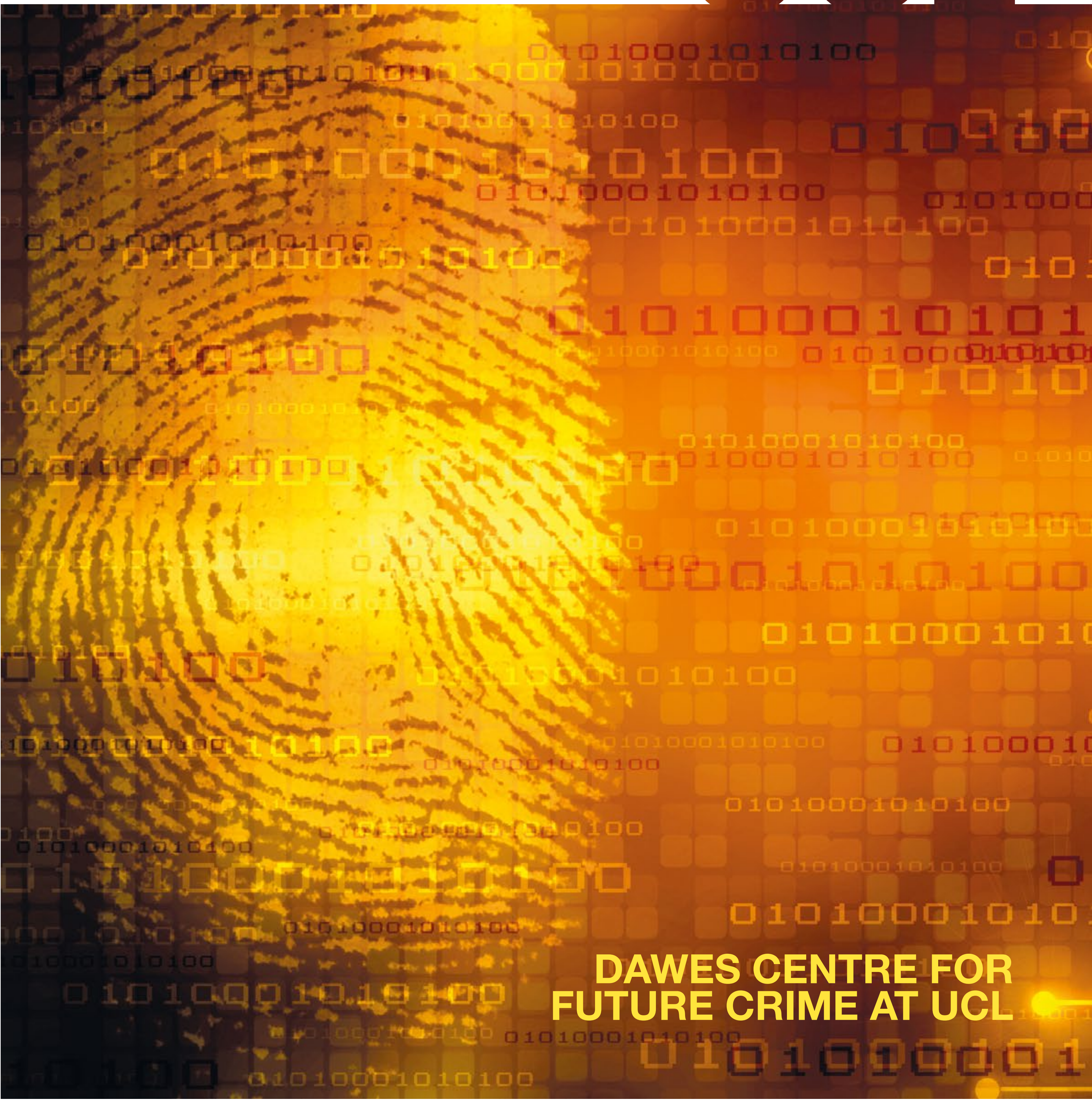
JILL DANDO INSTITUTE OF SECURITY AND CRIME SCIENCE
DAWES CENTRE FOR FUTURE CRIME AT UCL



DAWES CENTRE FOR FUTURE CRIME AT UCL

ANNUAL REPORT
1 MARCH 2018 – 28 FEBRUARY 2019

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 2018 to 28 February 2019. 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 second full year of activity of the centre. In this period, we have continued to build on the momentum generated in the first year of activity, and as a strategic priority have built capacity in the areas of data science and cyber crime. New scoping studies and PhD projects have come on stream, with a number of 'sandpit' workshops in these areas taking place to bring together academics with practitioners to examine particular future crime topics. For instance, we held a truly eye-opening sandpit around Artificial Intelligence and its potential to generate new forms of crime in January this year.

Engagement with the Centre by academics, practitioners, and other stakeholders, has continued on its upward trajectory, so much so that our 2019 annual conference is in partnership with the Society of Evidence Based Policing at the prestigious Royal Society in London. Our sandpit 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, which will grow as more projects come to fruition. We continue to engage in thought-provoking discussions with researchers from across the disciplines and stakeholders across an increasing range of organisations. We look forward to working with all of our partners in the coming year 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 will:

- 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
- 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 nine permanent members, constituted of representatives from:

The Dawes Trust

Sir Stephen Lander
John Graham
Stephen Webb

Independent Advisors

Sir Richard Broadbent
Business Sector[1]

Professor Andy Bell
Home Office Centre for Applied Science and Technology

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 (Researcher), Mr Vaseem Khan (Project Manager), and the Centre Administrator.

[1] Sir Richard Broadbent stepped down from this role in January 2019.

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**

The **scoping study on recent and future trends in counterfeit goods** was completed during this period.

2 **Current projects**

Five other projects are underway covering topics ranging from **Advanced materials to combat crime** to **Refugee flows and instability**.

