JILL DANDO INSTITUTE OF SECURITY AND CRIME SCIENCE
DAWES CENTRE FOR FUTURE CRIME AT UCL

UCL

DAWES CENTRE FOR FUTURE CRIME AT UCL

ANNUAL REPORT

1 MARCH 2019 – 29 FEBRUARY 2020

Contents

Foreword

This report provides a summary of the activity of the Dawes Centre for Future Crime at UCL (henceforth referred to as the Centre) for the period 1 March 2019 to 29 February 2020. It seeks to provide a concise account of current projects of the Centre, and activities emanating from and around those projects including external engagement, dissemination, publications, and impact.

The reporting period represents the third full year of activity of the centre. In this period, we have continued to build on the momentum already generated, and, as strategic priorities, have continued to build capacity in the areas of data science and cyber crime. Particularly notable was the launch of the new £5.4M EPSRC-funded Centre for Doctoral Training in Cybersecurity at UCL, which is a collaboration with the departments of Computer Science and Science, Technology, Engineering and Public Policy. New scoping studies have come on stream, with 'sandpit' workshops bringing together academics and stakeholders to examine future crime topics and how we might address them. An example for this reporting period, was a sandpit on cryptcurrencies and how they can and may enable new types of fraud that was attended by stakeholders from around the globe.

Our engagement with academics, practitioners, and other stakeholders continues to grow with our 2019 annual conference being run in partnership with the police-led Society of Evidence Based Policing at the prestigious Royal Society in London. Our activities have created forums for significant knowledge exchange between practitioners and academics, and more formal outputs are beginning to emerge from the Centre's research. Our work on the Internet of Things has, and continues to, inform policy in the UK and overseas and we will seek to generate similar impacts through other projects that are now starting to come to fruition. Despite finding ourselves in lockdown since March 2020, we continue to engage in thought-provoking discussions with researchers and stakeholders, and are exploring how lessons learned from the COVID19 situation can inform our understanding of future crime and opportunities to reduce it. We plan to launch some exciting new initiatives in the coming year, and look forward to working with all of our partners to realise the real-world impact of our work.

Professor Shane Johnson
Director

Background to the Centre

In a very real sense ‘crimes of the future’ are an emergent property of the advance of civilisation. It is not a question of if new criminal opportunities will be exploited, but when and how. The Dawes Centre for Future Crime at UCL was established to address these questions directly. To do this, the broad aims of the Centre are to look more systematically to the future to try to anticipate problems before they emerge or escalate and to advance solutions for tackling them effectively before they become established. As such, it seeks to:

- develop a global presence to fund and generate cutting-edge, application-focused research designed to meet the challenges of the changing nature of crime, and
- reduce fragmented activity by bringing together experts across scientific domains and stakeholders to identify, understand and propose solutions to problems identified

Key activities

Activities key to achieving the Centre’s mission include:

- horizon scanning for new and emerging crime problems, or solutions to combat crime
- engaging with our stakeholders to identify research need and to deliver research with real-world impact
- attracting external funding to multiply the Dawes Trust investment and to create partnerships with other research centres
- training the next generation of scientists – through our PhD programme and taught courses – to understand the crime implications of technological and social change, and
- communicating our research findings to raise the profile and agenda of the Centre, and to disseminate our findings to our network of stakeholders.

Governance of the centre

The Centre is governed through three principal mechanisms

The Executive Committee (EC)

The EC comprises eight permanent members, constituted of representatives from:

The Dawes Trust

Sir Stephen Lander
John Graham
Stephen Webb

Independent Advisors

Dr Helen Atkins
Defence Science and Technology Lab

Simon Ruda
Behavioural Insights Team

UCL

Professor Richard Wortley
Head of UCL Security and Crime Science and Committee Chair

Professor Nigel Titchener-Hooker
Dean of the Faculty of Engineering Sciences

Professor Shane Johnson
Director of the Dawes Centre for Future Crime at UCL

The Advisory Board (AB)

The AB comprises the following members:

Simon Parr QPM
Ex-Chief Constable Cambridge Police

Chris Rampton
Chief Technical Officer Centre for Applied Science and Technology (CAST).

Prof Dave Delpy
Chair of the UK Quantum Technology Strategic Advisory Board, former Chair of the Defence Scientific Advisory Council (DSAC) and former CEO of the Engineering and Physical Sciences Research Council.

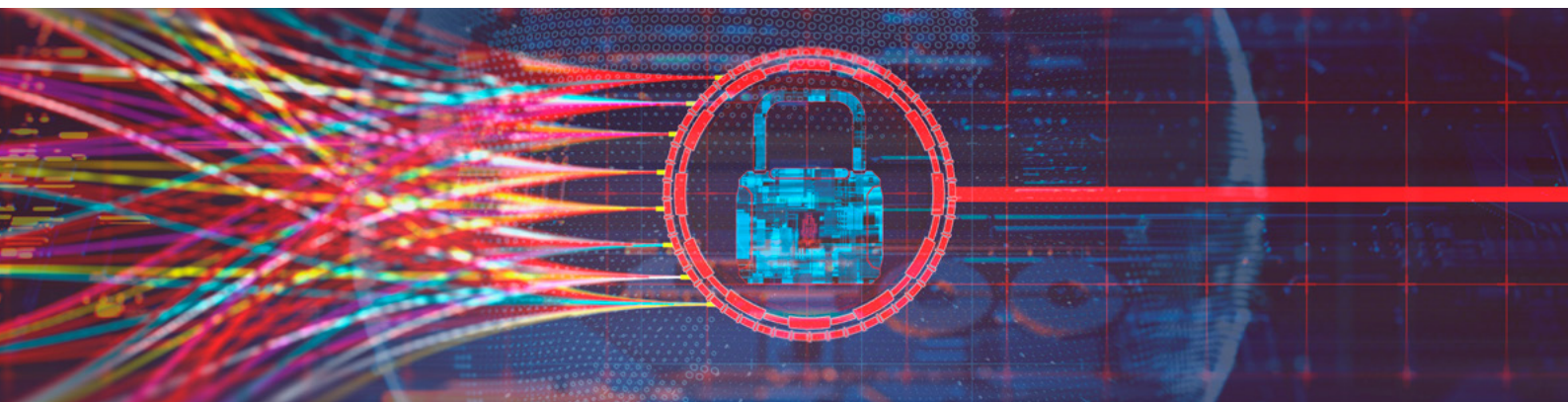
Dr Emma Barrett
University of Manchester, Professor of Psychology, Security and Trust and strategic lead for Digital Trust and Security. Formerly a senior UK Government behavioural science adviser for national security. Associate of the Centre for Research and Evidence on Security Threats (CREST) at the University of Lancaster.

Dr Deeph Chana
Institute for Security Science & Technology, Imperial University. Previously a senior UK government science policy adviser on critical infrastructure security in Whitehall

Dan Greaves
Crime Director, UK Home Office

The Centre Management Team

This team comprises Professor Shane Johnson (Director), Dr Bennett Kleinberg (Lecturer), Dr Manja Nikolovska (Researcher), Mr Vaseem Khan (Project Manager), and the Centre Administrator.



Summary of activities in the reporting period

Over the past year we have completed or begun a number of initiatives.

Research activities include:

1 Completed projects

five projects were completed during this period.
See below for details.

2 Current projects

five new projects are underway covering topics ranging from smart technology and domestic violence to looking at cybercrime aimed at the older generation.

3 PhD projects

this year, we recruited eight new PhD students, ranging from terrorist money laundering to cryptoasset fraud to cyberbullying.

