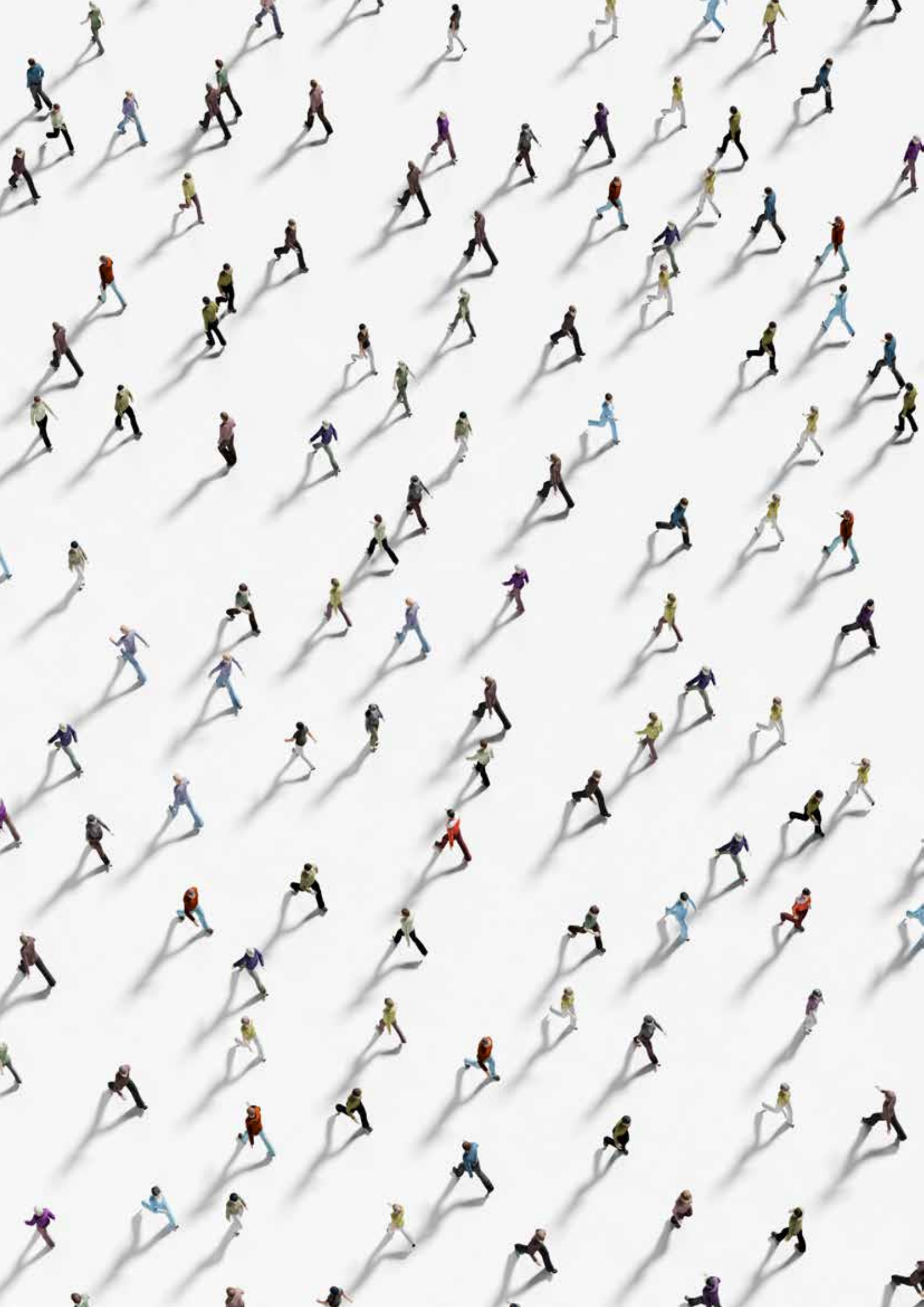
JILL DANDO INSTITUTE OF SECURITY AND CRIME SCIENCE
DAWES CENTRE FOR FUTURE CRIME AT UCL

