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 2021 – 28 February 2022

Contents

Executive Summary

Professor Shane Johnson, Director

The past year has seen communities from around the world come together in unprecedented fashion as we have gradually worked our way out of the disruption caused by the Coronovirus pandemic. We are still a long way from returning to pre-Covid levels of normality – and indeed, in many ways we will never return to the world as we knew it. Many things have changed – the way we work, interact, communicate, shop, and spend our leisure time. Predictably, criminals have not failed to spot opportunities in this new hyperlinked society.

This last period has been another 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 our researchers speaking at the United Nations to working closely with the UK Home Office, the Centre's research has created talking points and encouraged engagement. Information about these can be found in the ***Impact, Dissemination and External Engagement*** section. Links to the latest academic papers from the Centre can be found in the ***Academic Publications*** section.

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.

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 parties 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, a full scale conference could not be hosted, but instead the Centre hosted 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.

2 Current projects

THREE projects began in the reporting period and are ongoing.

3 PhD projects

– this year, SIX new PhD students were recruited, carrying out doctoral research in a range of topics.

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

In the coming period, more 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 2021 to 28 February 2022. 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 fifth 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.

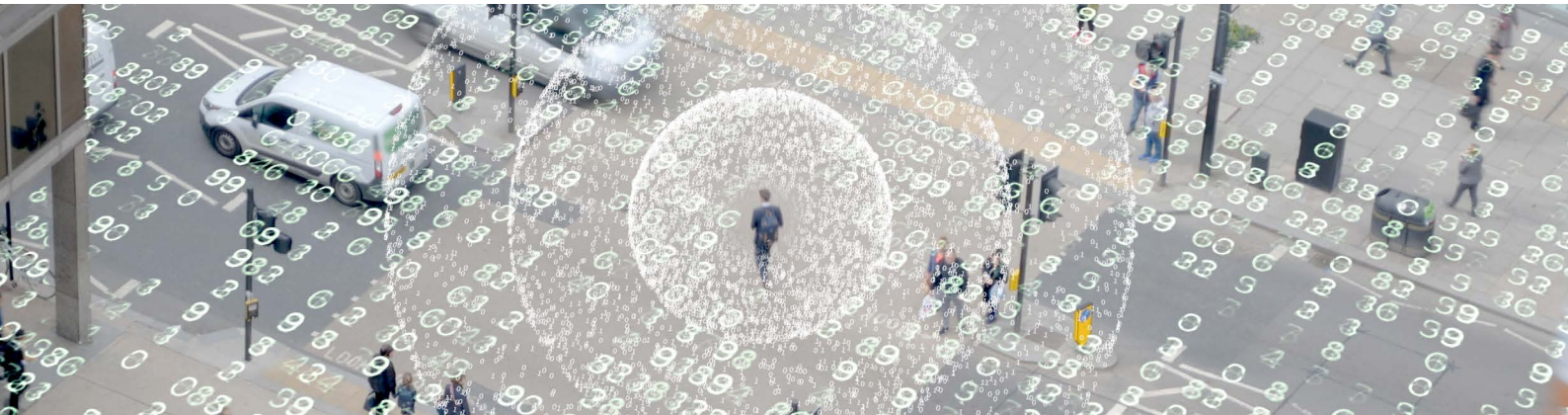
The Centre’s research anticipates how technological, social or environmental change might create new opportunities for offending, or have implications for how law enforcement (and others) combat crime. Projects generally comprise two phases:

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.



1 Research Highlights: Completed projects

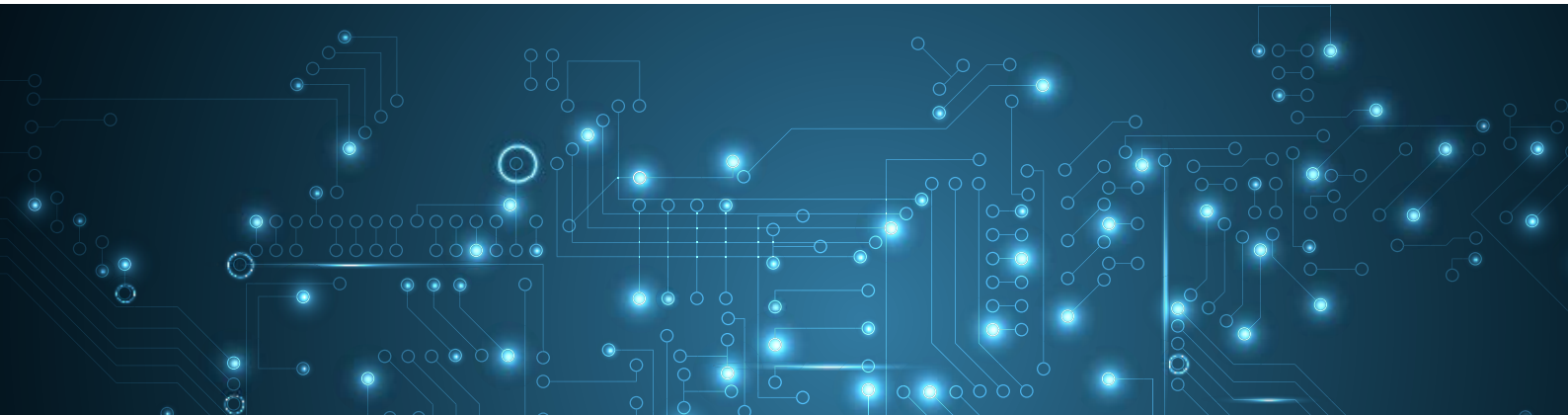
Reducing the Unanticipated Crime Harms of Covid-19 Policies

Covid-19 and related policies restricted movements and changed online interactions in ways that can influence crime risk. This project was a collaboration with the University of Leeds, working with the National Police Chief's Council, Neighbourhood Watch and the City of London Police, to understand how crime changed on- and off-line, and how policing adapted.

Key Findings: The research completed by the Dawes Centre to date had five key elements. The first examined UK police use of Twitter in the early stages of the Covid-19 pandemic, looking at what was posted, and what was re-tweeted (a measure of the impact of tweets). Key findings were that during the first stages of the pandemic there was a significant increase in tweets about fraud, cybercrime and domestic abuse. However, the increase in posts about domestic abuse occurred after the first lockdown, reducing opportunities for victims to act or contact support services. Messages were more likely to be retweeted if they came from "active" Twitter accounts, if the message focused on a specific type of crime, and if the message included a reference to Covid-19 or a photograph. This work contributes to a very limited evidence base on the effectiveness of police use of Twitter and provides recommendations (found here) as to how the police might make best use of social media during times of disruption.