Further details of all of the above are provided in the Research Highlights section below.

The year also saw us organise the **third** of a series of **future crime conferences**. Held at the Royal Society in London, the theme of the conference was the future of policing. Please see our Annual Conference section.

We also continued to build on our taught modules, including an undergraduate module (now in its third year) on Security Technologies, a module on Horizon Scanning (now in its second year), and a new module in applied data science. We summarise these modules in our Teaching section.

Research highlights

The aim of research conducted through the Dawes Centre for Future Crime is to anticipate how technological, social or environmental change might create new opportunities for offending, or have implications for how law enforcement (and others) combat crime. In the case of new crime opportunities, the Centre aims to propose methods for addressing potential threats before crimes emerge or become established. Research focuses on a mixture of new crimes about which little is known, and crimes that are likely to emerge in the near future, or medium- to long-term time horizons.

Projects generally comprise two phases:

PHASE 1

The aim of **Phase 1** projects is to review what is known about a particular technological, social or environmental issue. They will establish the state of the art on a particular topic and the implications for (future) crime. Phase 1 projects usually involve scoping activities to enable us to better understand potential opportunities and threats and include 'sandpit' workshops to bring together academics, practitioners and others to discuss a particular problem and what might be done about it.

PHASE 2

The aim of **Phase 2** projects is to complete original research intended to address a specific future crime problem, or to develop existing research to reach a technology readiness level suitable for deployment. We are also funding *feasibility studies* to explore the crime reduction potential of new or developing technologies.

Sandpits

The aim of the sandpits is to bring together an invited group of academics and stakeholders to participate in structured brainstorming sessions in a “neutral” environment. The ultimate aim of the sessions is to generate suggestions for further research, and to select those that have the greatest potential to realise real-world impact. Identified ideas are then considered by the Dawes team and those deemed worthy of being funded are put forward to the Dawes Executive Committee to consider for approval. The sandpits follow different formats, but as a minimum, include a presentation to set the scene about the technology or issue to be discussed, followed by group work intended to tease out answers to key questions, including the following:

- How important is a specific aspect of the topic (e.g. a specific crime threat) in terms of reach and severity?
- Which issues are the most pressing or predicted to grow?
- Which issues are most relevant to the practitioner community? And for which dimensions of a topic can we identify a stakeholder (or stakeholders) that can provide or facilitate pathways to real-world impact?
- What would a project to tackle these topics look like and how much might it cost?
- What (if any) are the ethical issues associated with the proposed research?

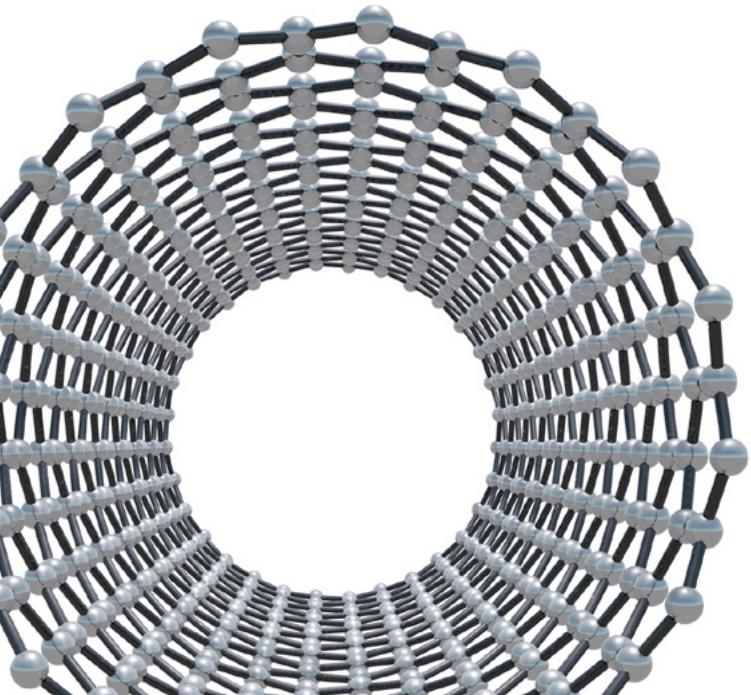
1 Research highlights: Completed projects

Advanced materials to combat crime

Work on advanced materials includes the discovery of new materials with novel properties, as well as the modification of existing ones to alter structural and/or functional properties in order to obtain superior performance for specific applications. Such materials include metal and alloys, ceramics, glass, semiconductors, polymers, composites, nanostructured materials, graphene and hybrid materials. The field of advanced materials is multidisciplinary involving materials science, chemistry, physics, biology, mathematics, engineering and nanotechnology.

Nanomaterials are produced at the nanometre (nm) scale – a human hair is 90,000nm

This project considered the potential of various advanced material technologies to combat crime. The research has involved exploring what applications are desirable, over what timescales their production is plausible, and what is required to make the exploitation of advanced materials for combatting crime feasible. This involved the identification of current approaches used by law enforcement, and the discussion of these with relevant stakeholders and industrial partners to identify user-need, potential developments and the likely timescales and costs required for production. Initial discussions included a teleconference with officers from six UK police forces (Durham, Cleveland, Leicestershire, Metropolitan, South Yorkshire, and Surrey), and a visit to the Home Office Centre for Applied Science and Technology (CAST). These discussions informed a review of the literature and a sandpit event which took place between 12–13 April 2018. Sixteen representatives from academia, British Transport Police (BTP), the Home Office, and from Durham, Hampshire, and West Midlands constabularies took part. Following the same format as the counterfeiting goods project, following presentations on advanced materials, participants worked in groups to generate a long list of problems and projects on day 1, from which a subset of seven were selected for more detailed discussion on day 2. The sandpit event served not only to identify potential research areas and application of materials science in crime prevention, but also enhanced the engagement of materials scientists and engineers with police forces and crime prevention units. The sandpit was followed by a visit to Ridgepoint house in the West Midlands to discuss the possible uses of advanced materials in the context of forensic science. A final report for this project, and a phase 2 proposal, has been drafted and will be submitted to the executive committee shortly.



This project has allowed the UCL Institute for Materials Discovery to establish a new research direction and this will continue with a PhD project working on biosensors to combat crime. In addition, we have been building capacity for the scientists of tomorrow by involving an MSc student in a research project on ***Advanced Materials to Combat Crime: Novel Finger-mark Detection*** in 2020/21.

Lead Investigator
Prof Kwang-Leong Choy

Crime, place and the Internet

Data from the Crime Survey of England and Wales clearly show that cybercrime is a substantial problem for the public, accounting for about 50% of all crime. Offences range in size, from everyday incidents to the spectacular, and in nature, from malicious attacks to those motivated by financial gain. As more and more services go online, the problem is likely to increase, in both the volume and range of crimes committed. Cybercrime differs from traditional urban crime in a number of important ways: for example, it is asymmetric, in the sense that a single offender can commit many offences, often with relative ease. Nevertheless, there are several aspects of criminal behaviour which are common to both, particularly in relation to the awareness and evaluation of targets. The aim of this project was to examine whether lessons learned in relation to urban crime can be applied or adapted to online environments.

The primary aim of the work was to develop a general framework for the analysis of crime occurring in non-geographic spaces. The range of such crimes (and indeed spaces) is very broad, with each likely to pose particular challenges and require bespoke treatment. Since it would be infeasible to consider all of these, the aim of this research was to identify general principles and to demonstrate how they can be applied in several illustrative cases identified in discussion with law enforcement and industry. These would act as proofs-of-concept for the overall approach and motivate its application to a more extensive range of issues.

