the 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 7 Leverhulme LINCS Doctoral Scholarships available in 2020, 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 (£4,327 per annum) for three years (based on 2019/20 rate – 2020/21 postgraduate research tuition fees will be set in early 2020)
- A maintenance award at the Research Councils UK Rates
- 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: Building Interpretable and De-biased AI for use in the legal system
Lead Supervisor: Dr Niall McLaughlin
Supervisory Team: Dr Niall McLaughlin, Prof John Morison, Dr Jésus Martinez-del-Rincon
Primary Location: CSIT

AI and machine learning are increasingly used to aid human decision making, or in some cases to almost entirely replace human decision makers in the legal context. If AI systems are to be tasked with making important decisions, we need to understand those decision-making processes better and develop better tools to enable us to reproduce where possible the behaviour of such systems and understand the circumstances under which they can be trusted.

The most common way to create an AI system today is through a process called supervised learning, where a large corpus of data is used by an algorithm to learn associations between input-output pairs. There are several problems with this approach to AI:

Firstly, the decision-making process is often opaque to the end-user. From the end-user's perspective the system simply produces a decision, but it is not capable of explaining the reasoning process used to reach that decision. Such ideas are inimical to any judicial process and ways of making the decision-making more visible need to be explored.

Secondly, due to inadequacies in the training dataset, combined with the ability of AI algorithms to find correlations, the decisions made by an AI system may take into account factors that should not be used in the legal decision-making process. This may be reflected in biased decisions made by the system or it at the very least it will be a closed system where new problems can only be addressed on the basis of previous solutions. This can lead to a feedback loop where the AI system reproduces and reinforces biases societal, historical and judicial biases.

In order to use AI in the context of legal decision making both these challenges should be addressed.

This PhD will have two key stages:

- Develop novel methods for explaining the decisions made by a modern AI system based on Deep-Learning neural networks. We will examine the links between interpretable AI and adversarial examples in order to generate human-understandable explanations of the AI's behaviour.
- Examine ways to produce more dynamic legal datasets. This will lead to the development of a novel method for representing data, such that AI systems can use

the data for decision making in ways that replicate socially grounded systems with any biases removed, so that a more impartial decision making can be reproduced.

Primary Academic Discipline: Computer Science/Machine Learning

PROJECT: Privacy-preserving functional cryptography
Lead Supervisor: Dr Ciara Rafferty
Supervisory Team: Dr Ciara Rafferty,
Primary Location: CSIT

This PhD will investigate the technological development of functional cryptography from a privacy perspective, taking into account legal and ethical concerns. Functional cryptography is a term describing advanced cryptographic primitives that offer extended functionalities in comparison to traditional encryption schemes and other cryptosystems. Cryptographers are developing a series of techniques that offer fine-grained access control and/or secure computation or communication within groups. These advanced methods are still being improved upon, and further research is necessary. Moreover, any such technologies often claim to be *privacy-preserving* solutions. Can we harness technology to provide privacy by default, to aid user privacy, and enable secure communications?

Despite recent advances, the impact on user privacy, secure communications and computations is yet to be fully explored. Furthermore, what ethical, legal and commercial considerations need to be made to ensure and increase online security and privacy, whilst enabling communication and computation services?

This PhD has the following core objectives:

- Investigate the state of the art in advanced cryptographic primitives and privacy-preserving technologies, particularly functional cryptography
- Analysis of privacy provisions made by promising functional and other advanced cryptographic techniques
- Consideration of practical, legal and ethical considerations, and evaluation against current privacy-preserving approaches
- Analysis of the most suitable technological solutions, and proposal for improvements to user privacy and performance.

Primary Academic Discipline: Data Security

PROJECT: Automated Ethics: Managing Pre-Emptive Discrimination
Lead Supervisor: Professor Debbie Lisle
Supervisory Team: Professor Debbie Lisle, Dr Jésus Martinez-del-Rincon
Primary Location: Mitchell Institute

Recent public controversies have exposed the lingering structures of discrimination in our automated systems of surveillance and governance. Research by Browne (2015) shows us how historically grounded and persistent structures of racial discrimination operate through America's security apparatus, and recent work in Sociology charts how these racialized forms of surveillance make themselves felt throughout the crumbling Welfare State,

especially in Healthcare (Benjamin, 2019). This critical research is important because deconstructs the promise of automation – that by simply allowing the algorithms to connect multiple data points and produce a 'person of interest', we will get rid of human discrimination altogether (i.e. it is the *data* that tells us someone is risky, not the racist human border agent or bureaucrat). Starting from this position, we can see that logics of structures of power. How are these producers talking about such claims? How are they responding? Are there sector wide or systemic efforts to counter these charges? What do such training programmes look like, and who is enrolled in delivering them (e.g. academics? Activists?) Are there differences between how these sectors are responding? For example, are university responses different from military and commercial ones?