The second study examined how different types of residential burglary were affected by the pandemic and if and how this varied by time of day. According to the routine activity perspective, changes to people's activity patterns should alter when and where crime can and will occur. As expected, it was found that residential and attempted residential burglaries both decreased significantly, particularly during the day. Moreover, while changes were coincident with the timing and relaxation of restrictions, they were better explained by fluctuations in household occupancy than the types of restrictions in place. In contrast, while there were significant decreases in non-residential and attempted non-residential burglary, these were not related to changes in resident's activity patterns but rather the phase of the lockdown. From a practical perspective, the results suggest that when attempting to anticipate future trends of residential burglary, it will be useful to model expected changes in mobility and how proposed changes (e.g. work from home policies) might affect this.

The third study (found here) tested if and how Covid-19 containment policies impacted upon different types of fraud committed online and in a physical context (doorstep fraud). Using data for UK online sales, population mobility and monthly counts of crime, a time series statistical modelling framework was used to analyse changes over time. Findings show that while online fraud increased during the pandemic, doorstep fraud (which has a different opportunity structure) declined. The findings provide striking evidence that oscillations in people's day-to-day activities appear to explain levels of fraud committed on- and off-line.



The fourth study involved a survey of Neighbourhood Watch members. Findings show that, in line with the study above, the risk of successful and attempted victimisations increased during the pandemic. In terms of what predicted outcomes, after controlling for other factors (e.g. age and gender), it was found that those who engaged in more security behaviours were more likely to be aware of attempted attacks but less likely to be victimised. Certain types of security behaviours (e.g. "mouse overing" links before clicking on them) were found to be important in reducing victimisation risk, suggesting their value in cyber hygiene training and advice. Brewer et al. (2019) recently concluded that "*to date there has been little to no research evaluating the effects of crime prevention initiatives on cybercrime*" and hence these findings contribute to an important but limited evidence base.

The final completed study was a collaboration with the National Police Chief's Council (NPCC) in which expert opinion was elicited from UK law enforcement agencies to understand their perspectives about the police response to the pandemic, how it affected policing, what worked well and should continue, and how the pandemic affected crime. To provide insight into future disruptions, respondents were also asked about how they thought crime might change as a consequence of social and political change, climate change, and technological change. The findings are too numerous to summarise here but included views on *Community engagement, Communications, Staff Wellbeing, Policing Demand, and Covid19 Recovery*. With respect to future trends, two common themes that emerged were the need for investment in, and the coordination of, futures and foresight activity, and the need to prioritise the prevention and investigation of cybercrime. The findings motivated 12 key policy recommendations and 7 sub-recommendations which will be published shortly.

Lead Investigator(s):
Dr Dan Birks,
University of Leeds
Prof Kate Bowers,
UCL Security and Crime Science
Prof Graham Farrell,
University of Leeds
Prof Shane Johnson,
Dawes Centre for Future Crime at UCL
Prof Nicolas Malleson,
University of Leeds
Prof Nick Tilley,
UCL Security and Crime Science

UCL Researchers:
Dr Michael Frith,
Dr Manja Nikolovska,
Dawes Centre for Future Crime at UCL

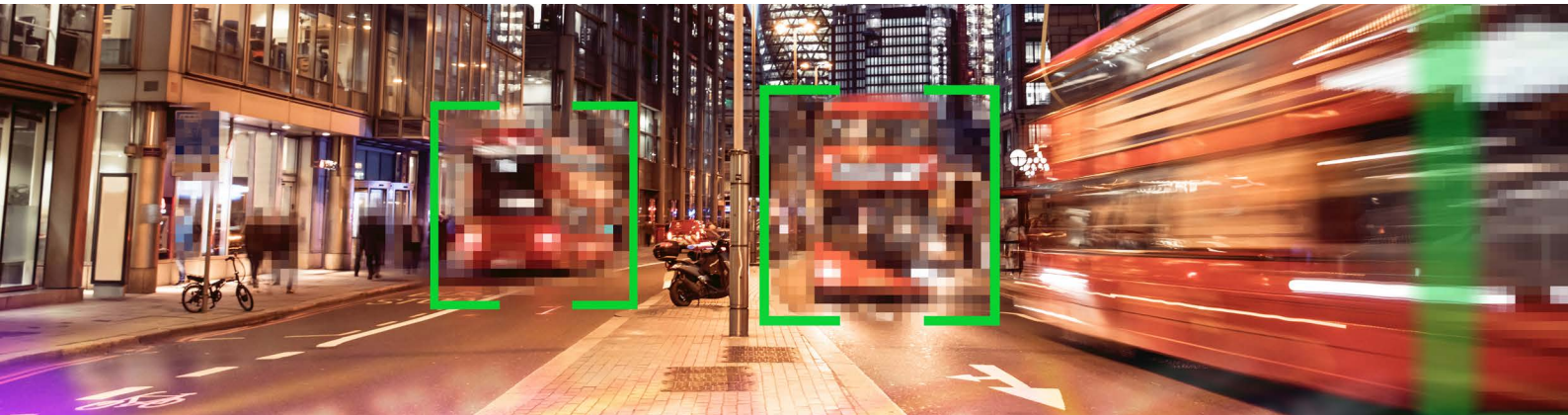
PITCHR: Prevention of IoT-enabled Crime using Home Routers

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 (e.g. Amazon Echo and Google Home), smart wearables (e.g. Fitbit), smart security (e.g. Ring and baby monitors), smart appliances (e.g. smart kettles, fridges and washing machines), smart energy (e.g. Nest and smart plugs) and many more. As shown in the Centre's research concerned with the Internet of Things (IoT), 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 cybercrime.

Key Findings: The PITCHR Project considered the role of the home router in facilitating and preventing cyber crime. During the study the researchers analysed the academic, industry and government literature, and held a number of focus group discussions with the key stakeholders – service providers, hardware manufacturers, citizen and citizen groups, government and academia. The discussions from the focus groups were pseudo-anonymised and critically analysed to identify themes and sub-themes, which offered insights into the perspectives of the various stakeholders and the challenges faced by each in the prevention of IoT-enabled crime using home routers. The study identified ten main themes:

1. Evolution of Home Router technology
2. Future of router technology
3. The role of Service Providers
4. The role of Hardware and Hardware Manufacturers
5. The role of Citizen and Industry Groups
6. Cost of Providing Home Router Security
7. Regulatory Role and Impact
8. Who is / should be Responsible for Home Router Security
9. User Awareness and Education
10. Changing Nature of Home Router Cyber Security Landscape



The study found that:

- it will take a combined effort from all the stakeholders to prevent IoT-enabled crime using home routers.
- Legislation – at the time there were currently no specific regulations in the IoT space, though the government had announced that is imminent to ensure that the market adhere to rigorous security requirements for IoT devices (Gov.uk, 2020).
- Much more stringent standards from the open standards community and frameworks are required to establish baselines for home router security.
- Service Providers spend significant amounts on protecting their networks but the investment does not necessarily trickle down to the home router network, particularly, inside the home environment.
- Service Providers do not collaborate sufficiently with each other and sharing intelligence on threat landscape is limited, if at all. This makes it easy for cyber criminals to deploy the same techniques to several networks successfully.
- Automation of home router network security may be vital to the Prevention of IoT-enabled Crime using Home Routers
- it is unclear who should be responsible for providing home router security.
- it is unclear who should pay for home router security.
- The average end-user of the home router does not have the knowledge and the capability to configure and secure their home router and devices.
- User awareness and education is vital in the Prevention of IoT-enabled Crime using Home Routers.

