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 2020 – 28 February 2021

Contents

Executive Summary

Professor Shane Johnson, Director

The past year has been one of the most remarkable in recent history. One of the few saving graces of the social and economic turbulence caused by the Coronovirus pandemic has been the reaffirmation of science as both a core strength and need of human society. The pandemic has also highlighted the need to continue to innovate and to horizon scan for threats that might impact society in the near to long term future.

In spite of the challenges, this period has been a productive one for the Dawes Centre. The Centre has seen a number of projects not only come to fruition, but gain traction in the 'real' world, raising the Centre's profile and generating impact and discussion among stakeholders. From newspaper headlines to an appearance on BBC's Countryfile show, the Centre's research has created talking points and encouraged engagement with stakeholders. Information about these can be found in the ***Policy Briefings, Impact and Wider Dissemination*** section. Links to the latest academic papers from the Centre can be found in the ***Research Publications*** section, covering such diverse topics as security in smart cities, policing disruption and mobilisation through Twitter, and the criminogenic potential of synthetic biology.

A particular highlight was a series of seminars organised by the Centre with the UK Home Office. The seminars were well attended and the appreciation expressed afterwards for helping the policy community to understand some of the issues around emerging crimes has been a testament to the Centre's ethos. Further information is available in the ***External Engagement*** section.

Despite lab closures and remote working, the Centre has continued to progress current projects and begin new ones. There is more information on these inside. Engagement with academics, practitioners, and other stakeholders continues to grow, though, during this reporting period, the Centre's annual conference could not be organised due to the lockdown. In 2021, again due to the ongoing effects of the pandemic, we could not organise a full scale conference, but did manage to host an online mini-conference entitled: *Cybercrime conference: fake news, legislative responses, and women in cyber*. To be kept abreast of future events please register for the Centre's mailing list by clicking here.

Professor Shane Johnson
Director

Summary of activities in the reporting period

In terms of activities, over the past year the Centre can report the following:

1 Completed projects

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

2 Current projects

SIX projects are ongoing, covering topics ranging from smart technology and domestic violence to looking at cybercrime targeted at the older generation.

3 PhD projects

EIGHT new PhD students were recruited, carrying out doctoral research in topics ranging from how technology has impacted human trafficking to Brexit and crime.

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

In the coming period, the first cohort of PhD students will graduate, hopefully taking up meaningful employment and continuing to contribute to the Centre's agenda. Funding partnerships with the private and public sector are critical to the Centre's work. Do get in touch if this is of interest.

Note: 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 2020 to 28 February 2021. 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 fourth full year of activity of the centre.

Aims of 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.

Our research anticipates how technological, social or environmental change might create new opportunities for offending, or have implications for how law enforcement (and others) combat crime. Our projects generally comprise two phases:

PHASE 1

Phase 1 projects review what is known about a particular technological, social or environmental issue. They establish the state of the art on a particular topic and the implications for (future) crime. They 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

Phase 2 projects involve original research intended to address a specific future crime problem, or to develop existing research to reach a technology readiness level suitable for deployment.

Mid Term Review

During this reporting period, as agreed with the Dawes Trust when the Centre was established, an independent review of the Centre was commissioned, which was carried out by Perpetuity Research. The review highlighted areas that we might address and areas in which we have performed at or beyond expectations.

The report remarked positively upon the strength of the Centre leadership and team, on the value achieved by projects that have been funded, on our engagement with stakeholders, and on the strengths of being part of an institution such as UCL.

The report suggested that areas that might be improved upon include the need for additional capacity to support the Centre Director to prevent delays in initiating new projects, and a guiding strategy document to inform the overall work of the Centre. Both these points are currently being addressed and the recommendations more generally will help us to build further upon our successes to date.

The Centre is grateful to Professor Martin Gill of Perpetuity Research for his thorough and helpful review.

1 Research highlights: Completed projects

AI-enabled Future Crime

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, for instance, by enabling identity forgery, AI snooping, and driverless weapons.

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.

As part of this project a sandpit event was held and attended by 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.

Key findings: This study identified 20 applications of AI and related technologies which could be used for crime now or in the future. Six crimes were identified as most concerning: audio and video impersonation, driverless vehicles as weapons, tailored phishing, disrupting AI-controlled systems, large-scale blackmail and AI-authored fake news.

The results of this work featured in an academic publication and a downloadable policy briefing, both of which achieved widespread interest and media coverage. Further detail about these can be found later in this report. Two PhD students are working on projects that evolved from this project.

Lead Investigator
Prof Lewis Griffin
UCL Security and Crime Science

NOTE: Neither of the faces shown above are of real people. Both were generated by generative adversarial networks (see, https://thispersondoesnotexist.com).

How secure is consumer IoT?*

Internet enabled devices, including smart televisions, security cameras and thermostats, are now commonly found around the home. Such devices have enormous potential to transform society, but 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, can they discover the security of devices prior to their purchase? 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 to examine the potential effectiveness of consumer labels in incentivising manufacturers to improve IoT device security, and to help consumers purchase more secure devices.

The results of this work featured in a downloadable policy briefing.

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

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
- large experiment of the effects of different labelling schemes on consumer choice, their willingness to pay for enhanced security, and how they interpret labels

Key findings: This research identified the variety of crimes associated with the consumer 'Internet of Things' (IoT) which include online offences such as denial of service, but also more "traditional" crimes such as stalking, and domestic burglary. It found that at the point of purchase, consumers are provided with little information to help them assess the security of devices – for example, for none of the devices reviewed was information provided about the period over which security updates would be provided. Our findings showed that consumers would be willing to pay for security and that labelling schemes positively affect consumer decision making in purchasing scenarios.

By working with DCMS, this research has and continues to inform policy. This work is discussed in detail in DCMS reports published 2018-2021 to motivate the need for government intervention and the potential benefits of consumer labelling schemes. Most recently, it was discussed in relation to, and as motivating, new cybersecurity laws planned by the UK Government. 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, and discussed in a Parliamentary Office for Science and Technology briefing.

Lead investigators
Prof Shane Johnson
Dr John Blythe
UCL Security and Crime Science

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. This lack of regulation, combined with their technical complexity and market volatility, makes them an attractive target for fraudulent activity.

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.