Amoore, Louise (2020) *Cloud Ethics: Algorithms and the Attributes of Ourselves and Others.* Duke University Press.
Amoore, Louise (2013) *The Politics of Possibility: Risk & Security Beyond Probability.* Duke University Press.
Benjamin, Ruha (2019) 'Assessing Risk: Automating Racism', *Science,* 366(6464): 421-22.
Browne, Simone (2015) *Dark* the forthcoming work by Amoore (2020) Primarily *Matters: On the Surveillance of Blackness.* Duke University Press.
Hall, Alexandra (2017) 'Decisions at the data border: Discretion, discernment and security', *Security Dialogue,* 48(6): 488-504

This project will require access to each sector, and this may set the parameters of the project quite early on. It is envisaged that collaboration with computer scientists and engineers in CSIT and EEEC will give the researcher insight not only into how 'unconcious bias' can be inadvertently sutured into algorithms, but also how producers are discussing these charges of 'discrimination by design.' It is hoped that existing industry links with CSIT and EEEC will enable the researcher to build networks into the commercial sector.

Primary Academic Discipline: International Security

PROJECT: Robotics, Autonomous Learning and the Algorithm: Delineating Criminal Responsibility and Legal Liability in the New Machine Age
Lead Supervisor: Dr Paul Miller
Supervisory Team: 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: From Private to Public: The inter-operability and governance of private sector algorithmic solutions in the public sector
Lead Supervisor: Professor John Morison
Supervisory Team: Professor John Morison, Dr Jésus Martinez-del-Rincon
Primary Location: Mitchell Institute

This project looks at how private sector information technology and AI "solutions" from legal practice can translate to the public sector world of administrative justice.

The world of legal practice has long been an area for significant development in terms of bringing in new technology. Software that can scan documents for key words and phrases has already transformed the role of paralegals and legal assistants. There are predictions that lawyers and indeed even judges may soon be replaced, or certainly augmented, by algorithms and other technologies that can undertake functions presently carried out by humans alone. *The In-House Counsel's LegalTech Buyer's Guide* 2018 lists a huge range of products available in what is thought to be a $16 billon market in the USA alone. While motivations to promote AI have to date been largely commercial there is now an increasing pressure in the public sector to develop similar solutions. To date much of this has focused on risk assessment in the context of prison and probation services and in wider policing. But now there are a range of proposals to develop technology across a variety of areas throughout the administrative state in the UK and elsewhere.

This project looks at the development and interoperability of such technology as between the private and public sectors, and explores how values such good governance and human rights compliance as well as general administrative law principles, can be engineered into

such applications. This will involve considering the 'publicness' of such deployments of technology, how these may differ from uses of technology in a private sector context, and whether and how existing models of production designed to serve the private interests of corporations and their owners, with, for example, their opacity in design as required by considerations of commercial confidentiality, can be oriented properly towards a public service ethos which should involve openness and accountability.

In particular, and following on from the context set by the Report of the UN Special Rapporteur on Extreme Poverty and Human Rights (2019) into the digital welfare state, it considers how features such as inadvertent bias, opacity in the way in which evidence is considered, patterns of historical discrimination and political partiality can be managed within systems operating within the public sector. It also considers the role of legal mechanisms from human rights to the GDPR, and how these interact with ideas of dignity, equality and efficiency.