UCL

DAWES CENTRE FOR FUTURE CRIME AT UCL

Annual Report

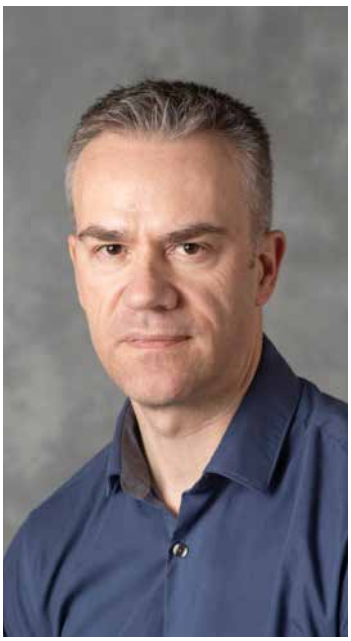
1 March 2022 – 28 February 2023



Contents

Executive Summary

Professor Shane Johnson, Director



The past year saw the world begin to recover from the devastating economic and social effects of the COVID pandemic, only to be then hit by multiple challenges caused by the ongoing war in Ukraine, fuel price rises, political turmoil, a burgeoning recession, widespread strike action, and the highest levels of inflation seen for a very long time. If anything, this has all underlined just how fragile our interconnected societies are in the face of global events. With such uncertainty, there comes risk – and opportunity – for both criminals and those seeking to mitigate their activities. More than ever it is important for us to look, as best we can, into the future and at emerging crime and security challenges

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. 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.

The Centre has continued to progress current projects and begin new ones. There is more information on these inside.

In 2022, again due to the impact of the pandemic, a full-scale annual conference could not be hosted, but instead the Centre hosted an online mini-conference entitled: ***Future Fraud***.

Summary of activities in the reporting period

Over the past year the Centre can report the following:

1 Completed projects

FOUR projects were completed during this period. (Note: Only two are shown in this report due to security sensitivity issues around the other two.)

2 Current projects

THREE projects began in the reporting period and are ongoing.

3 PhD projects

ONE new PhD student was recruited, carrying out doctoral research.

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 2022 to 28 February 2023. 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 sixth 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

The UK Computer Misuse Act 1990 and cases of technology-enabled domestic violence

This research evaluated 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.

Key Findings: Across two projects, over 500 cases were reviewed from three legal databases (January 2019 - May 2021). Tech abuse was found to be prevalent within the domestic abuse court cases analysed including via: phone (such as abusive text messages, phone calls, monitoring messages and contacts), social media, recording devices, CCTV in the home, and threats to release private sexual images. Our research showed that the CMA 1990 could have been applied to various cases, especially for those involving unauthorised access to their partner's messages and social media accounts and where perpetrators manipulated their partner's social media account, including deleting 'Facebook friends' and impersonating other men. The implications of our research point to the need for a clearer definition of tech abuse, due to the identified nuances of this form of abuse. To facilitate further research, as part of the project, we created an open-access database of the cases collated as part of this project. The database is hosted on the REPHRAIN website and will be made publicly available once our first article from this project is published.

Project Report: Stevens, F., Tanczer, L., Ridout, F., & Johnson, S. D. (2021). **The Applicability of the UK Computer Misuse Act 1990 onto Cases of Technology- Facilitated Domestic Violence and Abuse**. Home Office, University College London: London. Publication available here:

https://www.ucl.ac.uk/computer-science/sites/computer_science/files/the_applicability_of_the_uk_computer_misuse_act_1990_onto_cases_of_technology_facilitated_domestic_violence_and_abuse.pdf

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.

Systematic Review of Security and Privacy issues facilitated through non-mobile apps and app stores

The aim of this review, funded by the Department for Digital, Culture, Media and Sport (DCMS), was to inform DCMS's work on app security and privacy by conducting a review of recommendations suggested to improve the security and privacy of non-mobile apps and non-mobile app stores. This includes those linked to devices such as smart TVs, fitness, gaming and voice assistants. We used a systematic search methodology to review the academic literature and supplemented this with a review of open-source materials and "grey" literature that is not disseminated by academic publishers. Across the articles reviewed, authors identified a total of 11 types of security threats for which a total of ten recommendations were suggested for App stores and App developers.

Lead investigator(s):

Prof Shane Johnson,
Dawes Centre for Future Crime at UCL.

Dr Mariam Elgabry,
Dawes Centre for Future Crime at UCL.