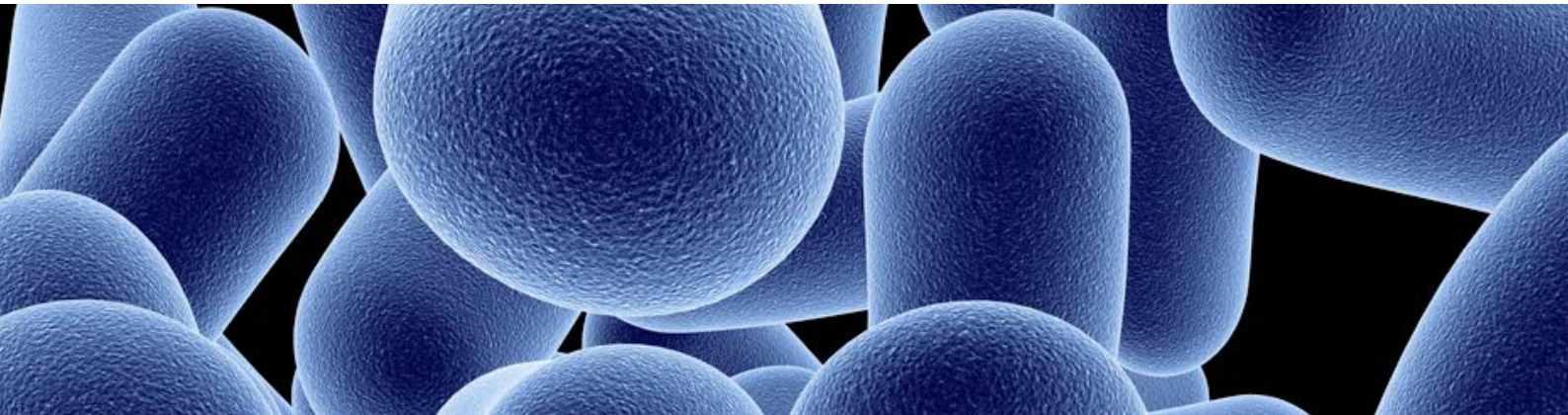
Key findings: This study identified seven cryptocurrency-based crimes which could be achieved now or in the future and ranked them in relation to the level of harm they can or could cause. Extortion (ransomware) and money laundering via Bitcoin ATMs were considered particularly harmful.

The results of this work featured in a downloadable policy briefing. 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 Kleinber
UCL Security and Crime Science

Research assistants
Eray Arkatuna, PhD researcher
UCL Security and Crime Science

Florian Hetzel
UCL Security and Crime Science



Smart Tagging and Proximity Detection for Crime Reduction*

Domestic abuse encompasses diverse forms of offending, both physical and psychological; addressing it involves various agencies as well as the police, and there are several different stages at which intervention could occur. These include the period before a pattern of behaviour is recognised as abuse (pre-awareness), during an ongoing pattern of abuse that is recognised as such, and the periods during and after criminal justice intervention. Provisions included in the Domestic Abuse Bill 2020 (England & Wales) will enable the police to issue immediate short-term protection notices that require offenders to stay away from victims for a 48-hour period, and to apply to the courts for protection orders that are longer in duration. It will also provide the courts with the power to use Electronic Monitoring (EM) technology to ensure that offenders comply with the requirements of orders given.

A systematic review of the costs of EM suggest that the costs are cheaper than custodial sentences but are nevertheless significant. Existing EM technologies rely on GPS or RFID, but do not currently employ what are now pervasive and relatively cheap technologies such as tagging and proximity-detection (e.g. Bluetooth Low Energy (BLE) & Ultra Wideband (UWB)). The use of proximity-detection and tagging in this context represent examples of how developing technologies could help reduce domestic abuse.

The aim of this project was to develop proof of concept interventions — that employ such technologies — intended to help reduce domestic abuse. Two workshops – attended by domain experts, designers and engineers – were held to identify possible technological solutions to problems of domestic abuse. The project aimed to explore the utility of these technologies.

Key findings: This study highlighted the richness of technological methods available for crime prevention in general and for domestic abuse support in particular. The project further identified the problems encountered by those working in intelligence, policy and crime and how technology can complement their work. The study identified prototype concepts with the most potential, as follows:

1. **Proximity Detection wearable to detect when a registered offender is in close proximity of a victim (and how close they are).**
   The research suggests substantial potential for the use of short-range communication technologies such as Bluetooth and WiFi. These technologies could be used alone or alongside current GPS monitoring to provide a more robust system that is able to detect proximity in both indoor and outdoor environments.
2. **NFC alert and information access framework**
   Near Field Communication technology in the form of smart tags embedded into everyday objects could be employed to trigger the collection of evidence, as a means of emergency reporting, or of accessing information. Several apps exist to report emergency situations and collect evidence but they commonly require the user to open the app and perform a specific action. NFC technology could be used in combination with such apps to make their use more subtle.

These prototypes are currently being trialled with the Met Police.

As an additional output, the wider implications of these technologies were explored in the context of reducing vulnerability in the COVID-19 pandemic. This research was featured in an academic paper entitled A COVID-19-Based Modified Epidemiological Model and Technological Approaches to Help Vulnerable Individuals Emerge from the Lockdown in the UK

Lead investigator
Dr Eiman Kanjo
Nottingham Trent University

Research assistant
Dario Ortega Anderez
Nottingham Trent University

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

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 from malicious attacks to those motivated by financial gain. As more and more services go online, the problem is likely to increase. Cybercrime differs from traditional urban crime in a number of 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. This research aimed 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.

As part of this project a sandpit event was held and attended by 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.

Key findings: This research argued that it would be beneficial for the information security community to look at the theories and systematic frameworks developed in environmental criminology to develop better mitigations against cybercrime.

The results of this work featured in a downloadable academic paper entitled 'Bridging Information Security and Environmental Criminology Research to Better Mitigate Cybercrime'. In this paper, the project researchers provide an overview of the research from environmental criminology and how it has been applied to cybercrime. They then survey some of the research proposed in the information security domain, drawing explicit parallels between the proposed mitigations and environmental criminology theories, and presenting some examples of new mitigations against cybercrime. Finally, they discuss the concept of cyberplaces and propose a framework in order to define them.

Further work has also been proposed including: 'mapping' disinformation, a 'digital breathalyser' based on profiling routine activities online, and the disruption of criminal business models via spoofing of criminal behaviour. The latter is currently being developed.

Additionally, a Dawes-funded PhD student, Octavian Bordeneau, is working on research related to this project. The findings till date of that research are as follows:

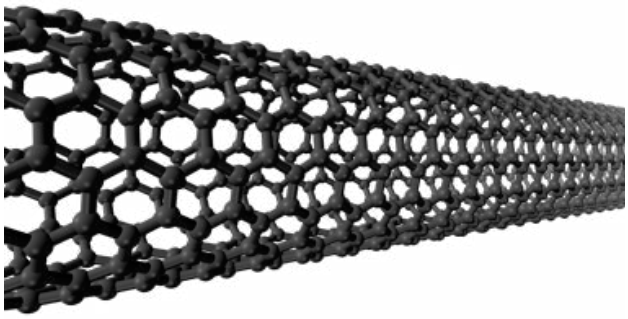
This project sought to explore whether cybercrime could be understood through the lens of environmental criminology, particularly by drawing analogies between cyber space and physical space. A review of existing literature suggested that several types of cybercrime could be framed in this way; however, it was also apparent that no single model of cyberspace was appropriate for all crime types. In particular, concepts such as place, distance and size differ depending on the type of cybercrime being investigated. Because of this, in this project, space was framed in a purely abstract way, determined solely by the properties of the data. This approach has been applied in a number of ways.

For example, a system – known as JABBIC (judge a book by its cover) lookups – has been proposed for assessing the risk of potential malware samples. The key principle of this approach is to project known samples into space in such a way that those with similar characteristics appear nearby. When a suspicious unknown file is subsequently received, it can be projected in the same way and classified according to which known files appear nearby; this results in improved detection of malware. In another aspect of the research, an exploratory analysis of the Mirai botnet attacks against Internet of Things devices was conducted. Using a similar 'embedding' approach, it was shown that attack behaviour displayed signs of coordination, with payloads often being delivered from different sources to those that initiate attacks; this is an aspect of the behaviour of the botnet that had not previously been identified.