The results of this work have been published in a paper entitled: Prevention of IoT-Enabled Crime Using Home Routers (PITCHR) in **EAI PFSM 2021 - EAI International Conference on Privacy and Forensics in Smart Mobility**.

This strong engagement with Government and Industry has led to a series of formal and informal, regular and ad-hoc follow-up meetings. Knowledge gained has been disseminated to provide input into the £2M Innovate UK-funded ManySecured project through its Special Interest Group, which has subsequently secured £2M further funding from Innovate UK. Current discussions with UK Government concern the role of regulation and manufacturers of similar equipment in industrial settings.

Lead Investigator:
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

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.

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.

This project responded 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).

Key findings: The team 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. There is minimal evidence regarding how to reduce risks from intervention studies, though cyber-training, cyber-guardians, and awareness videos were tested in single intervention studies.

The project also consulted a group of experts and practitioners through the duration of the project. At specially designed virtual sandpit exercises experts from police, banks, financial institutions, MoJ and cybersecurity firms identified the types of cybercrime that posed the greatest risk to older adults in UK. They also recommended practical and policy measures to mitigate the risks. For instance, in November 2020, a sandpit event was held with 21 experts, who offered 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.

The findings of the project featured in a policy briefing (see Policy briefings, Impact and Dissemination section below) that was used to inform the debate on the Online Safety Bill in the Parliament. The results were also published in the Experimental Gerontology journal. The findings of the research were also presented at a seminar series organised by the Dawes Centre for Future Crime at UCL and the Home Office conference on Future Crimes and the Changing World.

The project has led to the recruitment of a PhD student funded by the Dawes Centre for Future Crime. The aim of the PhD is to develop an intervention to protect older people from financial fraud online.

Lead investigator(s):
Professor Claudia Cooper,
UCL Division of Psychiatry
Dr Kartikeya Tripathi,
UCL Security and Crime Scienc

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 explored 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 were explored and concepts for end-user devices investigated.

A list of candidate agrochemicals that are typical targets for exploitation was 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 were 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.

.

Key findings: This project looked at various technologies that could be used as a screening tool for the identification of counterfeit and substandard agrochemicals. Efforts were concentrated on technologies that do not require any special sample preparation, could work through the chemical container and have the potential to be miniatured and simplified for field deployment with boarder control or regulatory personnel. The investigation showed that both Ramen spectroscopy and ultrasound analysis have good discrimination capability when the agrochemical is diluted with water – a common adulterant. While Raman is a typical technique for this kind of problem, ultrasound could meet all of the criteria outline above in a simple and relatively cheap form factor.

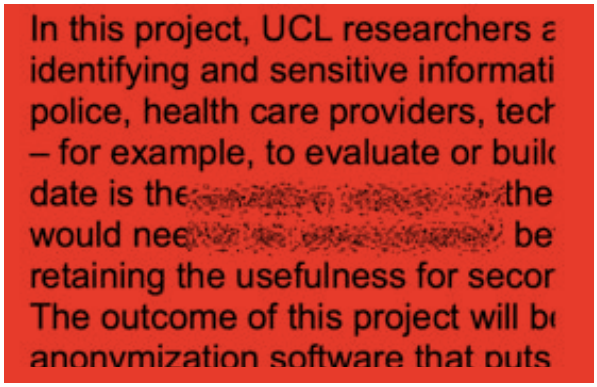
Outcomes of this project include a featured spot on the BBC Countryfile programme, a policy briefing document on future trends in counterfeit chemical goods and invited presentations to chemical manufacturers (Syngenta), industry groups (Croplife UK) and regulators (Red Tractor). In-kind support came in the form of free agrochemical samples from Corteva, BASF and LGC Group. In May 2022, LGC Dr. Ehrenstorfer™ hosted a webinar for UCL to showcase the work undertaken in this critical area.

Lead investigator(s):
Dr Rob Moss,
Prof Rob Speller,
UCL Dept of Medical Physics & Biomedical Engineering

Research Assistant:
Dr J.C. Khong,
UCL Dept of Medical Physics & Biomedical Engineering

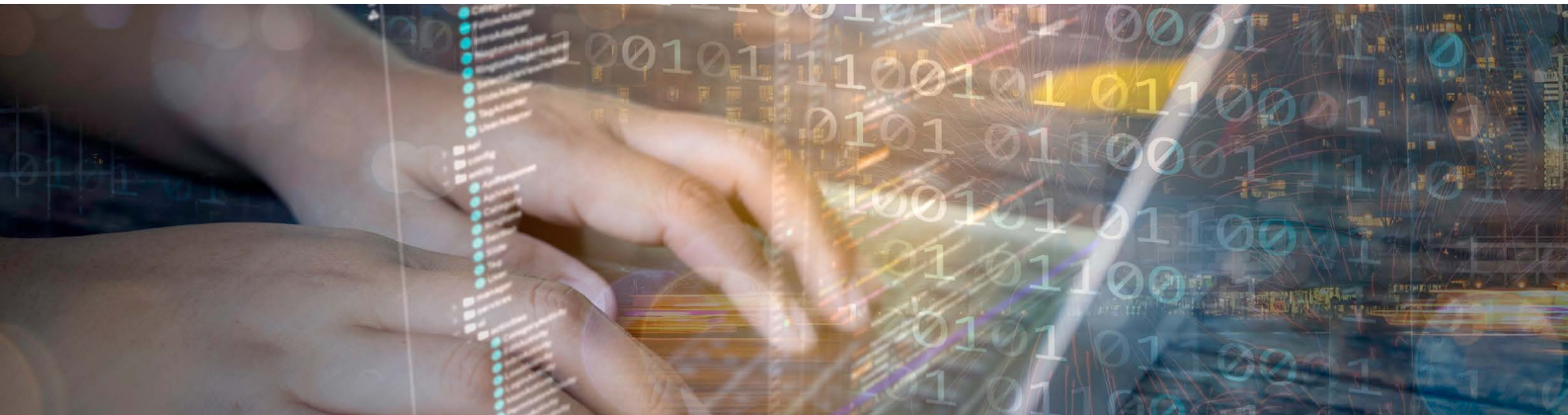
Textwash

For this project, UCL researchers 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 is the first empirically-validated and transparent anonymization software that puts all control in the hand of the users. Textwash was supported by a proof-of-concept grant from SAGE.