2 Research Highlights: Current projects

Scoping study of the future crime challenges of the metaverse

The metaverse is an emerging convergence of technologies (e.g., virtual reality and blockchains) that enables users to experience mixed/ extended realities for various legitimate purposes (e.g., gaming, tourism, manufacturing and education). This scoping study brought together academics, researchers, industry, government, law enforcement and the voluntary sector to consider the emerging and future crimes that the metaverse might facilitate. Participants were asked to consider the likely success of these new types of crimes, crime surface scalability, skills set required, economic motivations and what should be done to prevent them. Two workshops were conducted – one held in London, the other in Singapore (hosted by INTERPOL). As a result of a systematic review of the literature and discussions at the workshops, 30 emerging crimes were identified. Participants were asked to rate these according to their risk, likelihood, achievability and the difficulty of defeating them. Ratings were largely consistent across the two workshops, with crimes of a sexual nature (e.g., child sexual abuse material), and crimes against the person (e.g., hate crime) being rated as presenting the highest future risks (i.e. being high harm and high frequency) and being the most difficult to address.

A briefing about the study was produced for Baroness Berridge (at her request) who raised the problems identified in the study in the House of Lords during discussions concerning the Online Safety Bill. The briefing was discussed at some length and Baroness Berridge noted that she had “learned much about future-proofing from the expert work of the Dawes Centre for Future Crime at UCL” and that there was a need to consider the difference between “content” and “conduct” in the bill (as recommended in the briefing we provided). A PhD student has been recruited (funded by the EPSRC CDT in Cybersecurity at UCL) to start in September 2023 to work on the threats associated with child sex offending in the Metaverse (the crime threat identified as most harmful by workshop participants).

Lead investigator(s):

Professor Shane Johnson,
Dawes Centre for Future Crime at UCL.

Ms Juliana Gomez-Quintero,
UCL Security and Crime Science

Professor Herve Borrion,
UCL Security and Crime Science

Professor Samantha Lundrigan,
Anglia Ruskin University

Crime enabled by autonomous vehicles

According to Gartner, the number of vehicles with autonomous driving capability will reach 2.5 million by 2028. While autonomous vehicles, especially cars, promise to deliver many benefits including travel comfort, improved safety and a reduction in the number of road accidents and deaths due to human error, there are concerns around adoption including trust, privacy, reliability, liability, crime, security and resilience. Autonomous cars are highly connected vehicles that use large sets of data from a wide range of external and internal sensors – such as lidar, radar, cameras and ultrasonic sensors. Artificial intelligence (AI), especially machine learning (ML) techniques including deep learning (DL) have a critical role in processing these data to train and validate automation tasks and make real-time decisions to navigate through traffic effectively and safely. Unfortunately, the new technology that enables autonomous cars, including the operating environment and supporting infrastructure is vulnerable to cyber-attacks. Moreover, we are yet to understand how criminals might monetise (or otherwise benefit from) attacks against autonomous vehicles or use them as a tool for crime.

Possible security threats include coordinated attacks using multiple autonomous vehicles, exploiting autonomous vehicles as weapons, attacking other vehicles such as police cars, using ransomware for extortion, blocking roads, tunnels and other critical infrastructure, diverting traffic, stealing sensitive personal data and property, helping criminals escape or watch potential robbery locations, and cause collisions by hiding objects on the road.

Autonomous vehicles might also enable new crimes that we have not considered yet.

Consequently, this scoping study will bring together academics, researchers, industry, government, professionals and relevant professional bodies to consider the emerging and future crimes related to autonomous vehicle systems. The study will help to identify emerging crimes, and shape (and prioritise) future research directions to improve the security of future technological developments and legislation.

Lead investigator(s):

Dr Nilufer Tuptuk,
UCL Security and Crime Science.

Computer Misuse-Facilitated Fraud (CMFF)

This project, funded by the Home Office, will inform understanding of computer misuse-facilitated fraud (CMFF). It will involve a systematic search of relevant literature and case law and a workshop with stakeholders to understand what we know about the prevalence of CMFF, and what data might be used to estimate this. It will explore what we know about how computer misuse offences facilitate fraud, and identify Future research and policy challenges.

Lead investigator(s):

Dr Lorenzo Pasculli,
Dawes Centre for Future Crime at UCL.

Dr Manja Nikolovska,
Dawes Centre for Future Crime at UCL.

Professor Shane Johnson,
Dawes Centre for Future Crime at UCL

NOTE: Current (ongoing) projects that have been featured in previous reports can be found on our website. They include:

- Smart Doorbell Evaluation

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 project(s) that began during the current reporting period are described below:

Developing an intervention to protect older people from cybercrime

According to the Home Office, the proportion of adults aged 75 and over that use the internet has almost doubled from 29% in 2013 to 54% in 2020. This represents a steep increase in the number of potentially susceptible targets accessible by malicious actors online. In fact, older people (60+) are victims of fraud more than any other crime, and there is general consensus that elderly victims can suffer disproportionate psychological distress, not forgetting significant economic losses. The COVID-19 pandemic is thought to have exacerbated this situation, with more vulnerable people, heightened vulnerability, and an additional context with which attackers can frame their approaches.