Lead investigators
Dr Toby Davies
UCL Security and Crime Science,
Dr Gianlucca Stringhini
UCL Computer Science

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.



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 attended by representatives from academia, British Transport Police (BTP), the Home Office, and from Durham, Hampshire, and West Midlands constabularies took part. The event served to identify potential research areas and application of materials science in crime prevention. 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.

Key findings: This project provided a detailed summary of the nature of various advanced materials and how they are currently being used to combat crime, the limitations of these materials in terms of their performance and applications, and the future emergence of new advanced materials to open up new possibilities in the field. The project further identified some of the most important problems that might be addressed using advanced materials.

A policy briefing will be published in due course from this work.

This research has been extended via a PhD project on “Intelligent Biomaterials for the Development of High-performance Label Free Biosensors to Combat Crime”.

Lead investigator
Prof Kwang-Leong Choy
UCL Institute for Materials Discovery

2 Research highlights: Current projects

Reducing the Unanticipated Crime Harms of Covid-19 Policies

Covid-19 and related policies are changing the nature and distribution of crime in various ways. Lockdowns restrict movements and change everyday interactions that can produce crime. Crime such as burglary are likely to decline as people stay home (increasing guardianship) and commercial premises close. Public assaults and disorder may also decline with pub and entertainment district closures. However, greater time spent at home can be expected to provide increased interactions that lead to rises in other forms of crime. For example, fraud, in-person, via text, email and online, may increase because the pandemic offers a new set of 'conversation starters' for fraudsters, while remote working and online leisure activities provide more potential targets for online victimisation of various types. The restrictions associated with the lockdown also change the way the police can interact with the public, presenting both challenges and opportunities.

Working with a range of stakeholders to include the National Police Chief's Council, Neighbourhood Watch and the City of London Police, the research is quantifying these patterns and trends, identifying new and emerging crimes, examining police use of social media, and will combine lessons from cross-national comparative research. The overall aim is to identify lessons for policy and practice that reduce the harm from crime related to the policing of pandemics and other future disruptions.

Findings from our analysis of police use of Twitter during the pandemic can be found here, findings regarding the impact of covid-19 policies on urban crime can be found here, and findings regarding the impact of the pandemic on online fraud will be published in due course.

Lead investigators
Dr Dan Birks
University of Leeds

Prof Kate Bowers
UCL Security and Crime Science

Prof Graham Farrell
University of Leeds

Prof Shane Johnson
UCL Security and Crime Science

Prof Nicolas Malleson
University of Leeds

Prof Nick Tilley
UCL Security and Crime Science

Research Associates
Dr Michael Frith
UCL Security and Crime Science

Dr Manja Nikolovska
UCL Security and Crime Science

PITCHR: Prevention of IoT-enabled Crime using Home Routers

The home router is taking on increased importance as homes become smarter. Having traditionally been the point of entry for home users to access email and web services through a desktop computer, they are now becoming the entry point for a myriad of Internet-connected devices. These include smart assistants (eg Amazon Echo and Google Home), smart wearables (eg Fitbit), smart security (eg Ring and baby monitors), smart appliances (eg smart kettles, fridges and washing machines), smart energy (eg Nest and smart plugs) and many more. As shown in our project about the IoT (see above), this connectivity creates substantial new opportunities for crime.

Internet Service Providers (ISPs) are the organisations that provide consumers and businesses with services to access, use, or participate in the Internet. The question arises as to whether ISPs, through router intelligence, could play a substantive role in recognising threats and denying the traffic egress. If ISPs can combine central cyber intelligence and situational awareness with that at the edge, there is a huge potential to prevent and mitigate these forms of cyber crime.

This project aims to:

- To understand the perceived role of ISPs in preventing attacks using household consumer IoT – this will allow us to establish reasonable responsibility and expectations of ISPs
- To understand the role of manufacturers of home routers – this will allow us to understand whether there should be a minimum role played by manufacturers, in the way new expectations of device manufacturers have arisen
- To understand the cost implications of router-based defence systems – this will help inform recommendations for ISPs and manufacturers, since customers are price sensitive
- To understand the impact on, and benefits for, citizens – to enable a cost-benefit analysis
- To understand the current research landscape in the area

In 2020, the project delivered three workshops with 42 participants representing service providers, citizens' groups, and manufacturers. Through these workshops ten emergent themes were identified in home routers' security, ranging from socio-technical ramifications to legal and regulatory specificities. A further workshop was held with participants, to present and validate findings. Consensus was reached on security requirements lacking emphasis on the security-by-design principle and the necessity to share threat intelligence between different ISPs and manufacturers. The team is now preparing academic and industrial papers.

Lead investigators
Prof Carsten Maple
Professor of Cyber Systems
Engineering at the University of Warwick's
Cyber Security Centre (CSC)

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. 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 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 England, Scotland and Wales for Age UK found that over half (53 per cent) of people aged 65+ believe they have been targeted by fraudsters.

This project responds to the All Party Parliamentary Group (APPG) call for research to "better understand links between vulnerability and exploitation"; and built on a previous qualitative study by the team on cybercrime in Mumbai (J Elder Abuse Negl 2019;31(4-5):437-447).

To date, the team have conducted a realist review to find out how, why and in what circumstances older adults are cybercrime victims. They identified and synthesised findings from 24 primary research studies. They found a dearth of quantitative evidence regarding trends in cybercrime against older people, though in one Australian study, its prevalence was increasing. Relevant vulnerability factors included cognitive impairment, isolation and computer inexperience. Carers support, however, was protective. Victim-blaming reduced reporting.

In November 2020, a virtual sandpit event was held with 21 experts, who offered additional insights, including the need to consider distraction caused by mental ill health/stress as a risk factor, and the potential risks (as well as protection) from carer involvement, i.e. who is watching the guardians?. Offender's lack of awareness of the impact of their crimes was also identified as a potential area for future intervention. There was a broad consensus that identity theft, credit card fraud and romance scams were the most serious crimes. While identity theft and credit card fraud were seen as crimes that could be prevented, romance scams were identified as a crime that was hard to defeat because of multiple factors including the reluctance of the victims to report their victimisation. Special security measures by banks to prevent online victimisation of older people, use of AI to track suspicious transactions, option of recalling online payments for older people and increasing awareness about scams were considered effective measures of intervention. The experts also agreed that interventions that increase awareness of specific risk factors for cybercrime among older adults are needed, alongside targeted campaigns aimed at improving wider societal attitudes towards cybercrime and older people more broadly.

Findings will be published soon, with an associated press release discussing implications for the Online Safety Bill. The team have also developed a proposal for a doctoral fellowship within the Dawes Centre to take these findings forward and are in the process of appointing to it.

Lead investigators:
Professor Claudia Cooper
UCL Division of Psychiatry
Dr Kartikeya Tripathi
UCL Security and Crime Science

Research Associate(s):
Alexandra Burton
UCL Division of Psychiatry

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. For example, recent estimates 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, onsite testing might be the best opportunity to ensure fake agrochemicals are not used.

This project explores suitable technologies that could fit into a miniaturised system to identify counterfeit agrochemicals. Technologies that could be applied at the point of distribution or application are being explored and concepts for end-user devices investigated.