3 **PhD projects**

This year, we recruited six new PhD students, increasing the team of students conducting research in areas of interest to the centre to ten.

Further details of all of the above are provided in the Research Highlights section on page 6.

The year also saw us organise the second of a series of future crime conferences. Held at the British Library in London, the theme of the conference was Trafficking and Exploitation: using science and technology to tackle one of the world's greatest crime problems.

We also continued to build on our taught modules, including an undergraduate module on Security Technologies (now in its second year of delivery), and the introduction of a new module on horizon scanning. 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?

Research highlights: Completed projects

Scoping study on recent and future trends in counterfeit goods

Counterfeit products are big business, with an estimated value of half a trillion US dollars per year, and they can cause serious harms, including poor treatment of life threatening diseases, impaired pest control for food crops, and brand damage, to mention just a few. 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 need for fast analytical methods to test the chemical composition of the contents of such products. This project involved a scoping study to examine current and future trends in counterfeiting and to evaluate the technology that might be used to identify counterfeit goods.

Half a trillion USD – the worldwide estimated trade in counterfeit products in 2013[2]

Specifically, the project focused on products composed of chemical mixtures where the same or similar analytical techniques for authentication might apply.

These products include pharmaceutical medicines (the overall economic impact of fake drugs is estimated to be €10.2bn for the European pharmaceutical industry); food and drink (from horse meat scandals to diluted ‘wild’ honey – in an INTERPOL coordinated operation involving 57 countries, more than 10,000 tonnes and one million litres of hazardous fake food and drink were seized); agrochemicals (there are indications of increased trade in illegal and counterfeit plant protection products), and toiletries (online purchases of toiletries are increasing and it is currently estimated that ~30% are fake).

[2] OECD & EUIPO. Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact. (OECD Publishing, 2016). doi:10.1787/9789264252653-en

This project has now been completed with a final report submitted in September 2018. To inform the sandpit and the project more generally, the team initially conducted a review of the goods most likely to be affected by the production of fake materials. Informed by this, a range of stakeholders who could contribute most strongly to the research and its future directions were invited to the sandpit. This event was held on 11–12 April 2018, and attended by 16 participants from six universities, Border Force, the Intellectual Property Office, the Defence, Science and Technology Labs (DSTL), the Medicines and Healthcare Products Regulatory Agency, and the National Crime Agency. During the sandpit, participants discussed current problems and the future issues they anticipated. At the end of day one, each participant was asked to identify three problem areas for further discussion. On day two, the proposed problem areas were grouped into similar problems, and a vote held to select the top six. Discussions that followed focused on elaborating upon the topics, proposing solutions to them, articulating the research challenge (including ethical issues) and identifying implementation constraints.

30% of online toiletry purchases are estimated to be fake[3]

Ultimately, six areas of concern were identified and one was selected for further study. The selected topic was fake agrochemicals and how they might be prevented from being used in farming and other ground control activities. This topic has been submitted for follow-on funding as a Phase 2 project, and is currently under review by the Dawes Executive Committee. The team are currently preparing a Review Article on Fake Goods that will be submitted to the Crime Science Journal (subject to approval from the Executive Committee). A public-facing version of the Final Report will also be made available in due course.

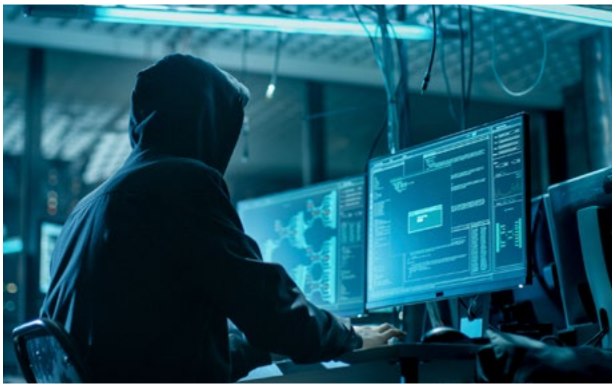
Lead investigator(s)
Prof Robert Speller,
Richard Lacey (Home Office CAST)

[3] MarkMonitor. Global Online Shopping Survey 2017 – Consumer Goods. (2017).

Research highlights: Current projects

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 the proposed project is to examine whether lessons learned in relation to urban crime can be applied or adapted to online environments.

The primary aim of the proposed work is 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 is 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. The sandpit followed the same format as the counterfeiting goods project, with participants working in groups to generate a long list of problems and projects on day 1, from which four were selected for development on day 2.

The team are currently completing the final report for this project which will be accompanied by a proposal for a phase 2 project.

Lead investigator(s)
Dr Toby Davies
Dr Gianlucca Stringhini

Advanced Materials to Combat Crime

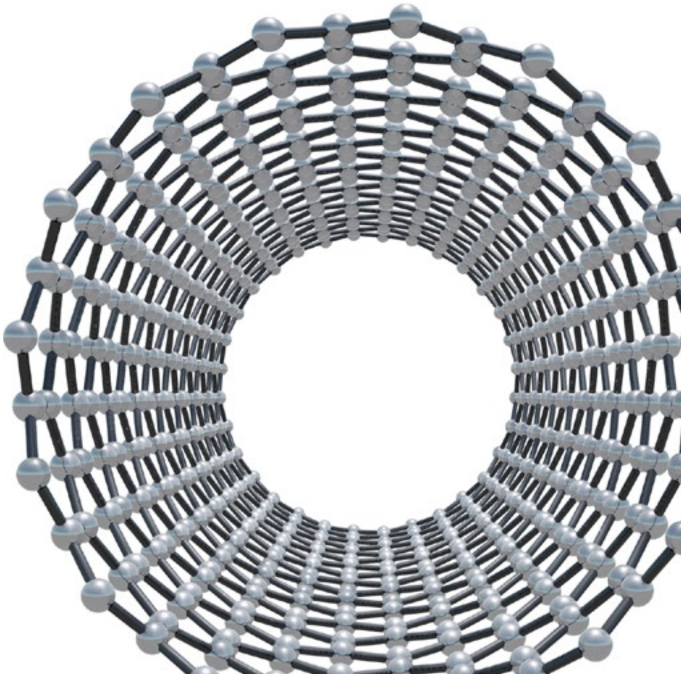
Work on advanced materials includes the discovery of new materials with novel properties, as well as the modification of existing ones to alter structural and/or functional properties in order to obtain superior performance for specific applications. Such materials include metal and alloys, ceramics, 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 considers 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 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.