A sandpit was held between 17–18 January 2019 and was attended by 20 representatives from four universities, the British Retail Consortium, the Defence, Science and Technology Labs (DSTL), the Home Office, the Metropolitan Police, the National Cyber Security Centre (NCSC), West Midlands Police, and Symantec. Participants worked in groups to generate a long list of problems and projects on day 1, from which four were selected for development on day 2.

Following the sandpit event, the project team drafted a Final Report for the project, which was presented to the Dawes Executive Committee later in 2019. This report contained a review of the literature, as well as a number of potential topics for Phase 2 studies: ‘mapping’ disinformation, a ‘digital breathalyser’ based on profiling routine activities online, and the disruption of criminal business models via spoofing of criminal behaviour. After discussion with the committee, the latter was identified as a candidate to be taken forward as a potential Phase 2 project, and this is currently being developed. Alongside this, an expanded version of the Final Report was written up as a review paper; this has been published as a pre-print and is currently under review. Additionally, a PhD student is working on research related to this project.

Lead investigators
Dr Toby Davies
Dr Gianlucca Stringhini

Future crime opportunities arising from Artificial Intelligence (AI)

Long-awaited, AI has arrived, delivered by advances in: machine learning to build algorithms from data; deep learning to do it like the brain; and computers to do it fast and cheap. While beneficial to society, AI also has the potential for criminal application, including:

Identity Forgery

AI methods can generate speech in a target's voice given a sample and couple it with synthesized video of them speaking. A senior citizen could be tricked into making financial transfers over video skype by an apparent trusted party.

AI Snooping

Phones, PCs, TVs and home hubs provide the sensors for audio snooping inside homes. Speech Recognition can sift the resulting data for exploitable fragments (e.g. passwords or bank details, affairs being admitted to).

Driverless Weapons

The driverless truck is close to the ideal urban attack robot for terrorists. GPS guidance could bring it to target, and Machine Vision could target pedestrians.

On the flip side, AI has potential for crime prevention. Most developed is machine perception in, for example, vehicle tracking, person recognition, and X-ray threat detection. However, all deep learnt vision systems so far studied are capable of being fooled by an adversary who has prior access to the software. This is achieved, not by hacking it, but by using AI methods to find its hidden weaknesses – minute adversarial perturbations of the input to the system that tip it into giving the wrong output. Understanding whether a particular security-critical system is vulnerable, and addressing the weakness by, for example, ensuring the software is not physically present in purchasable security scanners (but instead runs from a remote server which is not accessible by an adversary) can guard against a lurking problem.

This project examined the future crime potential of AI, and provided a basic taxonomy graded on scales of criminal profit, public harm, victim harm, effort, difficulty, and technology readiness.

A sandpit event took place between 14–15 February 2019 and was attended by 32 delegates from UK universities, Barclays Financial Crime unit, the NCSC, the NCA, DSTL, iProov (a biometric company), Synerize (an AI company), the BRC, the College of Policing, West Midlands police and the Home Office. This sandpit mixed group work with brief presentations on (future) threat scenarios (identified through a review of the literature) involving AI. In groups, participants were asked to discuss and rate each of the scenarios along four different dimensions concerned with the harm they could pose, the ease with which they could be achieved, the ease with which they could be detected, and the profit that could derived by criminals. These ratings have been analysed to rank the scenarios according to whether at present they should be ignored, require watching or likely require action now.

A final report for this project was submitted and a short video created in which Professor Griffin describes the key AI harms that emerged from the research. (The video is available on the Centre website.) This work will also feature in the first practitioner briefing that is being prepared jointly with UCL's public policy unit based in STEaPP and will be accompanied by a press release and the release of an academic publication. Two PhD students are working on projects that evolved from this project.

Lead investigator
Dr Lewis Griffin

Developing a consumer security index for domestic IOT devices (CSI)

Internet enabled devices, including smart televisions, security cameras and thermostats, are now commonly found around the home. Devices such as these have enormous potential to transform society, but they also provide opportunities for crime. For example, some devices (including 'security' cameras) lack basic password functionality or allow the use of default passwords that can easily be guessed or even found on forums. Such vulnerabilities have been exploited to conduct distributed denial of service (DDoS) attacks, which are used to overwhelm a website or online service, making it inoperable. Such attacks have been documented in the media several times. However, the types of crime that can be committed using vulnerable Internet-enabled devices is not limited to this type of activity. They can be targeted to steal personal information, including credit card details, or exploited by perpetrators of domestic abuse to (for example) gaslight their victims.

While security should be designed into devices, there is little incentive for manufacturers to do so consistently. Moreover, while consumers can easily find out the fat content of (for example) food products, or the energy efficiency of electronic devices, by looking at the labels on the front of the packets, at the point of purchase, consumers are not provided with simple information to help them assess the security of devices. The aim of this project was to better understand the potential crime threats associated with consumer IoT devices, understand what is communicated to consumers about security at the point of purchase, and examine the potential effectiveness of consumer labelsin incentivising manufacturers to improve IoT device security, and to help consumers purchase more secure devices.

The work included:

- A systematic review of the academic literature to map out the types of crime the consumer IoT has or may make possible.
- A review of 270 device manuals and online materials to analyse the security and 'cyber hygiene' advice they provide.

- A review of the effects of other types of labelling schemes on consumer decision making.
- Workshops with industry, retail, academics and policy makers on the form a label might take, how it might be accredited and the facilitators and barriers to adoption.
- A study of what consumers would be willing to pay for better security in domestic IoT products
- A large experiment of the effects of different labelling schemes on consumer choice, their willingness to pay for enhanced security, and how they interpret labels

By working with DCMS, this research has and continues to inform policy. Our work is discussed in detail in DCMS reports published in 2018 and 2019 to motivate the need for government intervention and the potential benefits of consumer labelling schemes. It is also heavily cited in a recent report by the Internet Society and Canadian Government on policy options for securing the Internet of Things (***https://iotsecurity2018.ca/wp-content/uploads/2019/02/Enhancing-IoT-Security-Draft-Outcomes-Report.pdf***), and discussed in a Parliamentary Office for Science and Technology briefing.

Lead investigators
Professor Shane Johnson
Dr John Blythe

*This project was co-funded by PETRAS, the Internet of Things hub.

Cryptocurrency fraud as a future challenge for large-scale financial crime

Cryptocurrencies are a form of non-fiat "digital money" that have become increasingly popular in recent years. They are a form of decentralised currency that facilitate secure and anonymous transactions between individuals. There exist many cryptocurrencies, with the most widely known being Bitcoin. Despite the vast amounts of money being invested and traded in cryptocurrencies, they are uncharted territory and are for a large part unregulated. That lack of regulation, combined with their technical complexity and market volatility, makes them an attractive target for fraudulent activity.

One example of cryptocurrency fraud is a so-called pump-and-dump scheme. In a pump-and-dump operation a nefarious actor first accumulates a commodity over time for a relatively low price. In the second step (pumping), the price is artificially inflated through coordinated group trading activity, targeted misinformation, or a combination of both. The demand created through fake information and hype drives the price and allows nefarious actors to sell off their previously accumulated commodities at a higher price (dumping), generating substantial proceeds.

This project aimed to shed light on this emerging yet currently under-researched and non-regulated problem space by:

1) Gaining a comprehensive overview of the problem of cryptocurrency fraud and its sub-types, as well as existing efforts to address this emerging problem
2) Identifying the key strategies and Modus Operandi used to defraud in the cryptocurrency market
3) Identifying the pressing research questions to develop appropriate mitigation, prevention and/or detection methods.