To date, a list of candidate agrochemicals that are typical targets for exploitation has been established. This list was compiled in consultation with experts at Harper Adams University. Commercially available examples were purchased and a test set created by altering the chemical composition in a way that mimics criminal methods (e.g. by dilution with water). Different technologies have been investigated for the testing system. Some of these were standard analytical laboratory instruments which could provide the ‘gold standard’, while others are research-based instruments, but have the genuine possibility of being miniaturised.

Findings from this work are due to be published in the second half of 2021.

Lead investigators
Dr Rob Moss
UCL Dept of Medical Physics & Biomedical Engineering

Prof Rob Speller
UCL Dept of Medical Physics & Biomedical Engineering

Research Assistant
Dr J.C. Khong
UCL 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. 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. As a first step, a systematic review of the literature – which can be found here – was conducted. This informed the development of a prototype modelling platform to explore these dynamics, to simulate 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 Security and Crime Science

Prof Alison Heppenstall,
University of Leeds

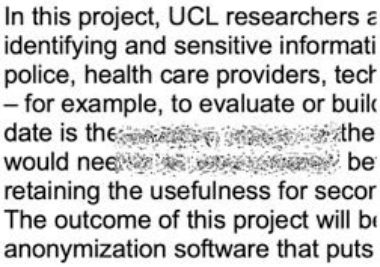
Prof Shane Johnson
UCL Security and Crime Science

Prof Ken Pease
University of Derby

UCL Researchers
Dr Michael Frith
Dr Eon Kim
Julian Laufs
UCL Security and Crime Science

*This project is being led by the University of Leeds and is funded by the Alan Turing Institute.

Textwash


In this project, UCL researchers a
identifying and sensitive informati
police, health care providers, tech
– for example, to evaluate or build
date is the [redacted] the
would nee[redacted] be
retaining the usefulness for secor
The outcome of this project will b
anonymization software that puts

For this project, UCL researchers have developed 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. Textwash is supported by a proof-of-concept grant from SAGE.

The system has now been validated in empirical studies and has received attention from stakeholders from industry and academia and is included in a European Commission consultation round on best practices for automated text anonymisation. The project will be continued as an open-source software project. A webinar provisionally scheduled for the second half of 2021 will launch the user-facing side of the tool to the public.
The webinar will be organised by Sage.

Lead investigators
Dr Toby Davies
UCL Security and Crime Science

Dr Bennett Kleinberg
UCL Security and Crime Science

Maximilian Mozes
UCL Security and Crime Science

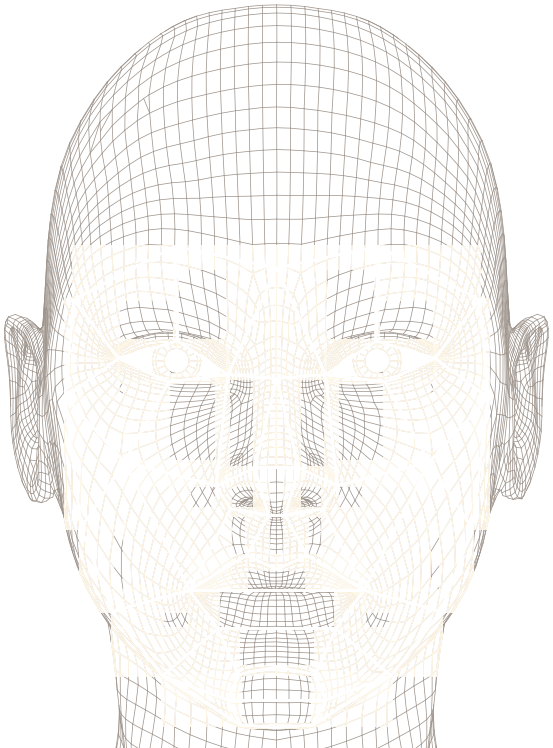
Note: Information about the project Challenges of preventing counterfeit goods, completed previously, can be found on our website.

3 Research highlights: PhD projects

The Dawes Centre funds a range of PhD projects covering an array of topics relevant to our agenda. There are currently 24 students on our programme, with 5 of these being part of the new CDT in Cybersecurity, which is a collaboration between the departments of Security and Crime Science, Computer Science, and STEaPP. The PhD projects that began during the current reporting period are described below:

Intelligent biomaterials for the development of high-performance label free biosensors to combat crime

In criminal investigations (street samples, biological fluids, gunshot residues, etc.) efficient and accurate methods are needed for detection and analysis of evidence. The crime scene offers many analytical challenges due to its complexity and therefore requires the use of a variety of techniques to assess evidence. Current technologies have issues of low specificity, detrimental effects on evidence recovery and an inability to be performed simultaneously. Biosensors can be applied in the detection of biomolecules and biological components (fingerprints, blood samples, odours etc.) found at crime scenes, which can aid in the identification and tracking of suspects. The application of biosensors represents a significant advancement for forensic sciences with the opportunity for untrained individuals in the field to carry out economic, rapid and decentralised testing of complex samples.



The recent rapid development in the research and development of biosensors is due mainly to advances in nanomaterial-based biosensors with advantages of rapid response time, high stability, superior biocompatibility and low cost. Despite the demonstrated versatility of design and usefulness in their potential for analysis of biological fluids and multiplexed determinations, biosensors in forensic analysis are less advanced than in other fields.

This project aims to explore this lack of positive identification and on-site testing by improving the application of biosensors, and their current vast development in other sectors, to forensics. A systematic review of current technologies and their potential for combating crime is currently be undertaken. These findings and further discussions with police forces and other stakeholders will determine appropriate biosensing technologies for further development. The overall aim of the project is the fabrication of a field-deployable biosensing device to combat crime.

PhD start year: 2020

PhD student: **Alice Cozens**

PhD supervisors:

Prof Kwang-Leong Choy, UCL Institute of Materials and **Prof Shane Johnson**, UCL Security and Crime Science

Contact: **alice.cozens.20@ucl.ac.uk**

Hybrid Threats

The nature of the international security environment is changing in the light of hybrid challenges. Although the concept of hybrid threats is not new, it has recently gained wider traction among Western countries due to the foreign interventions in Ukraine in 2014 and during the 2016 United States presidential election. The evolution of hybrid threats has been driven by the rise of the cyber domain and online information spaces. The potential deployment of cyberattacks against the target and the use of social networking services to conduct influencing activities are important attack methods for hybrid threats.

Since 2016, NATO and the European Union have decided that countering hybrid threats is a priority for cooperation. An important goal for the world's governments and international agencies is to respond to hybrid threats. Deciding on the appropriate and proportional response is difficult due to the complexity of the concept and underdeveloped methods for assessing the impact of hybrid threats. The aim of the research is to propose a method that helps to quantify the impact of hybrid threats. The results of the research will provide empirical basis for justifying response decisions and important contributions to the sparse body of existing literature.