Primary Academic Discipline: Law

PROJECT: Technological Solutions for Fair Unsupervised AI
Lead Supervisor: Dr Deepak Padmanabhan
Supervisory Team: Dr Deepak Padmanabhan, Dr Muiris MacCarthaigh
Primary Location: CSIT

In the digital era, governments and public organizations collect vast amounts of citizen, entity, and system data. These organizations are increasingly considering ways to use AI to inform policy and operational decisions through supervised machine learning and AI, raising important fairness and transparency questions. Yet an increasing amount of this data is unlabelled, necessitating unsupervised learning, particularly when increasingly large amounts of data are collected automatically through devices such as surveillance cameras and smart sensors. The latter trend has been facilitated by an expansion of the methods for 'passive' data collection, where data is collected through safety/surveillance cameras, IoT devices as part of smart city infrastructure, various kinds of sensors, smartphone apps, medical wearables, traffic sensing devices, public wifi and even social media monitoring. The scope of passive data collection has been expanding, fuelled by public-private partnerships such as those with camera manufacturers and urban analytics solution providers. This project will focus on developing a suite of algorithms that embed notions of fairness within their formulation, which will ensure that the results from those algorithms would be fair. Fairness will be quantified as distributional parity along sub-groups of data determined by way of dimensions that are deemed sensitive, such as gender, ethnicity, age, location, employment and education.

The purpose of this PhD project will be:

a) to identify fairness pitfalls while employing algorithmic solutions for processing vast amounts of unlabelled data using conventional exploratory analytics algorithms,
b) to devise algorithmic techniques to embed notions of fairness within exploratory analytics algorithms such as those for clustering, retrieval, representation learning and outlier detection,
c) to benchmark and evaluate the fairness in the results of the analytics algorithms, and evaluate their appropriateness within concrete use cases within the public sector.

The project will primarily involve technology development, but will be informed and

guided by the politics and philosophy of fairness, and more broadly the role of ethics in public service delivery and democratic government. Therefore, as well as demonstrating analytical capacity from a computer science background, the successful candidate will be expected to engage with the social sciences and where possible applications should identify knowledge of theories and concepts relevant to the study of fairness.

Primary Academic Discipline: Computer Science

PROJECT: Parliaments and Artificial Intelligence: Oversight, Regulation and Policy
Lead Supervisor: Dr Muiris MacCarthaigh
Supervisory Team: Dr Muiris MacCarthaigh, Dr Deepak Padmanabhan
Primary Location: Mitchell

Governments across the globe are adopting Artificial Intelligence (AI) and machine-learning technologies to address societal challenges, from disease eradication to agricultural development to social welfare system reform. In 2018 the European Commission published its strategy to foster the development and use of AI in Europe. It is well documented that these new technologies and policy developments present challenges for governments and their administrative systems, such as controlling costs, managing complex IT systems and upholding public service values of fairness and impartiality.

But what roles do and should national parliaments play in these developments and does the challenge of AI require new approaches from those used to address other policy problems that come before parliaments?

The purpose of this PhD project will be:

a) to identify the challenges AI pose for parliaments in respect of their traditional roles of executive oversight, legislative development and financial control
b) to examine the response to date of legislatures across Europe and the European Parliament, to the regulatory and policy challenges presented by AI in government,
c) to identify how best these challenges might be addressed.

The project may also consider the use of AI and machine learning *within* legislatures and how parliaments are using new technologies to perform their functions.

The primary disciplinary location will be political science but the project traverses both social (political) science and computer science and therefore the successful candidate will be expected to engage with both disciplines. Aptitude in computer science will therefore be welcome, but not essential.

The successful candidate will be expected to engage with the Political Studies Association's Specialist Group on Parliaments https://www.psa.ac.uk/specialist-groups/parliaments

Primary Academic Discipline: Politics

PROJECT: When is your smart device my problem?

Lead Supervisor: Dr Sandra Scott-Hayward
Supervisory Team: Dr Sandra Scott-Hayward, Dr Mike Bourne
Primary Location: CSIT

Recent industry reports identify that an unprotected Internet of Things (IoT) device is infected within 3 minutes or less of being connected to the network. To date, millions of IoT devices have been compromised and used in a range of network-based attacks. In addition, research and industry reports have identified how smart home devices can be used to "spy" on people in the home, whether deliberately or through poor design. Network connectivity can enable global access to the IoT devices.

The focus of this PhD is to explore the security and privacy of IoT devices at the intersection of technical design and social constructs.

We specifically ask:

- How can we integrate IoT devices into our home and office networks to adopt the benefits of the smart devices while ensuring that we're not leaking private information from our home/offices?
- How can we manage the use of these devices with visitors to our homes and offices?
- Are technical mechanisms capable of solving these challenges?
- Are regulatory directives effective in addressing these challenges?