With particular attention paid to social engineering scams (which are tailor-made to exploit vulnerability and hence highly relevant for the older demographic), this research first seeks to analyse the current cyber vs elderly landscape using primarily the Crime Survey of England and Wales. Subsequently, after identifying the most appropriate problem area, the plan is to collaborate with stakeholders from across the banking, cybersecurity, policing and social care sectors in order to design a targeted and practicable response that protects older people from cyber-attacks.

PhD start year: 2022
PhD researcher: Ben Havers
PhD supervisors: Prof Claudia Cooper, UCL Psychiatry, and Dr Kartikeya Tripathi, UCL Security and Crime Science

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:

1. Crime, place and the internet
2. Biocrime
3. Cybercrime risks to London's future street infrastructure
4. The effects of cyberweapons
5. Detecting emerging crimes using data science techniques
6. Addressing Probable Child Sexual Abusers and Victim Profile Characteristics on Instagram
7. Identifying opportunities for crime prevention in smart cities and evaluating their social acceptability
8. Money laundering and terrorist financing future directions
9. Guarding against Adversarial Perturbation in Automated Security Algorithms
10. Horizon scanning through computer-automated information prioritisation
11. Refugee Flows and Instability
12. Detection and Mitigation of Financial Fraud in the Cryptocurrency Space
13. Anomaly detection for security
14. Protecting the UK's News propagation systems against the threat of "deepfake" injection
15. Intelligent biomaterials for the development of high-performance label free biosensors to combat crime
16. Hybrid threats
17. Automated profiling of user vulnerabilities to online deception and intervening through dynamic user interfaces
18. Human trafficking, digitalisation and a global pandemic: how has technology changed the face of human trafficking?
19. Brexit and Crime
20. Deterring Criminal and Terrorist Planning
21. Project Terabytes; The role of social media intelligence in organised crime investigations involving child criminal exploitation
22. Take Back Control: Data Democracy with a Pro-Consumer Bias
23. Ethical and Explainable Machine Learning for Child Protection from Online Abuse
24. Young People, Drugs and Social Media
25. Technology facilitated abuse within intimate partner relationships
26. Measuring and Countering Present and Future Crimes Facilitated by Consumer IoT Devices
27. Small to Medium Enterprises and Cyber Vulnerabilities
28. Cybersecurity of Small and Medium Enterprises

PhD Publications

During the reporting year, our PhD researchers have published articles on their research in peer-reviewed journals. Brief summaries of these, organised by themes, are provided below to give a flavour of the doctorate work carried out at the Centre.

Future of Money Laundering

Akartuna, E.A., Johnson, S.D. & Thornton, A.E. (2022). The money laundering and terrorist financing risks of new and disruptive technologies: a futures-oriented scoping review. *Security Journal*, 36, 615-650.

New and disruptive technologies, including cryptocurrencies and new payment methods, are revolutionising the way people engage with finance. Although they provide significant benefits to consumers, they are also inadvertently creating new money laundering and terrorist financing risks. This paper examines the risks that are, or are predicted to be, prevalent in three technology sectors—distributed ledger technologies (including cryptocurrencies), new payment methods and financial technologies (FinTech), through a systematic scoping review process. Specifically, the paper identifies enablers of both crimes, the precise criminal methods they might facilitate, at-risk stakeholders (of exploitation and/or complicity) and risk characteristics. The study involves systematic scoping reviews of the academic and futures literatures as well as a consultation exercise with experts to assess the likely veracity of the findings. In addition to identifying an array of specific risks, we identify six underlying trends that facilitate them. We discuss these, their policy implications, future directions for research and their benefit for conducting risk assessments to assess forthcoming technological developments.

Akartuna, E. A., Johnson, S. D., & Thornton, A. (2022). Preventing the money laundering and terrorist financing risks of emerging technologies: An international policy Delphi study. *Technological Forecasting and Social Change*, 179, 121632.