Key findings: The system has now been validated in empirical studies and has received attention from industry and academia and is included in a European Commission consultation round on best practices for automated text anonymisation. The Textwash project has seen significant advancements in the underlying algorithms and is growing to a multi-language project with new funding from the Dutch Research Council (NWO). Textwash is further currently piloted as a key resource for the US National Archive of Criminal Justice Data for their mission to make research data widely available. The software is also being installed in the UCL Dept of Security and Crime Science data lab to facilitate data access.
A release to a non-technical audience as well as two initial scientific publications are envisioned for 2022.

Lead investigators
Dr Toby Davies
Dr Bennett Kleinberg,
Maximilian Mozes,
UCL Security and Crime Science



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.

Key findings: This project explored how advanced statistical and simulation techniques can be used to understand the interactions between police demand and its impacts on resourcing.
A systematic review of the existing literature which formed the initial stage of the project can be found here. A statistical analysis of the complex relationship between policing and crime, which used data for 42 police forces in England and Wales for a period of 13 years, will be published shortly. This showed that policing does impact upon crime and vice versa, that staff turnover has a negative impact on crime outcomes, and that differences are observed for models that consider crime volume and those that consider crime severity. In addition to analysing empirical data, the project involved the development of a prototype computational modelling platform to explore these dynamics, to simulate crime related demand, and subsequent police responses. Models were tested as a tool for modelling different demand scenarios (e.g. volume crime and public order policing), with the long-term aim of creating tools that can support police demand-related decision making.

Lead investigator(s):
Dr Dan Birks,
University of Leeds
Prof Kate Bowers,
UCL Security and Crime Science
Prof Alison Heppenstall,
University of Leeds
Prof Shane Johnson,
Dawes Centre for Future Crime at UCL.
Prof Ken Pease,
University of Derby

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

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

Note: Information about the previously completed projects can be found on the Centre website. These include:

- Challenges of preventing counterfeit goods
- AI-enabled Future Crime
- How secure is consumer IoT?
- Cryptocurrency fraud as a future challenge for large-scale financial crime
- Smart Tagging and Proximity Detection for Crime Reduction
- Crime, place and the Internet
- Advanced Materials to Combat Crime

2 Research Highlights: Current projects

Smart Doorbell Evaluation

Previous research, including that conducted by the Dawes Centre for Future Crime, has identified crimes that might be facilitated by internet connected devices (the Internet of Things, or IoT) and what might be done to address such threats. The IoT does, of course, also present numerous opportunities to reduce crime. Smart video doorbells are one example, but there exists no independent evaluation of their effectiveness in preventing crime. In this study, a large-scale randomised controlled trial will be conducted, which is funded by and being conducted in collaboration with, the Metropolitan Police Service. The study will examine the impact of Smart video doorbells on crimes to include residential burglary, and other offences committed around the home.

Lead investigator(s):
Prof Shane Johnson,
Dawes Centre for Future Crime at UCL.
Dr Alina Ristea,
Dr Michael Frith,
UCL Security and Crime Science

The applicability of the UK Computer Misuse Act 1990 for cases of technology-enabled domestic violence and abuse

This project is evaluating the applicability of the Computer Misuse Act 1990 for intimate partner violence (IPV) to give a better understanding of historic domestic abuse and CMA cases in order to give law enforcement agencies and the Crown Prosecution Service (CPS) a powerful tool to charge tech abusers, and help the research and practitioner community to develop awareness of the types of digital systems that are abused, refine technical mitigation strategies such as privacy enhancing technologies (PETS), and explore the usefulness of existing legislative means (such as the CMA) to deal with the harms derived from digital systems.

Lead investigator(s):
Dr Leonie Tanczer,
UCL Science, Technology, Engineering and Public Policy (STEaPP)
Prof Shane Johnson,
UCL Security and Crime Science
Francesca Stevens
UCL Science, Technology, Engineering and Public Policy (STEaPP) /City University of London
Frances Ridout,
School of Law, Queen Mary University of London

Cryptocurrency and Money Laundering

A study by Pol (2020) estimated that only 0.1% of global criminal finances are captured by traditional approaches to anti-money laundering (AML). Recent literature and discussions among law enforcement agencies, academics, banks, other financial institutions and financial regulators points to an emerging area of crime in which cryptocurrencies are or will be exploited to process illicit funds generated through crime. The role that cryptocurrencies do or could play in the facilitation of money laundering is evolving as are cryptocurrencies and associated technologies. This will further complicate the AML task. This project will review the role that cryptocurrencies do or might play in the facilitation of money laundering by undertaking an extensive futures-oriented review. The review will analyse numerous criminogenic enablers, specific money laundering and terrorist financing possibilities, relevant stakeholders and risk characteristics relating to distributed ledger technologies and also carry out a systematic appraisal of potential challenges, opportunities, and threats. The findings of the project will offer insights into different cryptocurrency-enabled money laundering and terrorist financing risks with the aim of informing the design of long-term strategies to address the issue.

Lead investigator(s):
Prof Shane Johnson,
Dawes Centre for Future Crime at UCL.
Prof Matt Manning,
Australia National University
Eray Arkatuna,
UCL Security and Crime Science

3 Research highlights: PhD projects

The Dawes Centre funds a range of PhD projects covering an array of topics relevant to the Centre's agenda. There are *currently* 29 researchers on the programme, with several of these being part of the new Centre for Doctoral Training in Cybersecurity at UCL, which is a collaboration between the departments of Computer Science, Security and Crime Science, and STEaPP that is co-directed by Professor Johnson. The PhD projects that began during the current reporting period are described below:

Ethical and Explainable Machine Learning for Child Protection from Online Abuse

Decision-making processes once delegated to humans are progressively mediated, if not even determined, by machine learning algorithms. Machine learning algorithms are powerful socio-tech constructs which may, however, raise non-ethically neutral outcomes. Examples nowadays abound, with the consequence that the ethical debate has gone mainstream. With over eighty AI ethics guides available in the public domain, the debate has primarily focused on principles - the 'what' of AI ethics. Hence, this PhD research aims to advance the question of 'how' to reach the 'what' when machine learning is employed in high impact and socially sensitive contexts, such as the child protection system.

PhD start year: 2021

PhD student: **Aliai Eusebi**

PhD supervisors: **Dr Enrico Mariconti**, **Dr Ella Cockbain**, UCL Security and Crime Science, and **Dr Marie Vasek**, UCL Computer Science.

Contact: aliai.eusebi.16@ucl.ac.uk

Young People, Drugs and Social Media

The online purchase of illicit substances has been happening on the Dark Web, but in recent years commercial activity has moved to popular social media apps. Teenagers can now buy and sell illicit substances through Instagram or Snapchat, without having to physically leave their homes. In a couple of clicks, posts advertising the sale of cannabis, cocaine, or ecstasy can be easily found. This has led to an increasing number of teenagers dying of overdoses, given the accessibility and perceived trust when buying drugs through social media.

This PhD project has 3 key objectives: to understand the extent of this issue cross-nationally, to evaluate the effectiveness of preventive solutions; and to inform policy. This research will use various disciplinary frameworks, including social sciences, public policy, crime and computer science methods.