The student will have access to a state-of-the-art network testbed in the Centre for Secure Information Technologies (CSIT), Belfast.

Primary Academic Discipline: Network Security

PROJECT: Looking through the hole in your Bitcoin wallet
Lead Supervisor: Dr Teresa Degenhardt
Supervisory Team: Dr Teresa Degenhardt, Dr Sandra Scott-Hayward
Primary Location: Mitchell

Crypto-currencies were initially seen as alternative economic model to support payments without a third party controlling the currency and profiting from it. However, according to the Internet Organised Crime Threat Assessment (IOCTA) 2019 report, Bitcoin is still the currency of choice in criminal markets and as payment for cyber-related extortion attempts, such as from ransomware or a Distributed Denial-of-Service (DDoS) attack. By design, Bitcoin is a pseudonymous coin, meaning that users can transact with the currency without revealing their true identity. To tackle the challenge of Bitcoin-related crime, a range of deanonymization techniques have been proposed. This PhD is a fascinating study of the ways in which these new economies and transactions that are purported to be either 'revolutionary' or 'criminal' are policed through specific technological arrangements.

This PhD involves research on the technology deployed to police bit-coin economy by investigating the ideas behind it and the scientists involved in the process. How are system

devised to detect cybercrime in these forms of transactions. How is a 'good cryptocurrency transaction' detected and separated from a 'bad one' in a context in which complex and novel legal, economic and moral logics are involved? What sort of ideas of risk and security are deployed? Who is leading these developments? What is considered relevant in this complex new economic space?

Sociologically, we are interested in investigating the ways in which this new form of economy is policed according to specific ideas of risk and threats, to proceed to the identification of the user, to ascertain whether or not this is implicated in criminal activities or indeed whether the transaction at play is the result of criminal activities. Relatedly, how are the 'good' from 'bad' transactions sorted? In other words, how are legal, economic and moral lines imagined within these networks, by different private, public, informal and formal actors and institutions?

We specifically ask:

- What techniques are used to suspect transactions and related actors? What are the ways in which the threat is then ascertained or how is a 'red alert' materialised, by whom, and to who is the risk information passed on, if to any formal organization or elsewhere?

How is the reaction to the 'suspicious interaction' and the 'control activity' devised? How are they impacting on the source of the threat, and, further, on the network's ability to perform its economic transaction safely? How is the instance of control encroaching on the economic and political logic of these networks?

What kind of investigation or control is considered morally valid and legitimate? How does that relate to our current understanding of privacy? How does it modify it?

Primary Academic Discipline: Criminology

PROJECT: The Regulation of risk and security in crypto-currency transactions: how is a 'good transaction' detected and separated from a 'bad one' in a context in which complex and novel legal, economic and moral logics are involved?
Lead Supervisor: Dr Teresa Degenhardt
Supervisory Team: Dr Teresa Degenhardt, Dr Sandra Scott-Hayward
Primary Location: Mitchell Institute

This PhD involves research on the sociological aspects of implementing cryptocurrency transaction analysis techniques for the purpose of cybercrime detection.

According to the Internet Organised Crime Threat Assessment (IOCTA) 2017 report, Bitcoin is still the currency of choice in criminal markets and as payment for cyber-related extortion attempts, such as from ransomware or a Distributed Denial-of-Service (DDoS) attack. Bitcoin is a public blockchain; everyone on the network knows about a transaction, and the history of a transaction can be traced back to the point where the bitcoins were produced.

So if bitcoin is traceable, why is it so popular for cybercrime? Although anyone can view the flow of bitcoins between addresses in the blockchain (or between bitcoin wallets), these addresses are just random numbers. In order to be able to identify an individual, it is necessary to trace the address to a real identity. A number of methods for the analysis of bitcoin user identities have already been proposed. Given the technologies available and the potential for accelerated analysis in software-defined networks, the challenge lies in maintaining privacy and anonymity for the general public while bringing the cybercriminal to account.

Sociologically, we are interested in investigating the ways in which the defender in the software-defined world may follow specific ideas of risk and threats to proceed to the identification of the user, to ascertain whether or not this is implicated in criminal activities or indeed whether the transaction at play is the result of criminal activities. Relatedly, how are the 'good' from 'bad' transactions sorted — how are the lines of legality- morality- economic- imagined within these networks, by different private, public, informal and formal actors and institutions?