Financial innovation and technological advances are growing at a pace unrivalled by any other period in history. However, as more stakeholders enter these markets, criminals are exploiting their inadvertent security deficiencies to launder illicit funds or finance terrorism. This three-round policy Delphi study involved consultations with 52 experts from different industries and countries to understand future risk-prone technological developments, possible prevention measures and relevant stakeholders. Results highlight a range of money laundering and terrorist financing risks being enabled by advances in distributed ledger technologies (predominantly through cryptocurrencies), new payment methods and financial technology (FinTech). These threats include privacy-enhanced cryptoassets, transaction laundering, e-currencies and digital-only financial services. Findings also suggest that detection-based countermeasures (currently the primary preventative approach) can be coupled with more diverse countermeasures to increase effectiveness. However, the unique circumstances and constraints specific to different stakeholders will affect the nature, utility, and extent to which they can implement certain countermeasures. As such, a ‘one-size-fits-all’ approach to prevention is undesirable. Drawing on expert insight from the study, we propose a framework and a 3-point standard of implementation to motivate cost-effective, user-friendly, and innovation-friendly measures to improve suspicious activity detection and futureproof technologies before their criminal exploitation becomes mainstream.

Future Threats associated with Biotechnologies

Elgabry, M., Nesbeth, D., Johnson, S., (2022), The Future of Biotechnology Crime: A Parallel Delphi Study with Non-Traditional Experts, *Futures*, 102970.

The way science is practiced is changing and forecasting biotechnology crime trends remains a challenge as future misuses become more sophisticated. A parallel Delphi study was conducted to elicit future biotechnology scenarios from two groups of experts. Traditional experts, such as professionals in national security/intelligence, were interviewed. They were asked to forecast emerging crime trends facilitated by biotechnology and what should be done to safeguard against them. Non-traditional experts, such as “biohackers” who experiment with biotechnology in unexpected ways, were also interviewed. The study entailed three rounds to obtain consensus on (i) biotechnology misuse anticipated and (ii) potential prevention strategies expected.Traditional and non-traditional experts strongly agreed that misuse is anticipated within the cyber-infrastructure of, for example, medical devices and hospitals, through breaches and corporate espionage. Preventative steps that both groups strongly advocated involved increasing public biosecurity literacy, and funding towards addressing biotechnology security. Both groups agreed that the responsibility for mitigation includes government bodies. Non-traditional experts generated more scenarios and had a greater diversity of views.

Future and emerging threats associated with Artificial Intelligence

Eusebi, A., Vasek, M., Cockbain, E., & Mariconti, E. (2022, June). The ethics of going deep: Challenges in machine learning for sensitive security domains. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 533-537). IEEE.

Sometimes, machine learning models can determine the trajectory of human life, and a series of cascading ethical failures could be irreversible. Ethical concerns are nevertheless set to increase, in particular when the injection of algorithmic forms of decision-making occurs in highly sensitive security contexts. In cybercrime, there have been cases of algorithms that have not identified racist and hateful speeches, as well as missing the identification of Image Based Sexual Abuse cases. Hence, this paper intends to add a voice of caution on the vulnerabilities pervading the different stages of a machine learning development pipeline and the ethical challenges that these potentially nurture and perpetuate. To highlight both the issues and potential fixes in an adversarial environment, we use Child Sexual Exploitation and its implications on the Internet as a case study, being 2021 its worst year according to the Internet Watch Foundation.

Mozes, M., Kleinberg, B. and Griffin, L., 2022, December. Identifying Human Strategies for Generating Word-Level Adversarial Examples. In *Findings of the Association for Computational Linguistics: EMNLP 2022* (pp. 6118-6126).

Adversarial examples in NLP are receiving increasing research attention. One line of investigation is the generation of word-level adversarial examples against fine-tuned Transformer models that preserve naturalness and grammaticality. Previous work found that human- and machine-generated adversarial examples are comparable in their naturalness and grammatical correctness. Most notably, humans were able to generate adversarial examples much more effortlessly than automated attacks. In this paper, we provide a detailed analysis of exactly how humans create these adversarial examples. By exploring the behavioural patterns of human workers during the generation process, we identify statistically significant tendencies based on which words humans prefer to select for adversarial replacement (e.g., word frequencies, word saliencies, sentiment) as well as where and when words are replaced in an input sequence. With our findings, we seek to inspire efforts that harness human strategies for more robust NLP models.

Soldner, F., Kleinberg, B., & Johnson, S. D. (2022). Confounds and overestimations in fake review detection: Experimentally controlling for product-ownership and data-origin. *Plos One*, 17(12), e0277869.