PhD start year: 2020

PhD student: **Kärt Padur**

PhD supervisors: **Prof Stephen Hailes**, UCL Computer Science and **Dr Herve Borrion,** UCL Security and Crime Science

Contact: **kart.padur.20@ucl.ac.uk**

Automated profiling of user vulnerabilities to online deception and intervening through dynamic user interfaces

Smartphones and laptops play increasingly essential roles in many people's daily lives. Studies find that the average adult in developed areas spends at least 4 hours every day looking at a screen. This makes online deceptions such as phishing and disinformation on social media increasingly attractive means for cybercriminals. Such attacks prove to be effective since they are easy to scale and cybercriminals can more easily hide their true identities from local law enforcers. A big phishing attack in 2015 for instance defrauded Facebook and Google for millions of dollars. Hence, it is important to understand why individuals fall for online deceptions and what individual differences and contextual factors may make certain people more vulnerable than others.

The aim of this research is to test if computers can be trained to automatically detect when individuals are particularly susceptible to online deceptions. If so, the goal is to develop interactive user interfaces that help to shield people from falling for such frauds, by dynamically changing the appearance of online environments. To this end, the research employs an eclectic mix of psychophysiological methods, web application development and machine learning.

PhD start year: 2020

PhD student: **Sarah Zheng**

PhD supervisors: **Prof Tali Sharot**, UCL Experimental Psychology and **Dr Ingolf Becker**, UCL Security and Crime Science

Contact: **sarah.zheng.16@ucl.ac.uk**

Human trafficking, digitalisation and a global pandemic: how has technology changed the face of human trafficking?

The global pandemic has impacted on society in numerous ways. The economic crisis, coupled with widespread physical and mental health impacts, has created an environment of heightened vulnerability for many groups. In particular, law enforcement agencies and charities around the UK have highlighted the effect on younger, vulnerable individuals suffering from increased feelings of isolation.

This PhD research aims to examine how human traffickers are taking advantage of this situation to target such vulnerable individuals. The project aims to discover whether and how criminal enterprises are utilising technology in new and more sophisticated ways to pursue this activity. By focusing on the modus operandi of traffickers, their psychological manipulation techniques, and the way they engage with technology, this research aims to look at how criminal digital interaction occurs from an offender's point of view.

PhD start year: 2020

PhD student: **Francesca Costi**

PhD supervisors: **Professor Kate Bowers** and **Dr Sanaz Zolghadriha**, UCL Security and Crime Science

Contact: **francesca.costi.19@ucl.ac.uk**

Deterring Criminal and Terrorist Planning

Smart cities take the principles of smart devices and apply them at scale to make cities more efficient and sustainable. This promise of efficiency means some environments may become increasingly automated and rely less on the physical presence of security guards and place managers. Research shows guardianship, including formal and natural surveillance, plays a clear role in the disruption of offending and is key to preventing crimes like hostile reconnaissance. Smart cities will generate potential opportunities for crime, but also generate disruption opportunities. This project seeks to understand the affordances and potential detriments a move toward smart cities has on criminal and terrorist attack planning (including hostile reconnaissance) and targeting. For example, place managers, such as bus drivers, parking lot attendants, train conductors and others, perform a surveillance function by virtue of their position of employment. Place managers may prevent crime because potential offenders are deterred by their increased subjective probability of being detected. These forms of surveillance may also increase the true probability of detection. If the amount of place managers declines, how can this role be incorporated into smart systems?

PhD start year: 2020

PhD student: **Phillip Doherty**

PhD supervisors: **Dr Paul Gill** and **Dr Sanaz Zolghadriha**, UCL Security and Crime Science

Contact: **philip.doherty.16@ucl.ac.uk**

Project Terabytes; The role of social media intelligence in organised crime investigations involving child criminal exploitation

This project seeks to outline the imperative for further research, on the evidential opportunities innate to social media usage by young persons engaged in organised criminal conduct. The phenomena of county line gangs (CLG) has received significant media attention. However, the criminal investigation techniques deployed by practitioners have undergone less public scrutiny. Social media intelligence, also known as internet intelligence investigations (III), is the operational tactic used by law enforcement organisations (LEO) to collect evidence from suspects and victims in a wide range of criminal investigations. This is a crucial intelligence development tool for organised crime investigations involving child criminal exploitation (CCE). Due to the pertinence of online dependence on communication and social networking for all young persons, which also encompasses county line gangs. Internet Intelligence & Investigations will be examined as a distinct form of digital forensic evidence that will be a key technique in the effective enforcement and disruption of internet enabled crime perpetuated through existent and emerging social networking sites.

PhD start year: 2020

PhD student: **Kane Brooks**

PhD supervisors: **Professor Kate Bowers** and **Dr Sanaz Zolghadriha**, UCL Security and Crime Science

Contact: **kane.brooks.20@ucl.ac.uk**

Take Back Control: Data Democracy with a Pro-Consumer Bias

High-profile scandals, data breaches, and daily cookie consent notices, have gradually raised the public's awareness to the potential use and misuse of their personal data. Data is the new oil and Big Data has created Big Tech and new business models. Privacy and data protection are important because the continued growth of the internet is predicated on a business model that harvests consumers' data to generate targeted advertising revenue that in turn funds the growth of the information industry. This research examines the intersection of technology, business, and public policy into how Big Tech can better accommodate consumer's privacy concerns in a win-win model.

PhD start year: 2020

PhD student: **Gerard Buckley**

PhD supervisors: **Dr Ingolf Becker**, Security and Crime Science; **Dr Tristan Caulfield**, Computer Science

Contact: **gerard.buckley.18@ucl.ac.uk**

Brexit and Crime

Brexit marks the first time in history that a state has withdrawn its membership from the European Union. This has presented one of the most important political rearrangements on the European scene since the fall of the Berlin Wall. While debates regarding the impact of Brexit on economic issues took the centre stage during the lead up to the Brexit referendum as well as during the withdrawal process, much less attention was paid to its impact on crime and security. At a time when major serious crimes are increasingly transnational in scope, the UK will face limited access to the EU's security and criminal justice infrastructure. At the same time, growing asymmetries between EU and UK laws and policies may create new criminal opportunities for serious and organised crime.

The objective of this PhD project is to create a coherent analytical product outlining alternative future crimes to guide strategic planners and decision-makers in designing robust policies capable of addressing various future scenarios and thus disrupting opportunities for criminals before they can manifest in full form. It will do so by, firstly, conducting a systematic review to examine the state-of-the-art in knowledge concerning the impact of Brexit on policing and serious crime in the UK, and secondly, by utilising foresight methodologies to identify types of opportunities for serious and organised crime which are likely to emanate from the social, political and legal changes caused by Brexit.