We specifically ask:

- How is detection of threat and risk within the transaction system identified?
- What sort of knowledge is used as part of the process of detection and suspicion of the threat?
- What techniques are used to suspect transactions and related actors? What are the ways in which the threat is then ascertained or how is a 'red alert' materialised, by whom, and to who is the risk information passed on, if to any formal organization or elsewhere? Is there some sort of censure or stop then activated in the transaction?
- How is the reaction to the 'suspicious interaction' and the 'control activity' devised? How are they impacting on the source of the threat, and, further, on the network's ability to perform its economic transaction safely?
- How is the logic of economic profit-seeking and security articulated within this software and imagined by the scientists enrolled in its production? How are these competing or indeed combining in the process?
- How is the instance of control encroaching on the economic and political logic of these networks?
- What represents order in this world? What sort of economic mobility is considered adequate to perform the service? In what way is that mobility regulated so as to guarantee safety and/or control of the actions of the consumers/actors involved?
- What kind of investigation or control is considered morally valid and legitimate? How does that relate to our current understanding of privacy? How does it modify it?

Primary Academic Discipline: Criminology

PROJECT: Breaking barriers to criminal justice communication; a secure information system approach
Lead Supervisor: Dr Sandra Scott-Hayward
Supervisory Team: Dr Sandra Scott-Hayward, Professor Sakir Sezer, Dr Michelle Butler

Primary Location: CSIT

This PhD will combine research on the technological development of secure distributed information systems with efforts by governments to develop a more effective and efficient criminal justice system.

There has been a growing diversification of providers working with offenders in the criminal justice system. However, contracts are often awarded to providers without information sharing protocols being agreed or established. Each provider tends to have their own secure information system which is not accessible to others or designed to share information. These barriers to information-sharing have hindered efforts to reduce reoffending and improve outcomes, sometimes placing individuals lives at risk as information about risks, needs and suicidal intention are not shared with relevant professionals. Frustrations are also evident among offenders, victims and their families as they must re-tell their stories multiple times with different providers, increasing the likelihood of disenfranchisement, disengagement and their needs not being met in a timely fashion.

This project will seek to pilot the development of a distributed information system which can overcome these barriers to information-sharing, while seeking to ensure data is held and shared securely and in a manner which addresses the privacy concerns of both the individuals involved and the respective providers.

This PhD will consist of 4 key stages:

- Stage 1: Interviews will be conducted with relevant criminal justice stakeholders to identify the main obstacles to effective information-sharing, as well as the cybersecurity, privacy and system design issues involved;
- Stage 2: The findings emerging from stage 1 will be used to inform the development of a new distributed system which will facilitate the sharing of information between providers in a quick, efficient and timely manner, while nonetheless ensuring data is shared securely and respecting privacy concerns;
- Stage 3: The developed system will be piloted with two different providers. Interviews conducted to obtain their feedback regarding the usability and appropriateness of this system, as well as its ability to enhance efforts to reduce re-offending and improve criminal justice outcomes.
- Stage 4: Based on the feedback from stage 3, the system will be amended to address any issues that may emerge during stage 3.

It is proposed to draw on Dr Butler's existing links with criminal justice agencies to recruit participants to take part in the proposed interviews, as well as recruit two different providers working within the criminal justice sector to pilot the proposed software.

Primary Academic Discipline: Network Security

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
Supervisory Team: 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)

PROJECT: Emerging Cyber Bordering Technologies
Lead Supervisor: Professor Sakir Sezer
Supervisory Team: Professor Sakir Sezer, Professor Cathal McCall
Primary Location: CSIT

Securing cyberspace borders is a rapidly evolving and crucial area of interest for governments, private sector interests, and individual citizens. 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, governments are also deeply implicated in 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 cyberspace borders of competitors in the name of innovation.

Firewalls, network-based application and user detection technologies and URL black and white lists present essential technological tools for building borders in cyberspace and preventing cross-border access to web-content. For example, large scale filtering of URLs in China restricts the access of its citizens to many US and European websites. On the other hand, service providers of streamed content (e.g. live football matches, movies, shows etc.) restrict international cross-border access due to broadcast restrictions of licensed content. For example, except BBC News, all Internet-based access to UK TV programmes are restricted by a firewall, ensuring that access is permitted to users within UK jurisdictions only. 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. The majority of these services are used for accessing terrorist or organised-crime related, copyright protected or illegal (offensive, abusive, sexual) content, stored or hosted in states with limited data protection and copyright laws.