Lead Investigator
Prof Kwang-Leong Choy



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

The 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 had a slightly different format to the others, mixing 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. The final report for this project, along with a proposal for a Phase 2 project, will be submitted to the executive committee shortly.

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.

10% – the number of IoT device manuals or associated online materials that advise consumers how to secure a device from cyber risks[4]

While security should be designed into devices, there is little incentive for manufacturers to do so consistently. Moreover, at the point of purchase, consumers are not provided with simple information to help them assess the security of devices. This differs from the traffic light system used for food products in supermarkets, or the energy efficiency ratings provided for many electronic goods. The aim of this ongoing project is to better understand the potential crime threats associated with consumer IoT devices, to develop a Consumer Security Index, and encourage its use to incentivise manufacturers to improve IoT device security, and to help consumers purchase more secure devices.

The work conducted to date has 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.

This research is already having a direct impact on policy as we have been working very closely with DCMS, and a labelling scheme is now a policy option that they are seriously considering as a way of addressing vulnerabilities in consumer IoT. Our work is cited in their Secure by Design Code of Practice and will be discussed in a forthcoming DCMS publication. Our work 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**).

*This project is co-funded by PETRAS, the Internet of Things hub, and DCMS funded data collection for the consumer choice study.

Lead investigator(s)
Professor Shane Johnson
Dr John Blythe

[4] Blythe, J.M., Sombatruang, N., Johnson, S.D. (2019). What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages? This is a finding from a Dawes Centre project reviewing 270 IoT device manuals. *Journal of Cybersecurity*, Volume 5, Issue 1, 2019, tyz005, **https://doi.org/10.1093/cybsec/tyz005**

Refugee Flows and Instability

More than 60 million people – approximately 1 in every 120 people on the planet – are currently displaced from their homes by conflict, persecution, famine, or natural disasters. In 2014 alone this amounted to 42,500 people each and every day being displaced. Of these, one quarter to one third are refugees. This project involves a collaboration with researchers at the University of Arizona that seeks to design tools for the collection and analysis of fine-grained data on the transnational movements of refugees out of conflict zones. These data will be used to test hypotheses about why individuals flee conflict zones as refugees, how they determine which routes to take, and what effect they have on the security and stability of the destinations at which they settle.

To date, a survey has been fielded with former Lebanese refugees from the Lebanese Civil War and current Syrian refugees in Lebanon. Focus groups have also been conducted with former Lebanese refugees from the Lebanese civil war and current Syrian refugees in Lebanon. The data collected are being analysed to understand:

- what influences refugee's decisions to flee, settle or return to their own country
- law breaking and law bending in terms of how international migrants negotiate state borders

We have also designed a baseline version of a computer simulation model of refugee flows that will be used to examine how different scenarios might impact on flows and instability.

The implications of this research project extend beyond the current refugee crisis. The findings will be relevant to forced migration crises that emerge across multiple regions and in response to a variety of event types that might occur in the future.

Lead investigators
Dr Alex Braithwaite, University of Arizona
Dr Faten Ghosn, University of Arizona
Dr Toby Davies, UCL
Professor Shane Johnson, UCL

Reducing Domestic Abuse using Technology

In 2018, we held two workshops to explore how developing technologies might help to reduce the incidence of, and/or harm from domestic abuse. The aim of the first workshop was to work with domain experts to produce a "requirements brief" that mapped out a handful of priority problems, together with any factors that constrain how they are dealt with now and how they might be dealt with in the future.

The aim of the second workshop was to identify possible solutions to the problems identified, and to this event we invited a mixture of domain experts, designers and engineers. The outcome of the second workshop was the identification of a set of candidate projects that the Centre might fund either using existing resources, through applications to external funders, or both. The following possible projects were identified:

- Detecting historic patterns of isolation in social media feeds of known victims using machine learning and social media data
- The use of GPS and/or Bluetooth beacons for offender geo-location tagging
- The use of Near Field Communication (NFC) or Bluetooth dots as a panic alarm or an evidence collection trigger for smart devices
- Removing or concealing digital footprints in survivor online search histories
- Use of chat bots to engage offenders, and automated persuasion systems to facilitate behaviour change
- Immersive (police) training on domestic abuse

Following the workshops, each of these ideas was explored with the potential project leads to explore what a project would look like and what funding or resources would be required to complete it. A new project, that will explore the potential uses of bluetooth beacons and NFC technology, that will be conducted and co-funded by researchers at Nottingham Trent University will commence in the next reporting period. Additional work will also commence with colleagues in the UCL department of Science, Technology, Engineering and Public Policy (STEaPP) to explore what might be learned about the changing nature of domestic abuse from data provided by CrimeStoppers.