PhD start year: 2020/21

PhD student: **Jakub Pinter**

PhD supervisors: **Prof Shane Johnson** and **Dr Manja Nikolovska**, UCL Security and Crime Science

Contact: **jakub.pinter.20@ucl.ac.uk**

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

- 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
- Money laundering and terrorist financing future directions
- Guarding against Adversarial Perturbation in Automated Security Algorithms
- Anomaly detection for security
- Computational Analysis of Cryptoasset Fraud
- Using Machine Learning and Natural Language Processing to automatically detect cyberbullying within educational institutions in order to predict and prevent such occurrences
- Detection and Mitigation of Financial Fraud in the Cryptocurrency Space
- Protecting the UK's News propagation systems against the threat of "deepfake" injection

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

Benefits of our teaching programme

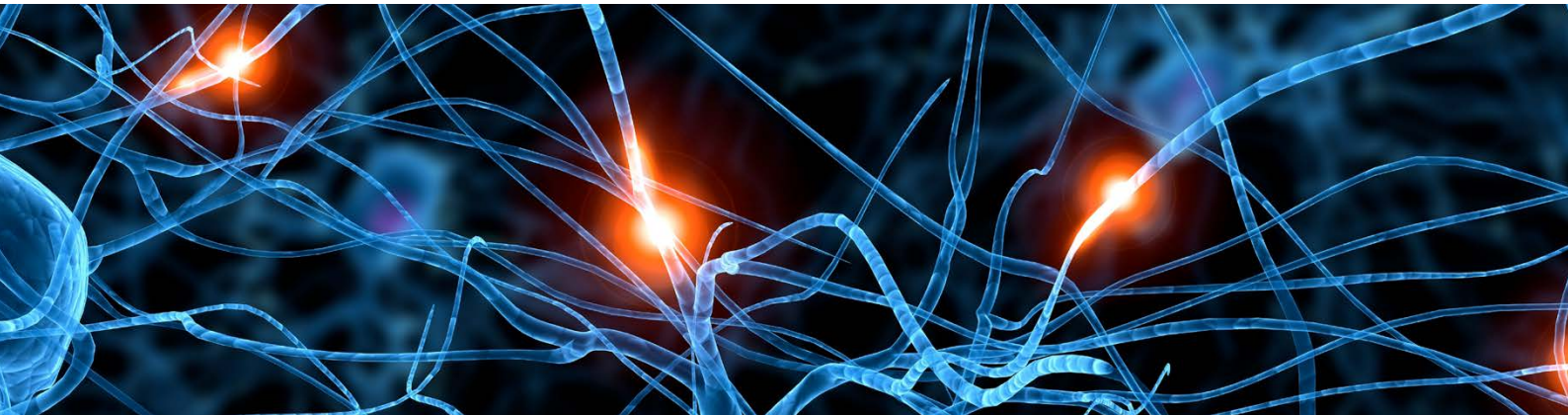
A principal benefit of the teaching modules we offer is that they facilitate the opportunity to engage, via training, a new generation of students to think about the future crime implications of technological and other changes. Furthermore, the content of our modules has helped to reinforce external relationships. For instance, for one of our modules, students produce horizon scanning posters which are presented annually at the Home Office. This year, the event was held online, and despite the disruption was very well attended.

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 ourselves as leaders in this intellectual space. The course has proved extremely popular and lays the foundation for incorporating the futures dimension in all aspects of crime science.

Some of the topics that students have produced horizon scanning reports on include the threats associated with climate change, autonomous vehicles, Hyperloop, and 4D printing.

PhD teaching

Our PhD teaching encompasses doctoral students funded directly by the Dawes Centre and those funded as part of our partnership with the CDT in Cybersecurity (co-directed by Professor Johnson), a collaboration between the departments of Security and Crime Science, Computer Science, and STEaPP. 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' systematic reviews of the literature. 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.

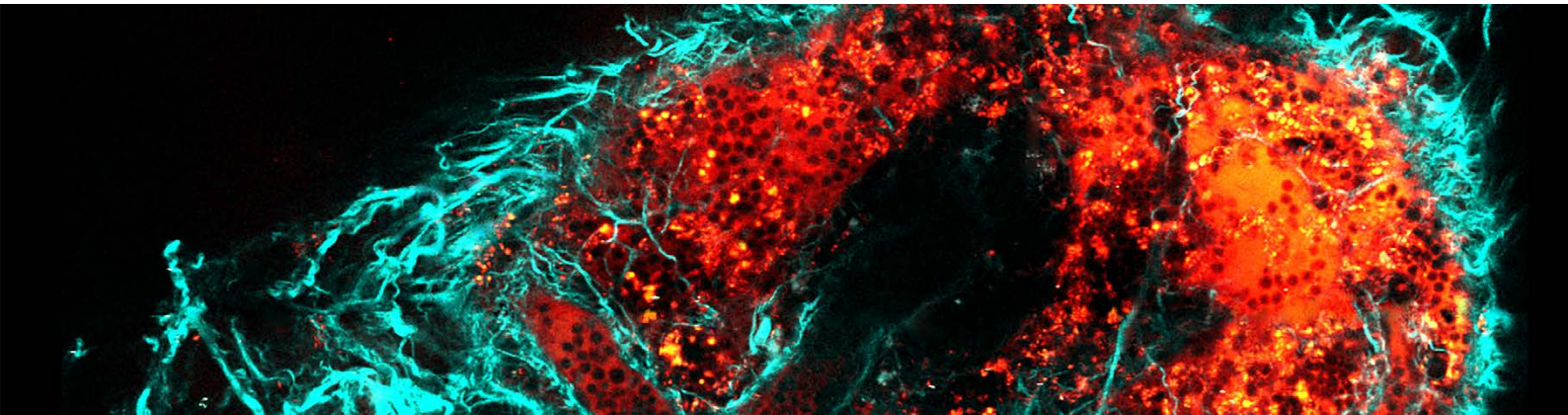


External engagement

Engagement with other research centres and agencies helps us better understand current initiatives in the future crime problems space and opportunities for collaboration.

Engagement activities include our stakeholder “sandpits” workshops, which are conducted as part of our scoping studies, stakeholder involvement in research projects, guest lectures on our taught programmes, and input to PhD research.

A particularly fruitful activity that we recently conducted has been a series of special events that we hosted with the UK Home Office around emerging and future crimes. These were exceptionally well attended, and received very positive feedback.



Policy Briefings, impact and dissemination

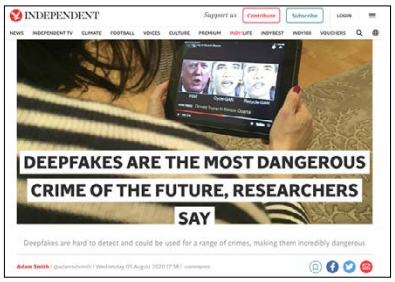
Our research is carried out with the aim of enabling crime prevention in the real world. We aim to achieve such impact by disseminating our work to those who can best use it. We do this in several ways including at events, publishing research papers, and publishing other forms of output such as reports and policy briefings.

Over the course of the past year we have published several 'policy briefings' designed for busy practitioners. These condense the results of our research into short documents that quickly summarise it. The briefings are sent to our mailing lists and published on our website, but they are also published in the Police Insight and sent to a targeted list of actors who our research suggests may find them useful. The briefings are prepared with the help of colleagues in the UCL Department of Science, Technology, Engineering and Public Policy (STEaPP). These briefings have been hugely successful in drawing attention to the centre.

In 2020, the following briefings were published and can be downloaded from our website.

- AI-enabled future crime policy briefing
- How Secure is Consumer IoT
- Challenges of Preventing Counterfeit Goods
- Cryptocurrencies and future crime

Impact Highlights



A top 5% accessed paper

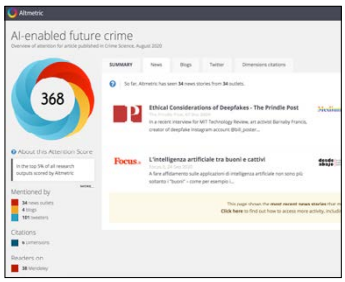
The 'AI-enabled future crime' policy briefing was published along with an accompanying academic paper available here. That work has been featured in newspapers and media around the world. The paper has been accessed over 15000 times and scored in the top 5% of all research outputs as scored by Altmetric.