This project was completed and a final report submitted. Outputs related to the project were presented at The First Annual Conference on Crime, Risk and Economics (London), The annual conference of fraud investigation of the Netherlands (The Hague), The Policing 2.0 conference (London), and in a special session at the Institute for Financial Crime (The Hague).

The project has also led to the recruitment of two PhD students, one funded by the Centre and one by the affiliated Centre of Doctoral Training in Cybercrime at UCL. Both projects address the issue of future financial crime through cryptocurrencies; one of them from a computational perspective, the other from a legal and cybercrime perspective.

Lead investigator
Dr Bennett Kleinberg

Research assistants
Florian Hetzel
Eray Arkatuna (PhD researcher)

2 Research highlights: Current projects

Realist review to develop a model of vulnerabilities to cybercrime in the UK's older population

The proportion of populations across the world who are older (aged 60 years or above) is growing. Older people are also the fastest growing demographic group of novice internet users, commonly using it to access banking, shopping and healthcare management services and for social media and other communication. Historically, older people have been a prime target for fraud because of factors including their relative wealth, loneliness, memory loss, being from a generation characterised by high levels of trust and hesitancy to report the crime to authorities. A move to close down physical bank branches, encouraging their customers to conduct commercial transactions online, may also heighten this vulnerability. Without appropriate safeguards and support to navigate (or circumvent) this new terrain safely however, global digitalisation could lead to an epidemic of cybercrime victimisation.

A 2015 Populus survey of 1200 adults in Enland, Scotland and Wales for Age UK found that over half (53 per cent) of people aged 65+ believe they have been targeted by fraudsters.

conduct commercial transactions have a generic design and it is possible that these designs are not supporting older people to negotiate them securely. For example, memory loss has implications for use of passwords and memorable information, and older people may face challenges complying with the technical specifications on secure behaviour. From the criminal's perspective, cybercrime against older people is a low risk crime.

This project will carry out a scoping review aimed at informing stakeholders planning future intervention approaches to increase cyber security for vulnerable older adults. Stakeholders need to know what interventions work, for whom, and in what context.

Lead investigators
Dr Kartikeya Tripathi
Professor Claudia Cooper

Research Associate
Alexandra Burton

Onsite counterfeit detection system for agrochemicals

This project follows on from an earlier Dawes Centre funded scoping study on current and future trends in the counterfeiting of chemical products. Counterfeiters have become increasingly proficient at producing authentic-looking products and/or packaging, honing their methods to the point where their products pass visual inspection – the first line of defence. Thus, there is a growing requirement for fast analytical methods to test the chemical composition of the contents of such products where traditional product protection methods or track-and-trace do not exist or are ineffective.

The threat of counterfeit agrochemicals such as counterfeit pesticides is a neglected area with potential widespread negative impacts in terms of public health and environmental contamination as well as economic losses. (Eg. estimates made in recent years suggest that illegal pesticides comprise 10% of the EU market for pesticides.) Unlike medicines where there is a very carefully controlled supply chain agrochemicals offer many opportunities for criminal activity throughout the supply chain. Hence, on-site testing might be the best opportunity to ensure fake agrochemicals are not used.

The aim of this project is to carry out a laboratory-based investigation into suitable technologies that could fit into a miniaturised system to identify counterfeit agrochemicals. Such technologies do not exist. Technologies that could be applied at the point of distribution or application would be targeted and concepts for end-user devices investigated.

Both optical and ionising radiation might be used as suitable probes for developing test procedures that could be deployed prior to dilution of pesticides in the sprayer tanks on tractors or railway vehicles. Both techniques would form part of this project – optical techniques have the advantage of not requiring protection from ionising radiation but the X-ray based techniques might provide more detailed information about the agrochemical components. Miniature X-ray sources using the pyroelectric effect are available that have been used for X-ray fluorescence; others have been developed using carbon nanotube cathodes. There are also many options for small laser sources. With a compact source of suitable radiation, several analysis techniques could be considered. It is not intended to carry out a full chemical breakdown of the materials but rather to provide a rapid, green light-red light decision on whether or not the 'fingerprint' offered by the material under test matches that of a previously obtained reference sample already stored in a database (some data already exists but this would be extended as part of this project).

To date, a list of candidate agrochemicals that are typical targets for exploitation has been established. This list has been compiled in consultation with experts at Harper Adams University. Commercially available examples will be purchased and a test set created by altering the chemical composition in a way that mimics criminal methods (e.g. by dilution with water). A series of different technologies have been identified that will be investigated. Some of these are standard analytical laboratory instruments which will provide the 'gold standard', while others are research-based instruments, but have the genuine possibility of being miniaturised. To facilitate this assessment, a test matrix has been developed, with colleagues in Statistical Sciences, which describe the size of the test set and the number of repeats required to determine which system (or combination of systems) provides the best specificity for substandard agrochemical identification.

Lead investigators
Dr Rob Moss,
Dept of Medical Physics & Biomedical Engineering
Prof Rob Speller
Dept of Medical Physics & Biomedical Engineering

Research assistant
Dr J.C. Khong
Dept of Medical Physics & Biomedical Engineering

Developing a prototype computational modelling platform of crime-related demand and police supply dynamics

Limited policing resource is a current and future reality. A key priority for applied policing is to better understand, anticipate and forecast the impact of changes to short-, medium- and long-term demand. Some priority areas for which demand needs to be better understood (and met) include online crime, high harm crimes against the most vulnerable, and serious and organised crime. At the same time, demand is also poorly understood for volume crimes, which are – after a period of reduction – on the rise again. Models of both police demand and supply – i.e. the configuration of resources utilised in an attempt to meet demand – are required to support police decision-making in ways that minimise threat, risk and harm to communities. Yet, understanding police supply and demand dynamics is a non-trivial task. An array of factors, both internal and external to police, influence the nature and occurrence of demand and the subsequent impacts on supply that responding to those demands creates. These factors are highly interdependent and thus difficult to model using traditional analytical techniques. This project explores how advanced simulation techniques might help understand the interactions between police demand and its impacts on resourcing. The research will develop a prototype modelling platform to explore these dynamics, developing techniques for simulating crime related demand, and subsequent police responses. Models will be tested as a tool for modelling different demand scenarios, with a long-term aim of creating tools that can support police demand-related decision making.

Lead investigators
Dr Dan Birks,
University of Leeds

Prof Kate Bowers,
UCL

Prof Shane Johnson,
UCL Dawes Centre for Future Crime

Prof Alison Heppenstall,
University of Leeds

Prof Ken Pease,
University of Derby

UCL Researcher
Ms Eon Kim, UCL

Note: This project is being led by the University of Leeds and is funded by the Alan Turing Institute

Smart tagging and proximity detection for crime reduction

The electronic tagging of criminals to track their movement is already used with the aim of preventing crime. For example, electronic tags that use GPS monitoring are employed to ensure that offenders comply with Home Detention Curfews. However, GPS technology has limitations as it operates mainly in outdoor environments, which means that GPS signals can be lost in indoor environments, such as shopping malls or hospitals. This project is examining how sensing technologies, such as Bluetooth, can be used for such applications and for crime prevention in general.