Lead investigators
Prof Shane Johnson
Dr Eiman Kanjo, Nottingham Trent University

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 nine students on our programme, and the PhD projects that began during the current reporting period are described below:

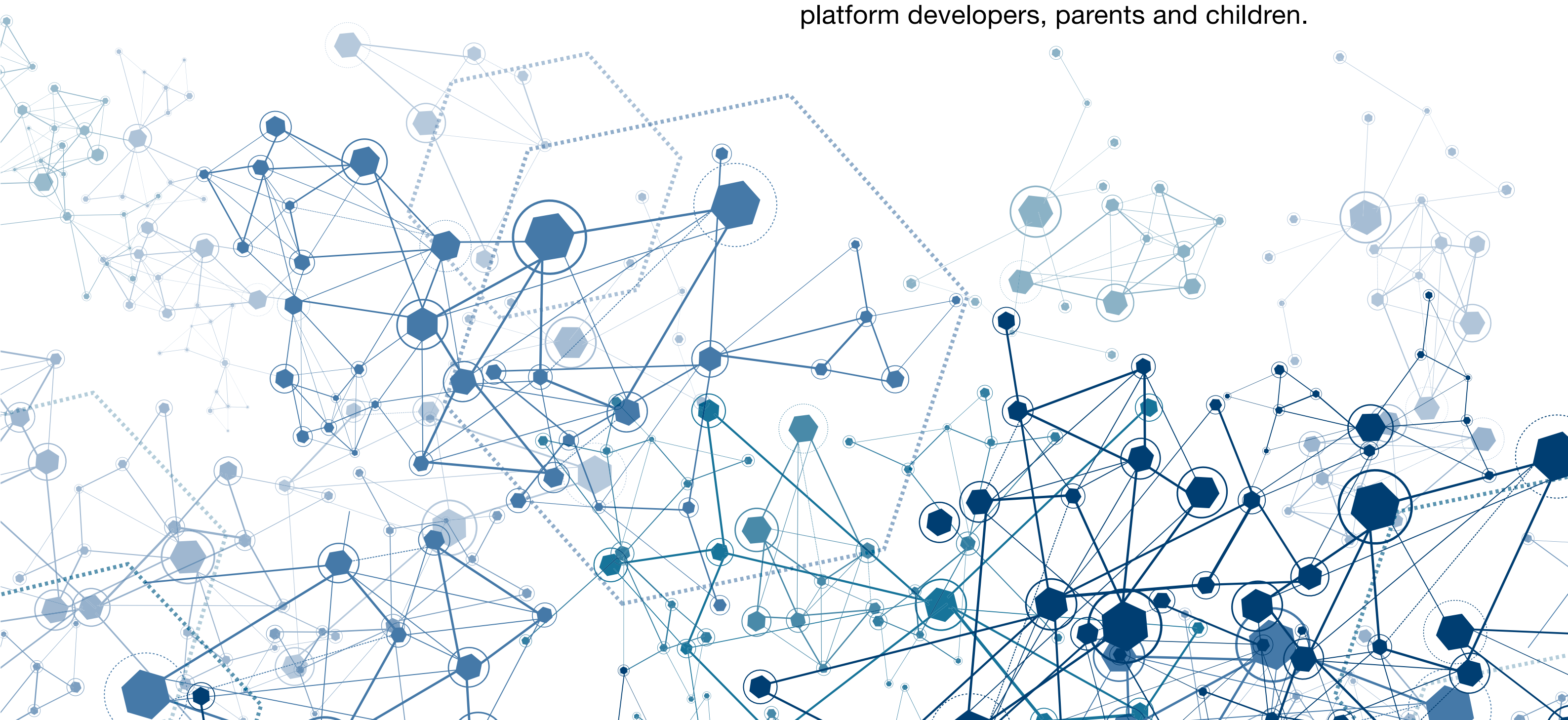
Detecting emerging crimes using data science techniques

More and more people engage in online activities through social media platforms (Facebook, Twitter etc.) or online markets (e-bay, Amazon etc.). Such environments enable individuals with malicious intent to affect large numbers of people. The amount of data available is simply too much to be analyzed by humans alone. Automated methods, such as machine learning (ML) or natural language processing (NLP) techniques are able to meaningfully analyze enormous amounts of data. NLP methods can extract grammatical or semantic information from text. For example, finding linguistic commonalities of fraudulent advertisements can be utilized to train ML classifiers, which can then categorize advertisements as being fraudulent or non-fraudulent. With the help of such techniques possible emerging crimes can be uncovered. The goal of this research is to combine human knowledge and data science techniques to find potential emerging crimes, support future human decision making and find ways of preventing new crimes.

Addressing Probable Child Sexual Abusers and Victim Profile Characteristics on Instagram

The use of the Internet and online Social Networks (OSN) has increased drastically in recent years, and increased exposure of children to child sexual abuse (CSA) has followed. However, few empirical studies have been conducted to address the factors that contribute to exposing children to child sexual abusers online and to identify the characteristics of the individuals who contact them. Recent studies have demonstrated that child sexual abusers come from various demographic backgrounds and that it is a challenge to describe a ‘typical’ offender. Studies have also shown that girls are more exposed to CSA attacks than boys but identified no differences in victim ethnicities.

Based on the routine activity approach (RAA), this PhD research extends published work by introducing a methodology to explore the online social communities where probable offenders and children interact and investigating the characteristics of both, as well as any associations between them. The knowledge obtained from this experiment could be used by many private and public sectors such as: law enforcement, child protection entities, school teachers, social media platform developers, parents and children.



Identifying opportunities for crime prevention in smart cities and evaluating their social acceptability

The use of smart city technology is growing rapidly around the world. While most of the technologies employed in such systems already exist in various other contexts (e.g. cameras or audio sensors), it is the depth of interconnectivity and the use of vast amounts of data that are key to the idea of a smart city. In addition to the advantages these technologies offer for many urban challenges such as transportation, waste management, and environmental protection, they also create new opportunities for crime prevention now and in the future.

However, new security technologies may cause controversy because of the threat they can pose to personal data and privacy, which can lead to a lack public support, making them fail in the long-term. This can have serious consequences for the companies designing them, the end-users who employ them, the governments who authorise them, and the citizens whose security or personal data may be compromised.