PhD start year: 2021

PhD student: **Ashly Fuller**

PhD supervisors: **Prof. Shane Johnson**, **Dr. Enrico Mariconti**, UCL Security and Crime Science, and **Dr. Marie Vasek**, UCL Computer Science.

Contact: ashly.fuller.16@ucl.ac.uk

Technology facilitated abuse within intimate partner relationships

In 2018 technology-facilitated abuse was identified by Comic Relief and the charity SafeLives as an emerging concern. Following the work of teams that include the G-IoT project at UCL, there is work taking place that explores this prevalent form of abuse. However, within the Violence Against Women and Girls (VAWG) sector this form of abuse has only recently begun to be acknowledged as a risk indicator. Efforts thus far within the industry, in response, have included dedicated tech abuse caseworkers and device how-to guides. Sector-wide understanding, sharing of learning, and assessments to develop evidence-based responses in the United Kingdom remain few and far between. This PhD seeks to understand the prevalence of technology-facilitated abuse in the context of intimate partner relationships. Key areas of focus will include: the understanding of tech abuse within the Domestic Abuse sector, how the sector assesses this form of abuse, what implementations are currently being utilized to support survivors of tech abuse, and could this form of abuse be considered a high-risk of harm indicator? It is hoped that, through collaboration with Domestic Abuse sector researchers, policymakers, and service providers, a better understanding of technology facility abuse can be achieved.

PhD start year: 2021

PhD student: **Demelza Penaluna**

PhD supervisors: **Dr Leonie Maria Tanczer**, Lecturer in International Security and Emerging technologies,
and **Professor Shane Johnson**, Director, Dawes Centre for Future Crime at UCL.

Contact: demelza.penaluna.21@ucl.ac.uk

Measuring and Countering Present and Future Crimes Facilitated by Consumer IoT Devices

Internet of Things (IoT) devices are now ubiquitous with most parts of day-to-day life, used to monitor health and wellbeing through devices such as Smart Watches, for entertainment purposes such as using Smart TV's and Games Consoles, and to monitor household energy consumption through Smart Meters. They are also used to power cars through Smart Vehicles. In addition, they are also now used to monitor individuals that approach properties using Smart Cameras/CCTV and Smart Doorbells. The applications for IoT devices are limitless and they provide amazing benefits. However, ordinary Consumers do not consider the potential dangers to these devices that can occur through present and future Cyber Attacks and the types of Heinous and Sometimes Dangerous Crimes that can be committed using these IoT devices as attack vectors through attacks such as Man-in-the-middle, Replay Attacks, etc. As such this topic aims to conduct a review of the potential attacks that can be committed on these devices and then to conduct a Systematic Testing methodology to identify what attacks are possible and list potential crimes that can be committed such as Cyber Stalking, Household Burglaries, etc.

PhD start year: 2021

PhD student: **Ashley Brown**

PhD supervisors: **Dr Enrico Mariconti**, UCL Security and Crime Science,
and **Prof Shane Johnson**, Dawes Centre for Future Crime at UCL.

Contact: ashley.brown.21@ucl.ac.uk

Small to Medium Enterprises and Cyber Vulnerabilities

Small to Medium Enterprises (SMEs) are known to be prolifically targeted by cyber criminals. This is due in part to their apparent inability to counteract the ever-changing cyber threat landscape, along with a potential/ perceived disregard from the decision makers within these organisations to do so. Despite the fact that SMEs account for an estimated 99% of businesses and contribute to 60% of employment, there continues to be a focus on the risks associated with cyber attacks on larger businesses and not how the vulnerabilities within their smaller counterparts can negatively impact on the supply chain. This thesis will therefore aim to outline these vulnerabilities in the context of real business victim experiences of cyber attacks, with this knowledge used to better inform a framework that can be applied by SMEs to protect themselves in the future.

PhD start year: 2022 (Jan)

PhD student: **Siobhan McCrea**

PhD supervisors: **Dr Ingolf Becker,** UCL Security and Crime Science, and **Prof Shane Johnson**, Dawes Centre for Future Crime at UCL.

Contact: siobhan.mccrea.18@ucl.ac.uk

Cybersecurity of Small and Medium Enterprises

A surge in cyber-threats has resulted in an increasing rate of data breaches within companies, leading to financial and economic impacts across the globe. For decades, cybersecurity efforts have concentrated on large corporations, leaving Small and Medium Enterprises (SMEs) ill-equipped to handle cyberattacks. Yet, SMEs represent a vast majority of the global economy - according to the UK parliament, over 99% of the 5.6 million businesses in Britain are considered SMEs and are responsible for 61% of employment and 52% of the country's turnover. Consequently, SMEs have become attractive targets as they struggle to implement solutions designed for larger organisations with in-house cybersecurity resources. While it is evident that SMEs must address security issues, they lack financial resources, expertise and sometimes awareness to address cybersecurity threats. This research presents a systematic and empirical approach to chart threats faced by SMEs, mapping uptake controls along with challenges and constraints in adhering to cybersecurity practices. The ultimate aim is to provide a tailored set of recommendations to equip SMEs with cyber-resilience.

PhD start year: 2021

PhD student: **Carlos Rombaldo Jr.**

PhD supervisors: **Prof Dr Ingolf Becker**, UCL Security and Crime Science; and **Prof Shane Johnson**, Dawes Centre for Future Crime at UCL.

Contact: carlos.rombaldo.21@ucl.ac.uk

Note: For details of PhD projects that began (or were completed) prior to the current reporting period please refer to the Centre's website. These projects include:

- Crime, place and the internet
- Biocrime
- Cybercrime risks to London's future street infrastructure
- The effects of cyberweapons
- Detecting emerging crimes using data science techniques
- Addressing Probable Child Sexual Abusers and Victim Profile Characteristics on Instagram
- 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
- Horizon scanning through computer-automated information prioritisation
- Refugee Flows and Instability
- 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
- Anomaly detection for security
- Protecting the UK's News propagation systems against the threat of "deepfake" injection
- Intelligent biomaterials for the development of high-performance label free biosensors to combat crime
- Hybrid threats
- Automated profiling of user vulnerabilities to online deception and intervening through dynamic user interfaces
- Human trafficking, digitalisation and a global pandemic: how has technology changed the face of human trafficking?
- Brexit and Crime
- Deterring Criminal and Terrorist Planning
- Project Terabytes; The role of social media intelligence in organised crime investigations involving child criminal exploitation
- Take Back Control: Data Democracy with a Pro-Consumer Bias

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 doctoral students. The Centre currently offers modules covering security technologies, data science for crime scientists, applied data science, cybercrime, and horizon scanning.

Benefits of the Centre's teaching programme

A principal benefit of the teaching modules 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 modules has helped to reinforce external relationships. For instance, for one of the 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 sovereign identity, the metaverse, and Non-fungibal Tokens.