Coverage in Policing magazines

Our work is now being published in several policing publications. This has helped increase awareness of the Centre's research with police communities around the world. You can view one such article on Crypto-Currency Enabled Future Crime on The Police Foundation blog, a leading police think tank in the UK.

Making a worldwide news splash with our AI-enabled future crime project

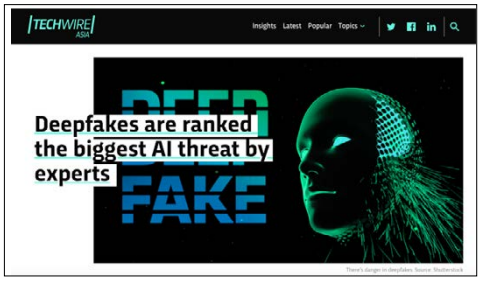
The 'AI-enabled future crime' policy research was picked up by news agencies around the world.



A Guardian newspaper article featuring our COVID work

In Dec 2020, a Guardian article by Laura Spinney entitled The great opportunity: how Covid transformed global crime featured work originating from our Reducing the Unanticipated Harms of Covid-19 Policies project. You can read the full article here. Below is the quote regarding our work.

"In September, the crime scientists Graham Farrell of the University of Leeds and Shane Johnson of UCL warned of possible thefts of vaccine shipments, bribes and backhanders for preferential treatment from suppliers, and even the chilling prospect of deliberate virus-spreading "to prime the market". They urged governments to resist the temptation to wave through light-touch controls on vaccine supply lines, fearing that these would only fuel crime. Since then, several fake Covid-19 vaccines have been seized, police have taken down online ads for others, and there have been reports of vaccine thefts and cyber-attacks on organisations that will distribute the real vaccines."



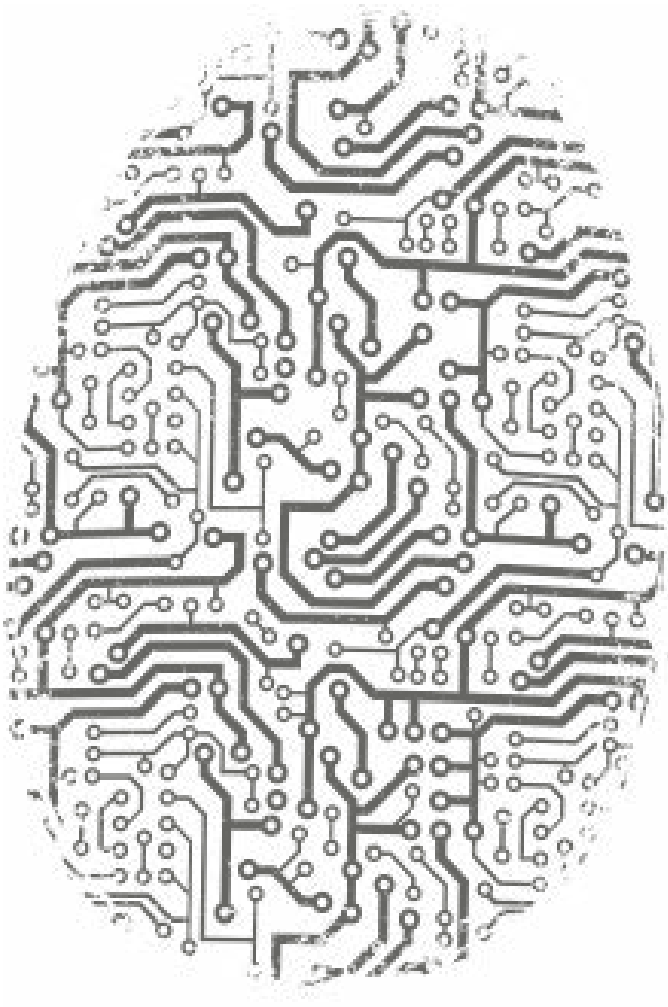
TV coverage for our counterfeit goods project

The 'Challenges of preventing counterfeit goods' research was featured on Countryfile, a BBC topical news that has been running since 1988 and focuses on rural, agricultural and environmental issues in the UK. Here they are filming the project leads, Dr Rob Moss and Dr J.C. Khong, at UCL.

Conclusion

This year the Dawes Centre has made a significant splash. The Centre's work is making a clear impact on the emerging and future crimes agenda. It is satisfying to be able to see the groundwork established over the past few years now being translated into actionable intelligence and research that is helping to create awareness of these new crime types among the law enforcement, security, policy and voluntary sector communities. The hope is that awareness will lead to changes in practice and policy, and the development of interventions, and the Centre will endeavour to help in those efforts wherever feasible.

Feedback from stakeholders has been gratifying. There is a clear appetite for the Centre's work. The aim over the next period is to consolidate this impact by continuing engagement with stakeholders, and publishing further briefings, reports, and papers that similarly feed into the hot button crime issues of the near to mid-term horizon.



With all this activity, the Centre's profile has continued to rise. Leveraging external relationships, both internal and external to UCL, has helped in this endeavour, and a variety of partnerships are now established that will stand the Centre in good stead.

As we move into the new reporting year, the world is still shaking off the effects of the global social and economic crisis caused by the Covid pandemic. The Centre is pleased to have played a small role in combating that disruption via the 'Reducing the Unanticipated Harms of Covid-19 Policies' project. One of the most exciting projects in the coming year is around modelling the vulnerability of older people in the UK to cybercrime. Given the prevalence of aging populations around the world this is a particularly topical piece of work.

The Centre is looking forward at a strategic level. With a new strategy now in place, time has been taken to consider how to build on the work so far carried out. One way to do this is by deepening research around particular themes, such as cybersecurity. In this respect our work in helping to establish and run the CDT in Cybersecurity at UCL (co-directed by Prof Johnson) – with the UCL departments of Computer Science and STEaPP – will stand the Centre in good stead in the coming years. This strategic partnership allows the Centre to think about cybersecurity in non-traditional ways, and several projects already speak to this goal, including work on bio-hacking, smart cities, and future planned research on autonomous vehicles. All in all, the coming period brings with it a sense of excitement and optimism.

Appendix 1

Governance of the centre

The Executive Committee (EC)

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

- The Dawes Trust – Sir Stephen Lander, John Graham, and Stephen Webb,
- Independent advisors – Dr Helen Atkins (Defence Science and Technology Lab), and Simon Ruda (formerly of Behavioural Insights Team), and
- UCL – Professor Kate Bowers (Head of UCL Security and Crime Science and Committee Chair), Professor Nigel Titchener-Hooker (Dean of the Faculty of Engineering Sciences), and Professor Shane Johnson (Director of the Dawes Centre for Future Crime at UCL).

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.

Appendix 2 – Academic Publications

The following Centre-related articles authored by Centre staff and students were published during the reporting period. For previous publications please visit our website.