The goal of the proposed research is to identify how new smart city technologies may be used for crime prevention and identify possible obstacles to their implementation. Special emphasis will be placed on how different technologies are perceived and with what level of public support they are met. In addition, the study aims to test to what extent public perception of smart city interventions correlates with risks previously identified by practitioners. Overall, the study aims for practical applicability by identifying specific interventions and criteria for their '(social) acceptability', laying the groundwork for their future implementation in the United Kingdom.

Low energy X-ray backscatter imaging for non-destructive evidence harvesting

When X-rays interact with a material, one process that can occur is inelastic or Compton scattering where the X-ray loses some energy to an electron in the material and consequentially changes direction. Sometimes the X-ray will be scattered in the backwards direction. The probability of an X-ray scattering in a direction which is useful for backscatter imaging is dependent on the incident X-ray energy and the density of the material it interacts with.

This relationship is described by the Klein-Nishina equation but, importantly, the probability of an X-ray scattering in the backwards direction is greatest for low energy X-rays interacting with low density materials (i.e. organics). This makes X-ray backscatter imaging a useful technique for investigating surface contaminates (e.g. oils, biological material, drugs, explosives, etc.) and features. For example, it may be possible to build a single-sided imaging system that could be used as a non-contact, non-destructive tool for recording fingerprints, particularly on surfaces that are difficult with current techniques (e.g. textured surfaces).

This project is about investigating the technical trade-offs associated with X-ray backscatter imaging for the purpose of scene-of-crime evidence collecting. The project will design and build a lab based experimental setup to develop an understanding of how the X-ray generator/detector geometry and settings can be adjusted to optimise the technique. The project will also investigate how information is affected by background substrate, X-ray energy and detector characteristics.

Horizon scanning through computer-automated information prioritisation

Police forces are seeking to advance their repertoire of analytical and predictive tools to deal with emerging crimes as they adapt to the repercussions of penurious fiscal policies. However, the volume, variety and velocity of data both recorded by police forces and available through open sources means that analysing such data can be an ambitious and challenging undertaking. Despite the aforementioned obstacles, horizon scanning is set to become a prominent aspect of future policing, allowing police forces to identify emerging threats, anticipate imminent crimes and to extinguish future methods of perpetration, in essence, allowing the police to stay one step ahead of criminals.

The aim of this PhD is to develop working relationships with law enforcement organisations to resolve current blockades in horizon scanning. The first stages of the PhD will be to gather information on the structural and relational limitations of the multifarious systems used by police forces. Using this information, and a selection of data science techniques, automated tools will be developed that can identify and prioritise emerging trends in vast amounts of data using natural language processing and machine learning, whilst being able to communicate these results appropriately to the relevant users and stakeholders by employing suitable interactive data visualisations. As the research develops the aspiration will be to incorporate different data sources and types (for example, employing computer vision and deep learning on social media posts) into large scale threat scanning models.

Refugee flows and instability

The massive flow of refugees from conflict zones since the Syrian Civil War has presented global society with increasingly complex problems related to security and economic stability. The crisis is well reflected in the annual report of UNHCR according to which 42,500 people are displaced everyday from conflict zones. The United Nations Refugee Agency reports 65 million people in the world are currently considered as refugees who are looking for asylum and this has triggered a global security issue.

This project investigates why some people flee from conflict zones, where they go and how these movements impact the stability of host countries and global security. The project studies this phenomenon at both microscopic and macroscopic scales. The project will study and model how an individual's decision in conflict zones is affected by the small network of people around them as well as other factors such as social media, language, religion, and the capacity of host countries.

Climate change, conflicts, and many other factors reveal how irregular migration is not going to remain limited to this scale. Thereby, predictive models are growing as a subject of enquiry. The study will investigate patterns of movement on a global scale using network theories and statistical methods to produce predictive models. The approach is intended to enable the forecasting of movements and consequently to inform policy options to tackle the refugee crisis and support this group of migrants.

For details of PhD projects that began prior to the current reporting period please refer to our website. These projects are:

- **Crime, place and the Internet**
- **Biocrime – are we prepared for it?**
- **Cybercrime risks to London's future street infrastructure**
- **The effects of cyberweapons**

Annual Conference

UCL JILL DANDO INSTITUTE OF SECURITY AND CRIME SCIENCE

UCL

Trafficking and Exploitation
using science and technology to tackle
one of the world's greatest crime problems

12th INTERNATIONAL CRIME SCIENCE CONFERENCE
4th July 2018 British Library, London

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 on 4 July 2018 at the British Library in London. The theme of the conference was Trafficking and Exploitation: using science and technology to tackle one of the world's greatest crime problems.

As ever, the event showcased leading international research and responses to critical threats, and brought together 175 security and law enforcement practitioners, policy-makers, scientists, researchers and security industry professionals from around the world to promote interaction, inspiration and innovation.