PhD teaching

The Centre's PhD teaching encompasses doctoral students funded directly by the Dawes Centre, those funded as part of a 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, and self-funded students. Cross-disciplinary supervision of the PhD programme enables 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, industry and law enforcement to shape projects and have contributed bespoke 'state of the art' systematic reviews of the literature. This all augurs well for the Centre's aim to instill, via teaching, an early respect for the impact that Centre students should aim to generate in the real world through their work at the Centre.

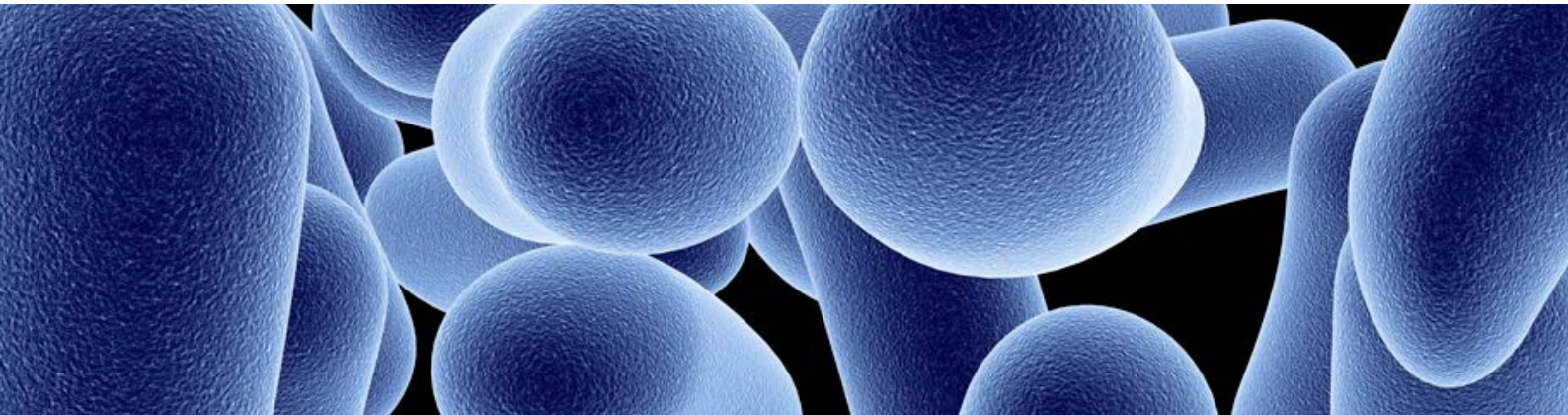
During this period the first PhD researcher graduated from the programme.

Here Julian Laufs describes his experience:

"When I began my PhD in 2018, focusing on crime prevention and detection technologies for smart cities, I did not know what was ahead of me. Now, three and a half years and one incredible journey later, I know that I not only found a great department to do my PhD but also so much more. The Dawes Centre enabled me to engage with various stakeholders to further my research and provided the resources to attend national and international conferences. In addition to my PhD project, I conducted other research, for example, on the impact of COVID-19 on policing. I also enjoyed working as a student representative at the Faculty of Engineering for over two years, working with staff and students to improve the PhD experience for everyone. With the support of the Dawes Centre, I co-founded the UCL Security Science Research and Training Society to facilitate wellbeing and academic exchange amongst PhD students at the department.

Today I find myself working for the German Cybersecurity Innovation Agency.

All in all, I would say that the Dawes Centre is a great place to complete a PhD. I would highly recommend it to anyone who enjoys interdisciplinary research and is looking for a supportive, collaborative, and international environment."



Impact, dissemination, and external engagement

The Centre's research is carried out with the aim of enabling crime prevention in the real world and to achieve impact by engaging with and disseminating the Centre's work to those who can best use it. This is done in several ways including at events, through collaboration or consutancies, by publishing research papers, and publishing other forms of output such as reports and policy briefings.

Policy Briefings

The Centre's 'policy briefings' condense the results of research into short easy-to-consume documents designed for busy practitioners. 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 the past period, the following briefings were published and can be downloaded from the Centre's website, where you will find also find previous briefings.

- Older adults as victims of online financial crime
- Synthetic biology and future crime

The following policy report was also published:

- Network and Information Systems: Improving Implementation

Previously published briefings:

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

Impact Highlights

Dawes PhD researcher presents to the United Nations

On the 23rd of November 2021, Dawes Centre-funded PhD researcher Mariam Elgabry delivered an individual NGO statement to the United Nations Biological Weapons Convention (BWC) Meeting of State Parties to expand on the joint NGO statement, endorsed by over 70 institutions and individuals. A proud moment for the Centre!

This was broadcast live on UN WebTV and can be re-watched here: https://lnkd.in/dr9Sj-7u

Mariam's individual statement can be read here: https://documents.unoda.org/wp-content/uploads/2021/11/UCL.pdf

The Joint NGO statement can be read here: https://documents.unoda.org/wp-content/uploads/2021/11/Joint-NGO-statement.pdf

Women in Cybercrime conference

On 21 July 2021, the Centre organised and hosted an online Cybercrime Conference on fake news, legislative responses to cybercrime, and women in cyber. The conference featured a range of sessions including:

- *Exploring eWhoring*, Professor Alice Hutching, Director, Cambridge University Cybercrime Centre;
- *Unpacking Image-Based Sexual Abuse Legislation*, Frances Ridout, Director, Queen Mary Legal Advice Centre, Queen Mary University School of Law, and practising Barrister
- *In the grey zone – tackling information manipulation in 2021*, Sabrina Spieleder - Policy Officer, Division of Strategic Communications and Information Analysis, European External Action Service"
- *How do we make people more aware of false information online?* Designing effective visual warnings to fight the spread of online misinformation, Dr Fiona Carrol, Senior Lecturer in Digital Media & Smart Technologies, Cardiff Metropolitan University

HACKATHON!

In the summer of 2021, Mariam Elgabry led an "Internet-of-Ingestible-Things Hackathon" - a series of workshops bringing together experts from cybersecurity with medical device regulatory bodies and makers, to help design security for the "Internet-of-Ingestible-Things." Ingestible Things are internet-connected, ingestible medical devices such as smart gut-sensing pills.

Why the Internet-of-Ingestible-Things?

Studies show that intestinal flora have the ability to combat disease, give us mental guidance, and in general keep us safe. Bio-cybersecurity must be considered early during medical design, now more than ever, as medical devices flood the market in response to COVID-19, which has only highlighted weakness in an overburdened healthcare system and in cyber-biosecurity supply chains.