Security and the smart city: A systematic review – Published April 2020
Laufs, J., Borrion, H., & Bradford, B. (2020). Security and the Smart City: A Systematic Review. Sustainable Cities & Society, 55, 102023. doi: https://doi.org/10.1016/j.scs.2020.102023

Frequency-Guided Word Substitutions for Detecting Textual Adversarial Examples – Published April 2020
Maximilian Mozes, Pontus Stenetorp, Bennett Kleinberg and Lewis D. Griffin (2021) arXiv:2004.05887 [cs.CL] . Frequency-Guided Word Substitutions for Detecting Textual Adversarial Examples. To appear in Proceedings of the 16th Conference of the European Chapter of the Association for Computational Linguistics (EACL).

The impact of IoT security labelling on consumer product choice and willingness to pay – Published June 2020
Johnson SD, Blythe JM, Manning M, Wong GTW (2020) The impact of IoT security labelling on consumer product choice and willingness to pay. PLoS ONE 15(1): e0227800. https://doi.org/10.1371/journal.pone.0227800

Manipulating emotions for ground truth emotion analysis – Published June 2020
Kleinberg, B. (2020). Manipulating emotions for ground truth emotion analysis. ArXiv:2006.08952 [Cs.CL].

Measuring Emotions in the COVID-19 Real World Worry Dataset – Published July 2020
Kleinberg, B., van der Vegt, I., & Mozes, M. (2020, July). Measuring Emotions in the COVID-19 Real World Worry Dataset. Proceedings of the 1st Workshop on NLP for COVID-19 at ACL 2020. ACL-NLP-COVID19 2020, Online.

Understanding the concept of 'demand' in policing: a scoping review and resulting implications for demand management – Published 15 July 2020
Laufs, J., Bowers, K., Birks, D., & Johnson, S. (2020). Understanding the Concept of 'Demand' in Policing: A Scoping Review and Resulting Implications for Demand Management. Policing & Society. DOI: 10.1080/10439463.2020.1791862

AI-enabled future crime – Published 05 August 2020
Caldwell, M., Andrews, J.T.A., Tanay, T. *et al.* AI-enabled future crime. *Crime Sci* **9,** 14 (2020). https://doi.org/10.1186/s40163-020-00123-8

A COVID-19-Based Modified Epidemiological Model and Technological Approaches to Help Vulnerable Individuals Emerge from the Lockdown in the UK – Published September 2020
Anderez, D.O.; Kanjo, E.; Pogrebna, G.; Kaiwartya, O.; Johnson, S.D.; Hunt, J.A. A COVID-19-Based Modified Epidemiological Model and Technological Approaches to Help Vulnerable Individuals Emerge from the Lockdown in the UK. *Sensors* **2020**, *20*, 4967. https://doi.org/10.3390/s20174967

Too good to be true? Predicting author profiles from abusive language – Published September 2020
van der Vegt, I., Kleinberg, B., & Gill, P. (2020). Too good to be true? Predicting author profiles from abusive language. ArXiv:2009.01126 [Cs.CL].

Online influence, offline violence: language use on YouTube surrounding the 'Unite the Right' rally - Published September 2020
van der Vegt, I., Mozes, M., Gill, P. *et al.* Online influence, offline violence: language use on YouTube surrounding the 'Unite the Right' rally. *J Comput Soc Sc* **4,** 333–354 (2021). https://doi.org/10.1007/s42001-020-00080-x

Women Worry About Family, Men About the Economy: Gender Differences in Emotional Responses to COVID-19 – Published October 2020
van der Vegt, I., & Kleinberg, B. (2020). Women Worry About Family, Men About the Economy: Gender Differences in Emotional Responses to COVID-19. In S. Aref, K. Bontcheva, M. Braghieri, F. Dignum, F. Giannotti, F. Grisolia, & D. Pedreschi (Eds.), Social Informatics (Vol. 12467, pp. 397–409). Springer.

A Systematic Review of the Criminogenic Potential of Synthetic Biology and Routes to Future Crime Prevention – Published October 2020
Elgabry M, Nesbeth D and Johnson SD (2020) A Systematic Review of the Criminogenic Potential of Synthetic Biology and Routes to Future Crime Prevention. *Front. Bioeng. Biotechnol.* 8:571672. https://doi.org/10.3389/fbioe.2020.571672

"Show this thread": policing, disruption and mobilisation through Twitter. An analysis of UK law enforcement tweeting practices during the Covid-19 pandemic – Published October 2020
Nikolovska, M., Johnson, S.D. & Ekblom, P. "Show this thread": policing, disruption and mobilisation through Twitter. An analysis of UK law enforcement tweeting practices during the Covid-19 pandemic. *Crime Sci* **9,** 20 (2020). https://doi.org/10.1186/s40163-020-00129-2

Are Repeatedly Extorted Businesses Different? A Multilevel Hurdle Model of Extortion Victimization – Published October 2020
Estévez-Soto, P.R., Johnson, S.D. & Tilley, N. Are Repeatedly Extorted Businesses Different? A Multilevel Hurdle Model of Extortion Victimization. *J Quant Criminol* (2020). https://doi.org/10.1007/s10940-020-09480-8

Law Breaking and Law Bending: How International Migrants Negotiate with State Borders – Published November 2020
Cassilde Schwartz, Miranda Simon, David Hudson, Shane D Johnson, Law Breaking and Law Bending: How International Migrants Negotiate with State Borders, *International Studies Quarterly*, Volume 65, Issue 1, March 2021, Pages 184–196, https://doi.org/10.1093/isq/sqaa079

Spatial analysis of border closure intervention scheme in conflict-induced displacement – Published November 2020
Jafari, Z., Davies, T., Johnson, S.D. (2020) Spatial analysis of border closure intervention scheme in conflict-induced displacement GeoSim '20: Proceedings of the 3rd ACM SIGSPATIAL International Workshop on GeoSpatial SimulationNovember 2020 Pages 1–9 https://doi.org/10.1145/3423335.3428162

Policing in pandemics: A systematic review and best practices for police response to COVID-19 – Published December 2020
Laufs, J. & Waseem, Z. (2020). Policing in Pandemics: A Systematic Review and Best Practices for Police Response to COVID-19. International Journal of Disaster Risk Reduction, Vol 51, 101812, ISSN 2212-4209. DOI: https://doi.org/10.1016/j.ijdrr.2020.101812

On the Feasibility of Acoustic Attacks Using Commodity Smart Devices – Published December 2020
M. Wixey, E. De Cristofaro and S. D. Johnson, "On the Feasibility of Acoustic Attacks Using Commodity Smart Devices," 2020 IEEE Security and Privacy Workshops (SPW), 2020, pp. 88-97, doi: 10.1109/SPW50608.2020.00031

How humans impair automated deception detection performance – Published February 2021
Kleinberg, B., & Verschuere, B. (2021). How humans impair automated deception detection performance. Acta Psychologica, Vol 213, 103250.

Other Outputs

Bio-crime and COVID-19 – Published May 2020
Elgabry (2020). UCL JDI Special Series on COVID-19: No. 14. ISSN 2635-1625 https://www.ucl.ac.uk/jill-dando-institute/sites/jill-dando-institute/files/bio-crime_and_covid-19_final_no_14_.pdf (free access)

Written evidence submitted by Mariam Elgabry – Published June 2020
UK Joint Committee on the National Security Strategy for Biosecurity and national security, in light of Covid -19.

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