The importance of trafficking as a crime issue affecting countries and communities around the world continues to grow, with law enforcement facing an increasing struggle to combat the problem as it evolves, enabled by technology and migration patterns. Yet peer-reviewed research in this domain is relatively scarce, when compared to other crime areas. The UCL Jill Dando Institute (within which the Dawes Centre is housed) is greatly interested in this domain and has leading expertise in the area. Amongst the many exciting presentations were:

- Keynote: **Kevin Hyland**, OBE, UK's Independent Anti-Slavery Commissioner and **Dr Ella Cockbain**, UCL Jill Dando Institute
- Internet as an enabler: sexual exploitation and adult services websites **Roy McComb**, Deputy Director, National Crime Agency
- Recruiting modern day slaves: the internet as a driver for human trafficking **Dr Ruth McAllister**, Ulster University
- Trust, triads and brokerage: on the formation and evolution of illicit networks **Professor David Bright**, Flinders University, Australia
- Labour exploitation and trafficking as corporate crime: supply chain activities in food production and cleaning services **Dr Natalia Ollus**, European Institute for Crime Prevention and Control and **Dr Jon Davies**, University of Manchester

The day ended with a panel discussion entitled: ***Are we losing the technology battle against trafficking and exploitation?*** Chaired by Professor **Jerry Ratcliffe**, Temple University, US, the panellists included **Justine Currell**, FRSA, Unseen, **Professor Edward Kleemans**, Vrije Universiteit Amsterdam, **Jaya Chakrabarti**, MBE, TISCreport.org, **Roy McComb**, Deputy Director, National Crime Agency and **Eric Anderson**, Head of Modern Slavery Programme & Senior Consultant – Human Rights, Corporate Affairs at BT.

Teaching

Dissertation Research

In addition to PhD supervision, Centre staff supervise MSc student dissertations. In the previous academic year (summer 2018), MSc students completed research projects to include:

- Two projects, conducted in collaboration with ECPAT and *Missing Children*, to estimate the number of children in care who are trafficked. The findings of this work were published in the report *Still in Harms Way,* available at: **www.ecpat.org.uk/still-in-harms-way**
- The use of Drones in domestic burglary
- The theft of keyless vehicles

Security Technologies

Our Security Technologies undergraduate module introduces students to the field of security technology and educates them in the fundamental scientific principles and processes, and associated mathematics underlying the operation of key domestic security technologies. These technologies include camera and video analytics; radio-frequency and biometric sensors; as well as X-ray scanners and other systems used for screening and threat detection. Students are also introduced to the concept of horizon scanning. This year's students produced horizon scanning papers on topics that included smart cities, drones, and smart dust.

As part of the Security Technologies module, the undergraduate students present a poster about the findings from a Horizon Scan. The Home Office hosted this year's poster event in Westminster, on Friday 30th November 2018. The event was so well received that it will be repeated next year