IoIT
INTERNET OF
INGESTIBLE THINGS

Hybrid Hackathon Delphi Model:

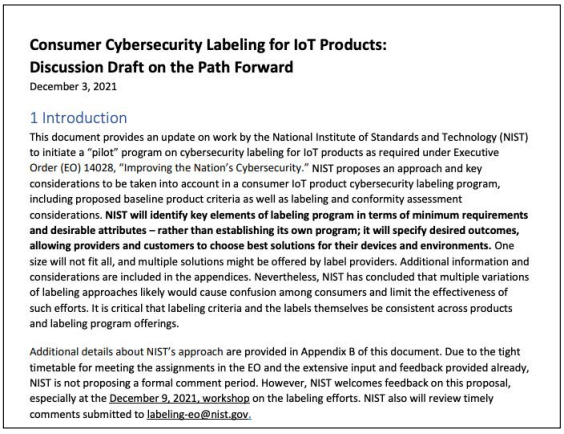
The Implementation plan of the Hybrid Hackathon Delphi Model constituted a three-month format, with three stages. The first stage comprised of contextual talks inviting stakeholders to share challenges of the technology under investigation. The second stage invited stakeholders of the industries of interest to form workshop teams and develop proposals for the topic. Finally, the teams' proposals were shared with an expert judging panel.

Over 200 individuals attended the pre-hackathon talks, 27 individual applicants and 7 team applicants, from a diverse set of backgrounds including pharma, security intelligence and neuroscience. The top 3 teams engaged with more than 4,000 people through their pitch videos and publics' vote raising security awareness for the emerging smart pill tech. The three finalist teams worked on three different proposals.

Team SMARTRACE designed an ingestible that would trace highly contagious infections such as the Norovirus, on cruise ships during quarantine. Their proposal, introduced the use of private blockchain for secure and transparent data transmission. Team IBDeactivate had specialist skills in embedded systems for IoT, and designed an Ingestible-Things™ device for targeted micro-dosing of anti-inflammatory drugs in the gut. Their proposal focused on the need for firmware coding and telecommunication security tailored for clinical and patient acceptance. Finally, team BIOTAI targeted the 10–15% of the worldwide population is estimated to suffer from some gastrointestinal issue, and proposed a secure cloud communication system designed for a wider consumer health market.

Reflections on the event can be read here: https://mariamelgabry.medium.com/ingestible-things-reflections-ad3152b0eb81

Videos can be viewed on Youtube:
IoiT Playlist https://www.youtube.com/playlist?list=PLImAx2L2dpKDwQiyMIGOGGoxyizuDXNxc



Consumer Cybersecurity Labeling for IoT Products: Discussion Draft on the Path Forward

December 3, 2021

1 Introduction

This document provides an update on work by the National Institute of Standards and Technology (NIST) to initiate a "pilot" program on cybersecurity labeling for IoT products as required under Executive Order (EO) 14028, "Improving the Nation's Cybersecurity." NIST proposes an approach and key considerations to be taken into account in a consumer IoT product cybersecurity labeling program, including proposed baseline product criteria as well as labeling and conformity assessment considerations. **NIST will identify key elements of labeling program in terms of minimum requirements and desirable attributes – rather than establishing its own program; it will specify desired outcomes, allowing providers and customers to choose best solutions for their devices and environments.** One size will not fit all, and multiple solutions might be offered by label providers. Additional information and considerations are included in the appendices. Nevertheless, NIST has concluded that multiple variations of labeling approaches likely would cause confusion among consumers and limit the effectiveness of such efforts. It is critical that labeling criteria and the labels themselves be consistent across products and labeling program offerings.

Additional details about NIST's approach are provided in Appendix B of this document. Due to the tight timetable for meeting the assignments in the EO and the extensive input and feedback provided already, NIST is not proposing a formal comment period. However, NIST welcomes feedback on this proposal, especially at the December 9, 2021, workshop on the labeling efforts. NIST also will review timely comments submitted to labeling-eo@nist.gov.

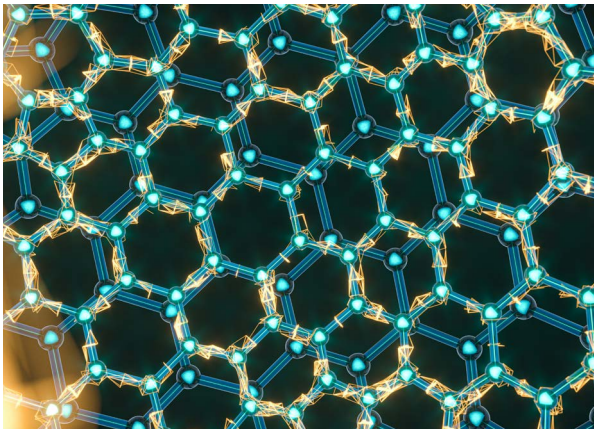
US National Institute for Standards and Technology (NIST) Engagement

Prof Johnson was invited to present at a NIST event about securing the IoT on 14-15 September 2021. The Dawes Centre's IoT labelling work was subsequently used in a draft paper entitled "**Consumer Cybersecurity Labelling for IoT Products: Discussion Draft on the Path Forward**" in Dec 2021 by NIST as part of their efforts to initiate a "pilot" program on cybersecurity labelling for IoT products as required under Executive Order (EO) 14028, "Improving the Nation's Cybersecurity."

NIST proposes an approach and key considerations to be taken into account in a consumer IoT product cybersecurity labelling program, including proposed baseline product criteria as well as labelling and conformity assessment considerations. NIST will identify key elements of a labelling program in terms of minimum requirements and desirable attributes – rather than establishing its own program; it will specify desired outcomes, allowing providers and customers to choose best solutions for their devices and environments. One size will not fit all, and multiple solutions might be offered by label providers.

The full discussion draft paper can be found here: https://www.nist.gov/system/files/documents/2021/12/03/FINAL_Consumer_IoT_Label_Discussion_Paper_20211202.pdf

The NIST event can be viewed here: https://www.nist.gov/news-events/events/2021/09/workshop-cybersecurity-labeling-programs-consumers-internet-things-iot



Impact 'down under'!

In January 2022, Dawes Centre-funded work on Synthetic Biology and Future Crime was featured in the Australian Institute of Police Management 'Know it Now' newsletter.

External engagement

Engagement with other research centres and agencies continued to help the Centre better understand current initiatives in the future crime problems space and offers opportunities for collaboration. Engagement activities include stakeholder "sandpits" workshops, which are conducted as part of scoping research, stakeholder involvement in research projects, guest lectures on taught programmes, and input to PhD research. A flagship activity this year has been a second series of seminars organised with the Home Office and Worshipful Company of Information Technologists which took place between Jan-April 2022. Topics covered included AI-enabled crime, immersive environments, and the changing nature of fraud.

Academic Publications

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

Bordeanu, O. C., Stringhini, G., Shen, Y., Davies, T. (2021), JABBIC Lookups: A Backend Telemetry-Based System for Malware Triage. In: Garcia-Alfaro J., Li S., Poovendran R., Debar H., Yung M. (eds) Security and Privacy in Communication Networks. (Note: The link has a paywall though. Below is a link to the UCL repository which is free: https://discovery.ucl.ac.uk/id/eprint/10139729/)

Delpech, D., Borrion, H., & Johnson, S. (2021). Systematic review of situational prevention methods for crime against species. *Crime science*, *10*(1), 1-20.