Lead investigator
Dr Eiman Kanjo
Nottingham Trent University

Research assistant
Dario Ortega Anderez
Nottingham Trent University

Textwash

In this project, UCL researchers are developing software that removes personally identifying and sensitive information from text data. While many stakeholders (e.g. the police, health care providers, tech companies) are keen to share text data with researchers – for example, to evaluate or build information extraction approaches – a key impediment to date is the sensitive nature of the data. Individuals have the right to privacy, so text data would need to be anonymized before it can be shared. To do this automatically while retaining the usefulness for secondary computational analyses, Textwash was developed. The outcome of this project will be the first empirically-validated and transparent anonymization software that puts all control in the hand of the users. The prototype will be launched this summer, and the product will be available by late 2020. Textwash is supported by a proof-of-concept grant from SAGE.

Lead investigators
Dr Bennett Kleinberg
Dr Toby Davies
Maximilian Mozes

Information about completed projects described in previous annual reports can now be found on our website:
www.ucl.ac.uk/jill-dando-institute/research/dawes-centre-future-crime

These projects include:
Scoping study on recent and future trends in counterfeit goods.

3 Research highlights: PhD projects

The Dawes Centre funds a range of PhD projects covering an array of topics of relevance to our agenda. There are currently 16 students on our programme, with three of these being part of the new CDT in Cybersecurity, which is a collaboration with the departments of Security and Crime Science, Computer Science, and STEaPP. The PhD projects that began during the current reporting period are described below:

Money laundering and terrorist financing future directions

International anti-money laundering and counter-terrorist financing (AML/CTF) efforts have grown exponentially since the 1990s. AML/CTF is now a key element of financial services, combining obligations set by both domestic and supranational organizations. However, these detection efforts are consistently increasing in implementation costs, while failing to keep up with the latest money laundering and terrorist financing risks. New payment methods are providing new opportunities for illicit transactions, while cryptocurrencies continue to pose new risks by increasing the anonymity of their users. Contemporary prevention initiatives are struggling to keep up with rapidly improving criminal sophistication. This project aims to apply a crime scripting approach to detecting the likelihood, nature and scale of suspected money laundering or terrorist financing offences. This involves understanding the motives, constraints and indicators involved in each stage of the offence to potentially predict the previous or subsequent stages. In doing so, the prevention, resource allocation and successful investigation rates of law enforcement agencies can be improved. The project includes a scoping review, a Delphi Study to identify future typologies based on projected risks, and a subsequent scripting exercise of past cases to explore whether crime scripting can be an effective means of contributing to contemporary AML/CTF efforts.

PhD start year: 2019
PhD researcher: **Eray Arkatuna**
PhD supervisors: **Dr Amy Thornton**, UCL Security and Crime Science, **Prof Shane Johnson**, UCL Security and Crime Science
Contact: **eray.akartuna.17@ucl.ac.uk**

Guarding against adversarial perturbation in automated security algorithms

Deep Learning algorithms can detect and classify people, activities and objects in images with performance at human-level. These methods are finding their way into consumer products. They also offer great potential in security applications for example in person verification at checkpoints, suspect-finding in video, discovering harmful content on the internet, and detecting threats in bags and parcels. However, they have a curious vulnerability ('adversarial perturbation'), which while harmless for consumer applications offers a potential exploit for determined adversaries in the security realm. An adversarial perturbation is a very small, but very precise, change to the image input into a classifier that causes the classifier output to dramatically change. For example, with just the right perturbation an image of a cat can be mis-classified as a dog, while still looking like a cat to a human viewer. In the context of security this method could allow an adversary to, for example: alter harmful video content to escape detection by automated methods; conceal threats in bags; or maliciously 'place' targeted individuals into pornographic content, so far as face-based search algorithms are concerned. At present there is no known fix for adversarial perturbations. Can this problem be fixed, or is it an issue that we need to learn to live with and safeguard against in other ways? This PhD will address this problem before adversaries develop the sophistication to exploit it.

PhD start year: 2019 (April)
PhD researcher: **Maximilian Mozes**
PhD supervisors: **Prof Lewis Griffin**, UCL Computer Science, **Dr Bennett Kleinberg**, UCL Security and Crime Science
Contact: **maximilian.mozes.18@ucl.ac.uk**

Anomaly detection for security

Anomaly detection is the task of identifying items or events which deviate significantly from normal appearance or behaviour. This is a well-established approach in financial fraud detection, but is applicable in many other areas within the security domain. In X-ray screening of baggage and cargo it can be used to detect concealment, even if a threat is not directly recognizable. In biometric verification it can be used to detect tampering, such as facial morph images which match two identities. In home security it can enable advanced alarm systems that warn when unusual physical or digital activity is occurring.

Anomaly Detection is a sub-problem of machine learning. It is common for machine learning applications to be hindered by a lack of sufficient available training data. This problem is raised to its most extreme form in anomaly detection, where there may be no available example anomalies. The answer, to be explored in this PhD project, is to use methods of self-supervised rather than supervised learning. Self-supervised learning uses proxy tasks which can be defined on normal data, allowing effective data representations to be learnt from that data alone, rather than on the contrast between normal and threat data. Effective representations allow effective modelling of the distribution of normal data so that anomalous deviations can be spotted.

The goal of the PhD will be to develop self-supervised learning methods that are effective for anomaly detection. The first problem to be worked on will be anomaly detection in X-ray security imaging. Other problems that we plan to explore are anomaly detection in audio (for deep fake detection), in video streams (as an AI-driven flexible home emergency/crime alarm), and in text (for detecting phishing, and similar, emails).

PhD start year: 2019

PhD Student: **Kimberly Ton-Mai**

PhD Supervisors: **Prof Lewis Griffin** and **Dr Toby Davies**

Contact: **kimberly.mai@ucl.ac.uk**

Computational Analysis of Cryptoasset Fraud

Cryptoassets represent a fundamental shift in the way we perceive, interact, and transact with financial instruments, potentially heralding in a new era of economic freedom and possibilities. Characterised by distributed decentralisation, cryptoassets promise freedom from centralised institutions and aim to bring the outdated financial sector fully into the internet age. Many cryptoasset projects are actively being developed and have not currently realised their full potential, yet the ideas of decentralised asset networks are showing promise, and may potentially have a global impact not only in the way in which we operate with our assets, but even in what we define our assets to be. Crime follows money, and financial crimes are amongst some of the longest existing types of crime, constantly needing to be battled and requiring countermeasures to be upgraded as monetary systems evolve. Just as the internet amplified existing problems (e.g. child pornography distribution), and brought new cybercrime problems of its own, there is no reason to think that cryptoassets will be any different, especially as there is often monetary incentive. The goal of this research is to examine the landscape of cryptoasset fraud to identify the current and potential fraud threats, and investigate these threats from a computational perspective, with a focus on potential preventive measures.

PhD start year: 2019

PhD researcher: **Josh Kamps**

PhD supervisors: **Dr Bennett Kleinberg**, UCL Security and Crime Science; **Dr Sarah Meiklejohn**, UCL Computer Science

Contact: **josh.kamps.18@ucl.ac.uk**

Using Machine Learning and Natural Language Processing to automatically detect cyberbullying within educational institutions in order to predict and prevent such occurrences

Bullying affects millions of children throughout the world each year. The Department for Education states that in the UK alone, one in six children aged 10–15 have reported being bullied, and 7% of these children have experienced some form of cyberbullying and cyberthreats made to them. Automatic cyberbullying detection is a task of growing interest, particularly in the Natural Language Processing and Machine Learning communities. As a result, it can be used to prevent individuals from receiving harmful online content in social networks, therefore aiding in the reduction of the incidence of cyberbullying.