The aim of this project is to explore various security, firewall and access control technologies that can be effectively used for policing and enforcing of cyber border policies. Many IT security technologies are developed for the Enterprise market and impose privacy and ethical concerns when they are used for bordering public cyber space. Scalability and global

deployment pose technological challenges and potential misuse of intercepted and/or logged information as part of the policing process.

Project Objectives:

- Investigate and evaluate various security technologies that are suitable for cyber bordering and cyber border enforcements.
- In collaboration with AHSS, derive feature specification for cyber bordering technology for national cyber space and national cyber border protection.
- Explore technologies for policing encrypted VPN tunnels without violating user privacy or exposing intellectual property or trade secrets.
- Develop traffic analytics algorithms for cyber border policy enforcement.
- Prototype and validate traffic analytics algorithms and assess their suitability for cyber bordering.

Assess the proposed analytics algorithms and developed bordering technology in terms of potential misuse for user privacy violation and ethical concerns.

Primary Academic Discipline: Computer Science (Social Science)

PROJECT: Cyberborder Development, Defence and Penetration: Technological and Governmental Aspects
Lead Supervisor: Professor Cathal McCall
Supervisory Team: , Professor Cathal McCall, Professor Sakir Sezer, Professor Hastings Donnan
Primary Location: Mitchell Institute

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.

The PhD will include a 3 month research internship with GCHQ or I-BOC.

Primary Academic Discipline: Border Studies

---

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

PROJECT: A Technology of Policing Delivery
Lead Supervisor: Dr John Topping
Supervisory Team: Dr John Topping; Dr Deepak Padmanabhan
Primary Location: Mitchell Institute

A multitude of data and information is gathered, analysed and deployed within policing organisations in order to plan, predict and operationalise police resources – both strategically, and operationally on the front line of policing.

Yet beyond individual technologies (whether equipment or software) situated within the police 'front' and 'back office', a number of questions arise. Particularly, how 'joined up' are the various technologies and data which underpin police decision-making and practice? How well do different systems of data communicate with each other? And how useful is the total amount of data collected by police organisations for officers on the ground?

Similarly, much police analysis of data remains a retrospective process – based on patterns and events which have already occurred. In this regard, what technological options exist with regard to generating better 'real-time' data for use by police. And on a related point, what is 'useful' data for police officers on the frontline of policing; and how does that compare with the data they currently use?

It may be seen that much policing technology tends to be path dependent in terms of its use and deployment. New technologies are adopted which in turn become self-reinforcing – strategies are created around the technology; officers are trained in its use; results and outputs around are based around the technology; and changes or reversion to previous technologies or approaches become increasingly difficult or costly. In this regard, a much deeper examination of policing technologies (as broadly conceived) is key to understanding the balance between tech-enabled policing and tech-led policing.

The proposed PhD will be situated within the Mitchell Institute, with a potential criminological focus. However, other disciplinary perspectives will be considered.

It is anticipated that collaboration with a police service will be required in order to undertake the core research for the PhD.

Primary Academic Discipline: Criminology

PROJECT: Enhancing Human Rights and Ethical Applications of the Law: Stop & Search
Lead Supervisor: Dr John Topping
Supervisory Team: Dr John Topping, Dr Deepak Padmanabhan
Primary Location: Mitchell Institute

This PhD proposal seeks to combine the latest technological advance in point-of-contact data capture between police officers and the public in the application of stop and search powers.

The use of stop and search powers across the U.K. have attracted voluminous attention over the past 40 years. Yet focus on use of the powers generally, and specifically 'everyday' powers of stop and search have, until recently, remained marked by their lack of academic or policy attention.

The most recent research indicates PSNI are using stop and search at much higher rates than all other UK police forces (Topping & Bradford, 2018; Topping & Schbotz, 2018). But beyond the general application of the power, this emerging body of research also points to the power as a disciplinary tool, demarcating the boundaries between, and flagging up, young, urban, socio-economic deprived males for special attention relative to the rest of the population. In essence, virtual geographic and socio-economic boundaries exist to influence the use of stop and search above and beyond any crime considerations.