Elgabry, M. and Camilleri, J. (2021) Conducting hidden populations research: A reflective case study on researching the biohacking community, Futures, 132.

Hutt, O. K., Bowers, K., & Johnson, S. D. (2021). The effect of GPS refresh rate on measuring police patrol in micro-places. *Crime Science*, *10*(1), 1-14.

Laufs, J., & Borrion, H. (2021). Technological innovation in policing and crime prevention: Practitioner perspectives from London. International Journal of Police Science & Management, 14613557211064053. doi:10.1177/14613557211064053

Laufs, J., Bowers, K., Birks, D., & Johnson, S. D. (2021). Understanding the concept of 'demand'in policing: a scoping review and resulting implications for demand management. *Policing and society*, *31*(8), 895-918.

Mai, K.T.; Davies, T.; Griffin, L.D. Brittle Features May Help Anomaly Detection. *9th Women in Computer Vision workshop at CVPR.*

Mozes, M., Stenetorp, P., Kleinberg, B. and Griffin, L., 2021, April. Frequency-Guided Word Substitutions for Detecting Textual Adversarial Examples. In *Proceedings of the 16th Conference of the European Chapter of the Association for Computational Linguistics: Main Volume* (pp. 171-186). Link: https://aclanthology.org/2021.eacl-main.13

Mozes, M., Bartolo, M., Stenetorp, P., Kleinberg, B. and Griffin, L., 2021, November. Contrasting Human-and Machine-Generated Word-Level Adversarial Examples for Text Classification. In *Proceedings of the 2021 Conference on Empirical Methods in Natural Language Processing* (pp. 8258-8270). Link: https://aclanthology.org/2021.emnlp-main.651/

Schwartz, C., Simon, M., Hudson, D., & Johnson, S. D. (2021). Law Breaking and Law Bending: How International Migrants Negotiate with State Borders. *International Studies Quarterly*, *65*(1), 184-196.

Soldner, F., Kleinberg, B., & Johnson, S. (2022). Trends in online consumer fraud: A data science perspective. In *A Fresh Look at Fraud* (pp. 167-191). Routledge.

Soldner, F., Tanczer, L. M., Hammocks, D., Lopez-Neira, I., & Johnson, S. D. (2021). Using Machine Learning Methods to Study Technology-Facilitated Abuse: Evidence from the Analysis of UK Crimestoppers' Text Data. In *The Palgrave Handbook of Gendered Violence and Technology* (pp. 481-503). Palgrave Macmillan, Cham.

Soldner, F., Kleinberg, B., & Johnson, S.D. (2021). Confounds and Overestimations in Fake Review Detection: Experimentally Controlling for Product-Ownership and Data-Origin. *arXiv preprint arXiv:2110.15130.* (Pre-print – currently under review.)

Tompson, L., Steinbach, R., Johnson, S. D., Teh, C. S., Perkins, C., Edwards, P., & Armstrong, B. (2022). Absence of Street Lighting May Prevent Vehicle Crime, but Spatial and Temporal Displacement Remains a Concern. *Journal of Quantitative Criminology*, 1-21.

Tompson, L., Belur, J., Thornton, A., Bowers, K. J., Johnson, S. D., Sidebottom, A., ... & Laycock, G. (2021). How strong is the evidence-base for crime reduction professionals?. *Justice Evaluation Journal*, *4*(1), 68-97.

Trozze, A., Kamps, J., Akartuna, E.A. *et al.* Cryptocurrencies and future financial crime. *Crime Sci* 11**,** 1 (2022). https://doi.org/10.1186/s40163-021-00163-8

Trozze, A., Davies, T. and Kleinberg, B. (2022), "Explaining prosecution outcomes for cryptocurrency-based financial crimes", Journal of Money Laundering Control, Vol. ahead-of-print No. ahead-of-print. https://discovery.ucl.ac.uk/id/eprint/10141126/

Other Outputs

Talk at Infosecurity Europe in 2021 – What do we prioritise to manage third party risks?

Independent Anti-Slavery Commissioner & University of Nottingham. (2021, November). *Re-trafficking: The current state of play.*

Joint and Individual NGO Statements to Biological Weapons Convention, United Nations, Meetings of State Parties, Geneva, 22 – 25 November 2021. UN Web TV

Joint NGO Statement to Biological Weapons Convention, United Nations, Meetings of Experts, Geneva, 30 August – 8 September 2021. UN Web TV

Elgabry, M. (2021) Policy brief: Synthetic biology and future crime, Dawes Centre for Future Crime, UCL.

Elgabry, M. (2021) "National Machinery: Red-Teaming Approach Written Evidence." *UK Parliament Joint Committee on National Security and Machinery*, UK Parliament.

Conclusion

During the past twelve months the Dawes Centre has continued to make a demonstrative impact on the emerging and future crimes agenda. The Centre continues to establish itself in the crime and security landscape and this has been helped by the work put into strengthening existing external relationships and creating new ones. The Dawes Centre 'brand' is now relatively well established in the UK and so the goal over the next few years is to broaden that awareness overseas.

It is satisfying to be able to see this groundwork slowly turn into meaningful collaboration. There is clearly an ever-growing appetite for the Centre's work. With cybercrime and other forms of tech-enabled crime increasing at a terrifying pace, it is inevitable that law and order practitioners find themselves in a modern day 'arms race' to keep up – this is where the Dawes Centre seeks to add value. The aim over the next period is to continue to engage with external parties to determine key areas of research interest and to use the Centre's resources in a focused manner to carry out work that can help illuminate those areas.

Once again it is worth mentioning the Centre's strategic partnership with the CDT in Cybersecurity at UCL (co-directed by Prof Johnson) – with the UCL departments of Computer Science and STEaPP – which continues to examine a raft of cybersecurity research topics. The Dawes Centre for Future Crime at UCL will also fund work in the coming period on crime opportunities afforded by autonomous vehicles and the metaverse(s), and will carry out a conference around 'future fraud', all exciting initiatives.

As the world moves further into the new year, society is faced with yet more uncertainty. The Ukraine war, spiralling global economic concerns, and the lingering effects of the pandemic have placed security issues at the forefront of political and social agendas worldwide. Such turbulence seems set to continue for the forseeable future. One can only speculate that this presents yet further opportunities for criminals to exploit vulnerabilities occasioned by such uncertainty. Despite this, the coming period brings with it a sense of excitement and optimism for the Dawes Centre and its much-needed work.

.

Appendix 1

Governance of the centre

The Centre is governed through two principal mechanisms:

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 Lorenzo Pasculi (starting autumn 2022), Dr Manja Nikolovska (Researcher), Dr Nilufer Tuptuk (Lecturer), Mr Vaseem Khan (Project Manager).

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