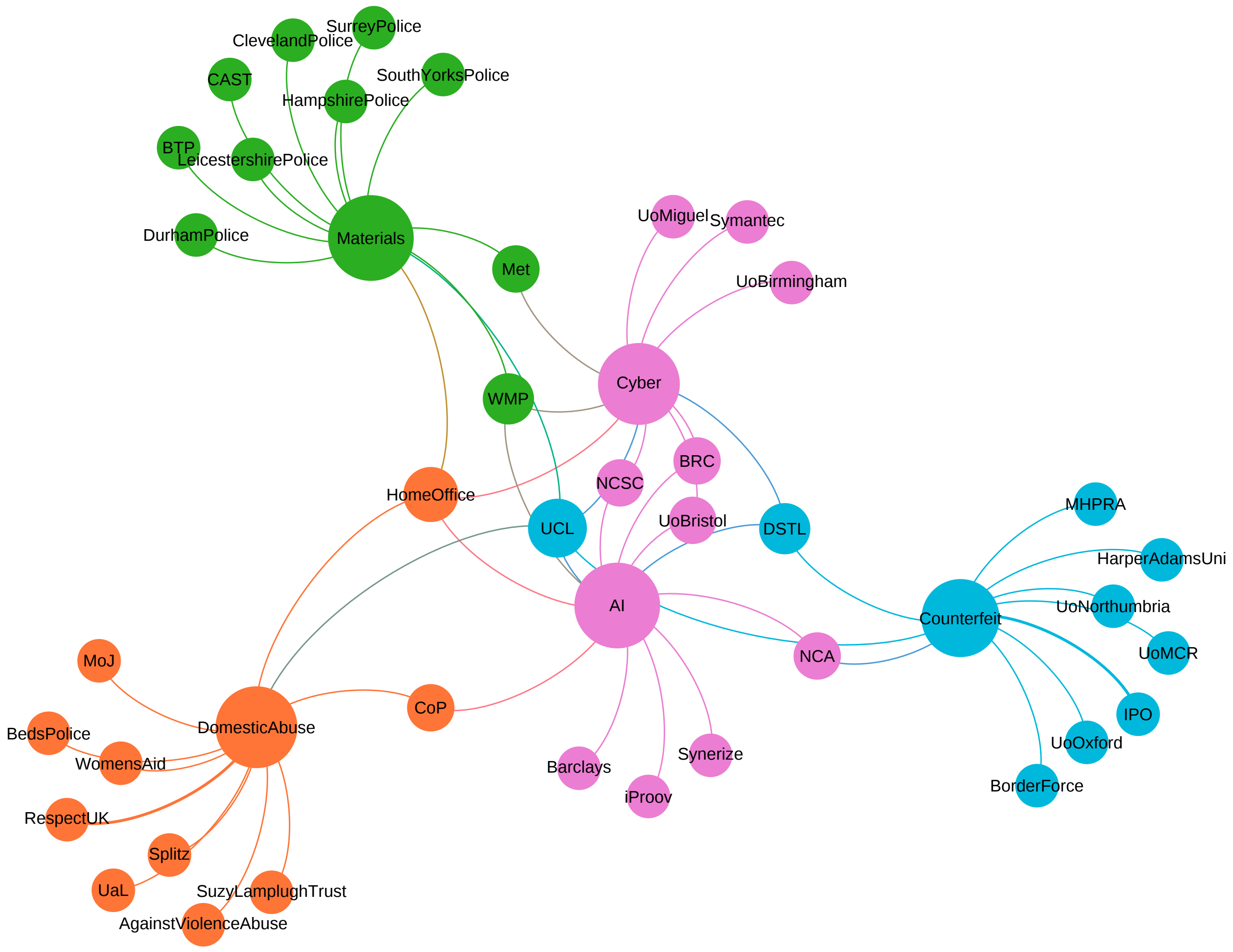
Horizon Scanning module

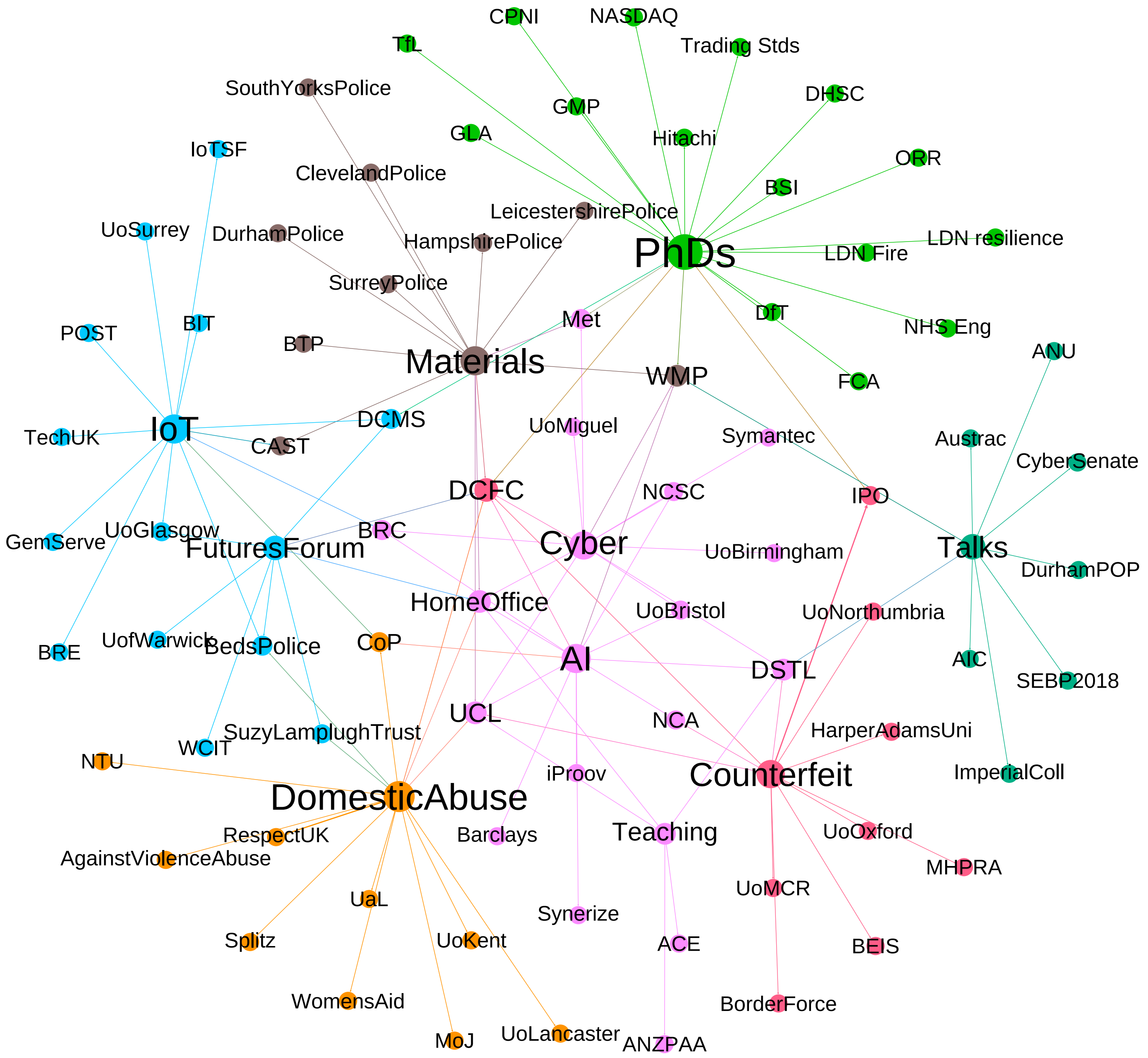
In the second term of the 2018/2019 academic year, we launched a new postgraduate module concerned with horizon scanning. This module considered the changing nature of crime. It begins with a discussion of how crime has evolved over time and the arms race in which offenders, law enforcement and others have been historically engaged. Cycles of innovation and how these might lead to new crime opportunities are considered, as is the role of industry and other players in designing out crime. Methods of horizon scanning and associated methodologies are discussed in general, followed by a focus on how such techniques can be applied in the context of crime, in particular. 17 students enrolled on this module in the 2018-2019 academic year, with additional students sitting in on the lectures. These students are due to present posters of their MSc work at our 2019 annual conference, at the Royal Society, with 200+ academics and police and law enforcement practitioners in attendance, including the Met Police Commisioner and numerous senior police officers from around the country interested in evidence-based policing.

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. The figure below summarises the organisations who have contributed to the scoping studies discussed above, including that on reducing domestic abuse. It provides an indication of the variety of organisations with whom we are working and illustrates the fact that some of those organisations are contributing to many or all of these projects.