PhD start year: 2019

PhD student: **Hawra Hosseini-Milani**

PhD supervisors: **Dr Ingolf Becker**, Security and Crime Science;
Dr Leonie Maria Tanczer, STEaPP;
Prof Shane Johnson, UCL Security and Crime Science

Contact: **hawra.hosseini-milani.19@ucl.ac.uk**

Detection and Mitigation of Financial Fraud in the Cryptocurrency Space

The rise in popularity of cryptocurrencies since the release of Bitcoin in 2009 has changed the face of financial fraud, facilitating lower-risk anonymous money laundering and fraudulent transfers on a massive scale. Methods of detecting, mitigating and preventing financial fraud remain underdeveloped relative to the value of the cryptocurrency market, and the efforts of academics, law enforcement and policymakers remain in their infancy. This project will adapt data science-based fraudulent transaction detection methods used in traditional financial services to the cryptocurrency market to ascertain their effectiveness in the cryptocurrency space. The results of this project will provide an empirical basis for policymakers to develop evidence-based legislation surrounding digital currencies worldwide, as well as provide a necessary contribution to this currently sparse body of academic literature. It will also enable innovation, facilitating the entry of conventional financial services companies into the cryptocurrency arena by providing a method for conducting due diligence on these transactions in the absence of accepted anti-money laundering processes.

PhD start year: 2019

PhD student: **Arianna Trozze**

PhD supervisors: **Dr Toby Davies**, UCL Security and Crime Science, and **Dr Bennett Kleinberg**, Security and Crime Science

Contact: **arianna.trozze.19@ucl.ac.uk**

Protecting the UK's News propagation systems against the threat of 'deepfake' injection

This Phd will investigate the levels of threat that "deepfakes" pose with regard to various contexts within human society, by means of conducting a human user study and testing to find contexts where humans are deceived by these deepfakes and whether any particular types of humans are particularly easily deceived. The main context to be studied will be news propagation. After establishing the various levels of threat posed by deepfakes, the project will aim to propose protection systems for the UK's mainstream news propagation networks, such that the UK might lead the way in protecting its news systems and journalists against the possibility of "deepfake news injection". The context of mainstream news propagation networks in the UK is one that is heavily adverse to outside regulation. The freedom of the press is important. However, with research evidencing that deepfakes are a threat to an array of important stakeholders via the context of news propagation, measures can be taken to implement such fixes as are necessary whilst leaving journalistic liberties intact.

PhD start year: 2019

PhD student: **Sergi bray**

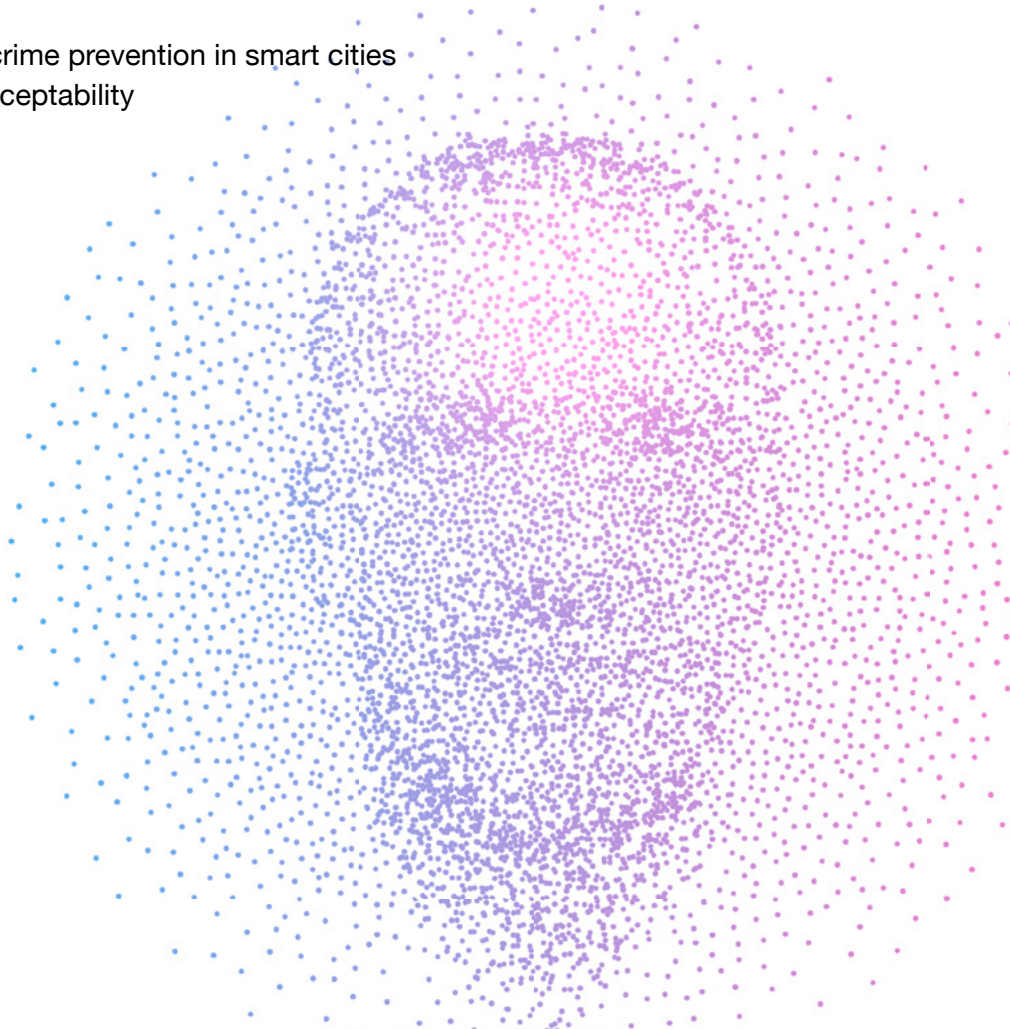
PhD supervisors: **Dr Bennett Kleinberg**, UCL Security and Crime Science, **Prof Shane Johnson**, UCL Security and Crime Science

Contact: **sergi.bray.18@ucl.ac.uk**

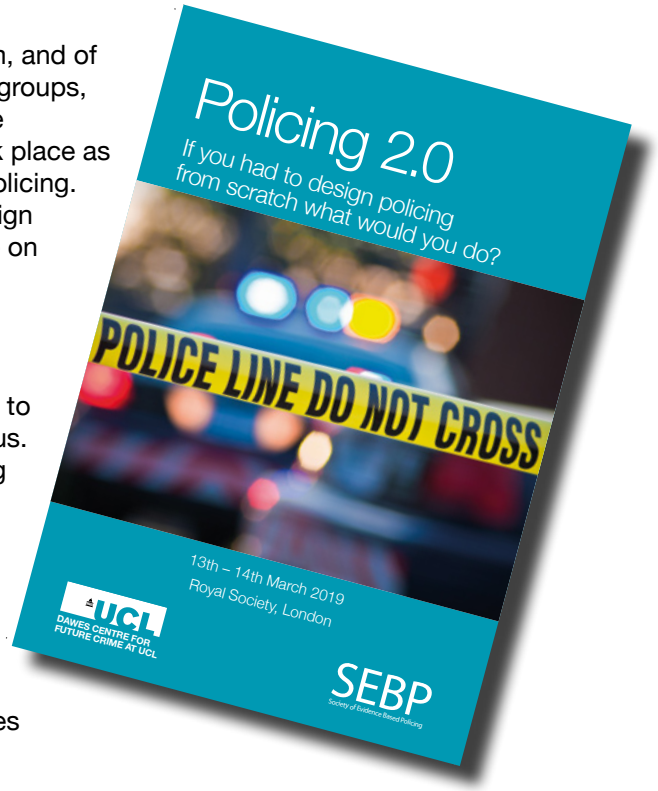
For details of PhD projects that began prior to the current reporting period please refer to our website:
www.ucl.ac.uk/jill-dando-institute/research/dawes-centre-future-crime