At present, public data around PSNI stop and search remains limited; while organisational recording practices and internal management of stop and search remains siloed, and contributes to little meaning understanding of how it is repetitively concentrated on certain populations and within certain geographic areas.

Drawing on the lessons from existing consultancy work with PSNI by Topping; and those derived from recent technological reform around stop and search by Police Scotland, this PhD will attempt to combine a range of ethical, human rights and accountability frameworks into user-friendly technology for both point of contact and subsequent monitoring / analysis related to use of the power. It is anticipated that once developed, such a system could be modified to include dynamics and variables unique to particular policing jurisdications.

This PhD will have 3 key stages:

1. Exploring the stop and search landscape in Northern Ireland / PSNI;
2. Examining existing police technologies around recording of stop and search from other jurisdictions;
3. Develop a computer system (including mobile app for police) which actively monitors

and flags up stop and search practice, which in turn will provide new data attuned to existing human rights and accountability frameworks unique to NI

In view of Topping's existing work with the PSNI / NIPB, and current consultancy work with PSNI, significant organisational interest from both organisations in terms of 'buy in' could be expected.

Topping is also involved in an EU COST network grant on stop and search across Europe, providing further opportunities for international interest and contacts for the prospective PhD student

Primary Academic Discipline: Criminology

PROJECT: The Vigilant Image: Documentary Technologies in the Age of Global (In)Security
Lead Supervisor: Dr Des O'Rawe
Supervisory Team: Dr Des O'Rawe, Dr Niall McLaughlin, Professor Cathal McCall
Primary Location: Mitchell Institute

The discourse of catastrophe has become particularly influential in contemporary global societies. In addition to environmental disasters and the spectre of economic collapse, there is now the emergence of complex, mutable, unpredictable forms of terrorism, forms that have in recent times become more effective in *terrorizing* by being simultaneously here and elsewhere, familiar and alien. The socio-psychological consequences of 'new terrorism' are significant in relation to how communities and citizens – especially, in the major global cities – are becoming habituated to a culture of normalised trauma and excessive vigilance. The role of contemporary liberal democracies – equipped with increasingly sophisticated surveillance and security technologies – and the mass media, remains similarly problematic in this context. Guy Debord's adage that 'the story of terrorism is written by the state' is still relevant to any understanding how responses to (and representations of) contemporary forms of political violence and the 'terrorist threat' undermine democratic power-relations and affect the sociology of everyday life in the West.

This PhD project explores how new and emergent documentary technologies contribute to cultures of excessive vigilance, and their influence on political and social behaviour in modern democracies. New digital technologies have transformed traditional modes and ontologies of documentary practice, with filmmakers increasingly experimenting with animated, VR/AR, 360, and interactive multimedia platforms. These developments have the capacity to both shape and critique perceptions of reality, especially within the political sphere where states and corporate interests compete with creative practitioners and activists to control the content and dissemination of these technologies. What is the role of these technologies in negotiating between modes of vigilance and technologies of surveillance? How might new documentary technologies be employed to critique the over-vigilant society, disrupting the legitimizing processes integral to 'states of exception', with its and direct and indirect forms of repressive legislation, censorship and regulation, and more generalised suspicion of the 'other'?

A PhD in this area would pivot the participation of the Mitchell Institute and CSIT in the £13m Future Screens NI, the collaboration between Queen's, Ulster University and local industry partners for creative industries in Northern Ireland. Future Screens NI aims to provide opportunity and growth across film and broadcast, animation, games and emerging technologies and industries. This PhD proposal speaks directly to its film and emerging technologies foci.

Primary Academic Discipline: Film Studies

HOW TO APPLY

The deadline for applications is 4:00pm, Tuesday 14 January 2020.

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 **LINCS20** 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 **LINCS20** 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 **400 - 800** 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 - 800 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 LINCS20 in the free text box may result in your application not being allocated or considered for funding.**

The deadline for applications is 4:00pm, Tuesday 14 January 2020

[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	**Dr Philip O'Kane** p.okane@qub.ac.uk
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 Cathal McCall** c.mccall@qub.ac.uk
Supervisory Teams Coordinators (Theme)	Cybersecurity: Technology and Ethics **Prof Sakir Sezer** s.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