CPNI
NASDAQ
TfL
Trading Stds
SouthYorksPolice
GMP
DHSC
GLA
IoTSF
Hitachi
ORR
ClevelandPolice
BSI
LeicestershirePolice
UoSurrey
DurhamPolice
HampshirePolice
LDN resilience
PhDs
LDN Fire
SurreyPolice
DfT
Met
NHS Eng
POST
BIT
BTP
ANU
Materials
WMP
FCA
DCMS
TechUK
IoT
UoMiguel
Symantec
CAST
Austrac
CyberSenate
DCFC
NCSC
IPO
GemServe
UoGlasgow
BRC
Cyber
UoBirmingham
FuturesForum
Talks
DurhamPOP
HomeOffice
UoBristol
UoNorthumbria
BRE
UofWarwick
BedsPolice
CoP
AI
AIC
DSTL
SEBP2018
UCL
NCA
HarperAdamsUni
SuzyLamplughTrust
NTU
WCIT
iProov
Counterfeit
ImperialColl
DomesticAbuse
RespectUK
Barclays
Teaching
UoOxford
AgainstViolenceAbuse
MHPRA
UoMCR
UaL
Synerize
Splitz
UoKent
ACE
BEIS
WomensAid
BorderForce
MoJ
UoLancaster
ANZPAA

166
82
48
90
100
110
120
130
140
150

Conclusion

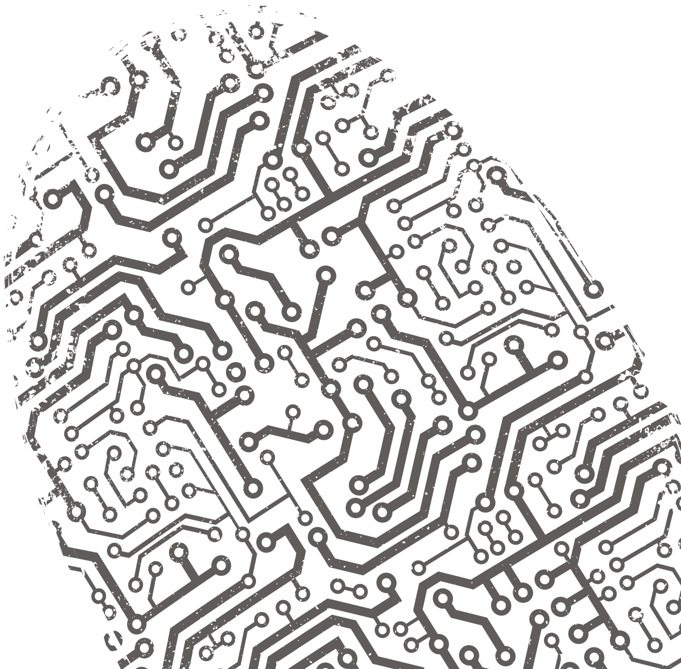
We have had a productive year. A number of exciting new projects have commenced while existing projects have been completed or progressed towards completion. We now have a strong cohort of PhD students on board providing a longer-term research capacity in key areas of interest. A particular highlight has been the sandpit workshops that took place this year. These were particularly fruitful in bringing together a wide array of practitioners working at the 'coalface' to engage with Dawes funded research.

The outcomes of those sandpits have helped shaped not only the projects, but also our wider thinking on the subject matter. Through these sandpits and other outreach activities we have strengthened our relationships with key partners and forged new links between them and us. Our profile has steadily risen and we intend to use this to help enable impact once publications and reports begin to roll out from the Centre. On this front we are delighted that some impact is already being felt from our work. For instance, research from our project on domestic IOT devices is informing DCMS policy on how to secure the Consumer Internet of Things (IoT), which has implications both for manufacturers and consumers.

We have also increased our staff capacity – a new lecturer in data science joined the team in September 2018 and will help to build our portfolio in this growing area of research, exploring how techniques such as machine learning can inform our understanding of new and emerging crime threats and how to combat them. The department has also appointed two new lecturers in cybersecurity, whose work will very much contribute to the agenda of the centre.

Finally, 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 will launch in September 2019 and provides funding for an additional 55 PhD students. Online offending is rapidly increasing in both scale and variety and hence this funding will help us to develop capacity in areas where there is clear current and future need. Through our role in directing this new CDT, we will also be able to train a new generation of scientists to think about the potential future crime consequences of their work, as well as how to secure the internet from existing threats.

Technological progress marches on. We move ever closer to autonomous vehicles on our transport networks; artificial intelligence continues to evolve at a staggering rate, and we are witnessing an increase in the use of cryptocurrencies. Law enforcement agencies around the world are working determinedly to tackle the crime and security implications of these changes. This is where the Dawes Centre has such a vital role to play. By positioning ourselves as a leading research organisation in this brave new world we are ideally placed to help. There is much to look forward to in the coming year.



Publications

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

Blythe, J., & Johnson, S.D. (2018). The Consumer Security Index for IoT: A protocol for developing an index to improve consumer decision making and to incentivize greater security provision in IoT devices. *In proceedings of the Living in the Internet of Things: Cybersecurity of the IoT Conference. IET. London, UK.*

Blythe, J., & Johnson, S.D. (2018). *Rapid Evidence Assessment on Labelling Schemes and Implications for Consumer IoT Security.* London: DCMS. (NOTE: This document can also be found on the GOV.UK website as part of the Government's Code of Practice for Consumer Internet of Things (IoT) Security for manufacturers, with guidance for consumers on smart devices at home: **www.gov.uk/government/publications/rapid-evidence-assessment-on-labelling-schemes-for-iot-security**

Johnson, S.D., Ekblom, P., Laycock, G., Frith, M.J., Sombatraung, N., Valdez, E.R. (2019). *Future Crime.* In R. Wortley, Sidebottom, A., Tilley, N., and Laycock, G. (Eds.). Routledge Handbook of Crime Science. Routledge.

Kamps, J., & Kleinberg, B. (2018). To the moon: defining and detecting cryptocurrency pump-and-dumps. *Crime Science*, 7(1), 18.

Reports to DCMS

Johnson, S.D., John M Blythe, Matthew Manning and Gabriel Wong (2019). The impact of IoT security labelling on consumer product choice and willingness to pay.

Blythe, J.M., Sombatruang, N., and Johnson, S.D. (2019). What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?

Blythe, J.M., Johnson, S.D., Manning, M., and Wong, G. (2019). What is security worth to consumers? Investigating Willingness to Pay for secure Internet of Things devices.

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