These projects are:

- Crime, place and the internet
- Biocrime – are we prepared for it?
- A study of potential cybercrime risks to the future street infrastructure of London
- The effects of cyberweapons
- Refugee Flows and Instability
- Detecting emerging crimes using data science techniques
- Addressing Probable Child Sexual Abusers and Victim Profile Characteristics on Instagram
- Horizon scanning through computer-automated information prioritisation
- Identifying opportunities for crime prevention in smart cities and evaluating their social acceptability



Annual Conference



Each year we organise a conference to highlight work from, and of interest to, the Dawes Centre and its associated research groups, institutes and centres at UCL. The conference is called the International Crime Science Conference and this year took place as part of a joint event with the Society of Evidence Based Policing. The conference was titled 'Policing 2.0 – If you had to design policing from scratch what would you do?' and took place on 13–14 March 2019.

Policing is changing. Part of that change is the result of external circumstances and partly the result of internal reflection and a desire to improve the service that we offer to the communities – local, national and global– that rely on us. This conference was aimed at all those involved in policing with an interest in shaping the future of the service.

This unique event looked at critical questions such as:

- What does the evidence base look like for interventions that we use in battling crime?
- What do we forecast to be the greatest crime challenges in the near future?
- How should we design policing to be most effective in battling those challenges?
- How do we continually test and learn?

The conference brought together leading police practitioners, policy-makers, private sector organisations and researchers to promote interaction, inspiration and innovation. Professor Lawrence Sherman (Cambridge University) opened proceedings by laying down the challenges in this critical space, and Chief Constable Sara Thornton then reflected on the obstacles that stand in the way of policing becoming more evidence based. The programme included presentations and discussion from practitioners and academics presenting some of the latest evidence in this area, including an analysis of case studies. The objective of the event was to spark discussion and reflection on police practise, collaboration between forces and between police and other stakeholders such as academia.

As ever, the event showcased leading international research and responses to critical threats, and brought together 200 professionals to promote interaction, inspiration and innovation.

Teaching

The Centre continues to grow and embed its teaching offering which now encompasses undergraduate and postgraduate modules, as well as the supervision of masters-level dissertation projects and, of course, supervision of our doctoral students. We currently offer modules covering security technologies, data science for crime scientists, applied data science, cybercrime, and horizon scanning. New for 2019, we launched a module in applied data science for postgraduate students who learn to translate practical problems into data science problems that can be addressed using computational methods.

Benefits of our teaching programme

A principal benefit of the teaching modules we offer is that they facilitate the opportunity to engage, via training, a new generation of students to think about the future crime implications of technological and other changes. Furthermore, the content of our modules has helped to reinforce external relationships. For instance, for one of our modules, students produce horizon scanning posters which are presented annually at the Home Office. These events have been attended by representatives from the MOD, NPCC, and HMIC as well as Home Office staff. This module on horizon scanning has been significant for several reasons. Crucially it has helped to identify the Centre with a specific approach, which is fundamental to understanding crime futures and helps us establish the intellectual space around crime futures. The course has proved extremely popular and lays the foundation for incorporating the futures dimension in all aspects of crime science.

PhD teaching

Our cross-disciplinary supervision of the PhD programme enables us to complete longer-term research that levers interdisciplinary (supervisory) expertise across UCL. Some of the Centre's PhD students are working directly with stakeholders, including government departments, to shape projects and have contributed bespoke 'state of the art' literature reviews. This all augurs well for our aim to instill, via our teaching, an early respect for the impact that we wish our students to generate in the real world through their work at the Centre.

We currently offer modules covering security technologies, data science for crime scientists, applied data science, cybercrime, and horizon scanning.

External engagement

Part of the Centre's strategy is to engage with other research centres and agencies involved in work related to the aims of the Centre. The objectives of this activity include promoting the Centre, better understanding what the police and other agencies are doing about future crime problems (in terms of trying to identify or prevent them), identifying opportunities for collaboration, uncovering potential sources of additional funding, and locating those who might usefully contribute to the work of the Centre or inform the direction of our activity.

For various reasons we cannot detail all of the organisations with whom we are interacting, but they include representatives from the police, professional bodies, the private sector and Non-Government Organisations involved in crime prevention.

Engagement activities include our stakeholder "sandpits", which are conducted as part of our scoping studies, stakeholder involvement in research projects, guest lectures on our taught programmes (with contributions from the College of Policing, Home Office, Australian and New Zealand Police Advisory Agency, ACE, and DSTL), and input to PhD research. Some notable stakeholder workshops this year have explored how cryptocurrencies might facilitate (future) crime, how we might better understand (future) police demand, and how emerging technologies might be used to reduce domestic abuse.

An ongoing collaboration with the Home Office, Worshipful Company of Information Technologists (WCIT), Suzy Lamplugh Trust and Neighbourhood watch is used to promote the future crime agenda to the voluntary sector, industry and other government departments. This has included a number of presentations at the Home Office attended by the voluntary sector, and industry representatives (e.g. Tech UK). The most recent event was a full-day event held at the WCIT premises in London in January 2020. There were over 40 attendees with representation from the College of Policing, CPS, dstl, Home Office, Institute for Corporate Responsibility, Ministry of Justice, Neighbourhood Watch, the NCA, the Police Foundation, academia (UCL, Oxford Brookes, Nottingham Trent, Bedfordshire) and the Charity Sector (e.g. Age UK, Against Violence and Abuse, CAF, Missing People, Women's Aid), the National Lottery Community Fund, and the WCIT. As well as promoting the agenda of the Centre, these events help to build our network of potential contributors to projects and attendees for sandpit events.

To facilitate the discussion of 'futures', we have hosted a number of events for other organisations engaged in this type of work. These include hosting the DSTL Future Communities of practice event in Sept 2019, and the College of Policing's Future Operating Environment scenario workshop in November 2019.

As a new venture, in 2019, Dr Kleinberg – together with Dr Paul McFarlane (Dept. of Security and Crime Science) - ran a number of data science "hackathon projects" with the Metropolitan Police. Their aim was to respond to practical problems quickly while offering high-quality advice and prototype solutions using an interdisciplinary team.

Finally, we have started working with the UCL Department of Science, Technology, Engineering and Public Policy (STEaPP) to produce briefings — based on completed research projects — for policy makers and other stakeholders. The first of these, on the topic of Artificial Intelligence and Crime, will be launched in 2020.


/Administration
/Human Resources
/Legal
/Accounting
/Finance
/Marketing
/Publicity
/Promotion
/Research
/Business
/Development
/Engineering
/Manufacturing
/Planning

Dissemination

Staff and students have given presentations at a variety of national and international conferences to include:

- Keynote at the Applied Research Crime and Justice conference, Brisbane, Australia (Feb 2020)
  Future Crime (Prof Johnson) available at:
  https://www.youtube.com/watch?v=2jo3zdH0maQ
  and for Queensland police (see QPS Bulletin, right)

- Keynote at the CityForum Annual Policing Roundtable, London, UK (July 2019)
  Emerging technologies and impacts on crime – can policing keep up? (Prof Johnson)

- European Science Advisors Forum, Dublin, Ireland (June 2019)
  How do you assess if your policy works? (Prof Johnson)

- Advances in Data Science, Manchester, UK (May 2019)
  The potential and problems of data science for crime research (Dr Kleinberg)

- Invited special session at the Institute for Financial Crime, The Hague, Netherlands (April 2019)
  Cryptocurrency fraud (Dr Kleinberg)

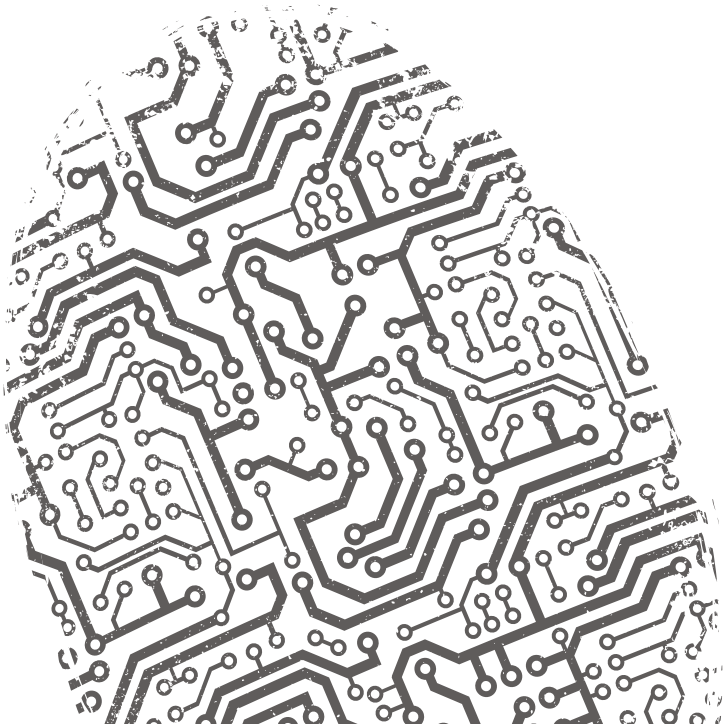
Conclusion

We have had another productive year. A number of exciting new projects have commenced while existing projects have been completed or progressed towards fruition. We have an ever expanding cohort of PhD students on board providing a longer-term research capacity in key areas of interest. A particular highlight has been our first cross-institutional projects, including one jointly-funded with Nottingham Trent University, looking at smart tech solutions to domestic abuse. This is a particularly pervasive problem that sometimes slips below the radar in terms of how modern technology and science might be applied to its mitigation, so we are excited at the possibilities of carrying out research in this area.

Our profile has continued to rise and this is making it increasingly possible to raise external funding. During this last period we were able to work with Leeds University on another joint project which was funded by the Alan Turing Institute. That project looks at changing police demand and how this might be modelled. We are pleased to announce that this project has been funded for a second and, recently, a third phase.

We have continued to increase our staff capacity – a new, full-time researcher has joined us, Dr Manja Nokolovski, and she is a very welcome addition to the team. Last year we announced that, in collaboration with the UCL departments of Computer Science and STEaPP, we were successful in an application to the EPSRC for a new Centre for Doctoral Training (CDT) in Cybersecurity. This centre accepted its first PhD cohort in September 2019, including a number working specifically on Dawes Centre topics.

As we move into the new reporting year, we are all caught up in the grip of an unprecedented social and economic crisis. The COVID-19 pandemic has disrupted society at a fundamental level and will continue to do so for some time to come. One of the ways that the Dawes Centre is seeking to respond is by examining how the pandemic has impacted upon crime in the UK and internationally to date and how different policy options might impact upon crime in the future. This work is intended to not only help us understand the impact of the current crisis on crime, but to provide insights into how other disruptions might affect crime and how we might respond to them in the future. To support this activity, with colleagues at the University of Leeds, we have succesfully acquired £0.6M funding from UKRI to tackle these meaningful questions. In the meantime we wish everyone the very best at an uncertain time. In spite of the current difficulties, we look forward to the coming year with hope and optimism.



Publications

The following Centre-related articles authored by Centre staff are published or in press:

Elgabry, M., Nesbeth, D., & Johnson, S. D. (2020). A systematic review protocol for crime trends facilitated by synthetic biology. *Systematic Reviews*, 9(1), 22.

Laufs, J., Borrion, H., & Bradford, B. (2020). Security and the smart city: A systematic review. *Sustainable Cities and Society*, *55*, 102023.

Johnson, S. D., Blythe, J. M., Manning, M., & Wong, G. T. (2020). The impact of IoT security labelling on consumer product choice and willingness to pay. *PloS One*, *15*(1), e0227800.

Wixey, M., Johnson, S., & De Cristofaro, E. (2020). On the Feasibility of Acoustic Attacks Using Commodity Smart Devices. *IEEE Conference SafeThings*, in press.

Blythe, J. M., Johnson, S. D., & Manning, M. (2020). What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices. *Crime Science*, *9*(1), 1.

Shukla, M., Johnson, S. D., & Jones, P. (2019, June). Does the NIS implementation strategy effectively address cyber security risks in the UK?. In 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security) (pp. 1-11). IEEE.

Soldner, F., Ho, J. C. T., Makhortykh, M., van der Vegt, I. W., Mozes, M., & Kleinberg, B. (2019, June). Uphill from here: Sentiment patterns in videos from left-and right-wing YouTube news channels. In *Proceedings of the Third Workshop on Natural Language Processing and Computational Social Science* (pp. 84-93).

Volodko, A., Cockbain, E., & Kleinberg, B. (2019). "Spotting the signs" of trafficking recruitment online: exploring the characteristics of advertisements targeted at migrant job-seekers. *Trends in Organized Crime*, 1-29.

Frith, M. J., Simon, M., Davies, T., Braithwaite, A., & Johnson, S. D. (2019). Spatial interaction and security: a review and case study of the Syrian refugee crisis. *Interdisciplinary Science Reviews*, *44*(3-4), 328-341.

Kleinberg, B., & McFarlane, P. (2019). Examining UK drill music through sentiment trajectory analysis. *ArXiv:1911.01324 [Cs]*. http://arxiv.org/abs/1911.01324

Kleinberg, B., van der Vegt, I., & Gill, P. (2020). The temporal evolution of a far-right forum. *Journal of Computational Social Science*. https://doi.org/10.1007/s42001-020-00064-x

Lukács, G., Kleinberg, B., Kunzi, M., & Ansorge, U. (2020). Response Time Concealed Information Test on Smartphones. *Collabra: Psychology*, *6*(1), 4. https://doi.org/10.1525/collabra.255

van der Vegt, I., Gill, P., Macdonald, S., & Kleinberg, B. (2019). Shedding Light on Terrorist and Extremist Content Removal. *Global Research Network on Terrorism and Technology*. https://rusi.org/sites/default/files/20190703_grntt_paper_3.pdf

Ife, C.C., Davies, T., Murdoch, S.J., & Stringhini, G. (2019). Bridging Information Security and Environmental Criminology Research to Better Mitigate Cybercrime, arXiv preprint *arXiv:1910.06380*, currently under review at *ACM Computing Surveys*. print *arXiv:1910.06380*, currently under review at *ACM Computing Surveys*.

Reports to DCMS

Nikolvska, M., and Johnson, S.D. (2020). IoT Device Support Periods and Default Passwords: An Update.

Dawes Centre for Future Crime at UCL
35 Tavistock Square
London
WC1H 9EZ