The popularity of online shopping is steadily increasing. At the same time, fake product reviews are published widely and have the potential to affect consumer purchasing behaviour. In response, previous work has developed automated methods utilizing natural language processing approaches to detect fake product reviews. However, studies vary considerably in how well they succeed in detecting deceptive reviews, and the reasons for such differences are unclear. A contributing factor may be the multitude of strategies used to collect data, introducing potential confounds which affect detection performance. Two possible confounds are data-origin (i.e., the dataset is composed of more than one source) and product ownership (i.e., reviews written by individuals who own or do not own the reviewed product). In the present study, we investigate the effect of both confounds for fake review detection. Using an experimental design, we manipulate data-origin, product ownership, review polarity, and veracity. Supervised learning analysis suggests that review veracity (60.26–69.87%) is somewhat detectable but reviews additionally confounded with product-ownership (66.19–74.17%), or with data-origin (84.44–86.94%) are easier to classify. Review veracity is most easily classified if confounded with product-ownership and data-origin combined (87.78–88.12%). These findings are moderated by review polarity. Overall, our findings suggest that detection accuracy may have been overestimated in previous studies, provide possible explanations as to why, and indicate how future studies might be designed to provide less biased estimates of detection accuracy.

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

Following the advent of the Internet, the interaction between sellers and consumers is increasingly shifting from a face-to-face towards an online environment. This chapter examines what online consumer fraud is, revisiting the definition and common fraud schemes. It reviews some of the current approaches non-governmental and commercial institutions take to detect and prevent online consumer fraud. The chapter discusses darknet markets – internet platforms that, amongst other things, sell both legal and illicit goods while providing anonymity – and how they facilitating online consumer fraud. It closes with a discussion of how methods from data science can be applied to support the detection and prevention of online consumer fraud. The dark web represents a small portion of the deep web, on which users and hosts are anonymized.

Future and emerging threats associated with Cryptocurrencies

Trozze, A., Kamps, J., Akartuna, E.A. et al. (2022). Cryptocurrencies and future financial crime. *Crime Science*, 11, 1.

Background: Cryptocurrency fraud has become a growing global concern, with various governments reporting an increase in the frequency of and losses from cryptocurrency scams. Despite increasing fraudulent activity involving cryptocurrencies, research on the potential of cryptocurrencies for fraud has not been examined in a systematic study. This review examines the current state of knowledge about what kinds of cryptocurrency fraud currently exist, or are expected to exist in the future, and provides comprehensive definitions of the frauds identified.

Methods: The study involved a scoping review of academic research and grey literature on cryptocurrency fraud and a 1.5-day expert consensus exercise. The review followed the PRISMA-ScR protocol, with eligibility criteria based on language, publication type, relevance to cryptocurrency fraud, and evidence provided. Researchers screened 391 academic records, 106 of which went on to the eligibility phase, and 63 of which were ultimately analysed. We screened 394 grey literature sources, 128 of which passed on to the eligibility phase, and 53 of which were included in our review. The expert consensus exercise was attended by high-profile participants from the private sector, government, and academia. It involved problem planning and analysis activities and discussion about the future of cryptocurrency crime.

Results: The academic literature identified 29 different types of cryptocurrency fraud; the grey literature discussed 32 types, 14 of which were not identified in the academic literature (i.e., 47 unique types in total). Ponzi schemes and (synonymous) high yield investment programmes were most discussed across all literature. Participants in the expert consensus exercise ranked pump-and-dump schemes and ransomware as the most profitable and feasible threats, though pump-and-dumps were, notably, perceived as the least harmful type of fraud.

Conclusions: The findings of this scoping review suggest cryptocurrency fraud research is rapidly developing in volume and breadth, though we remain at an early stage of thinking about future problems and scenarios involving cryptocurrencies. The findings of this work emphasise the need for better collaboration across sectors and consensus on definitions surrounding cryptocurrency fraud to address the problems identified.

Trozze, A., Davies, T. and Kleinberg, B. (2022). Explaining prosecution outcomes for cryptocurrency-based financial crimes, *Journal of Money Laundering Control*, 26(1), 172-188.

Purpose: Cryptocurrencies have been used to commit various offences, but enforcement efforts remain underdeveloped relative to the value of these crimes. This paper aims to examine factors associated with outcomes of US-based cryptocurrency financial crime prosecutions.

Design/methodology/approach: The authors studied the 37 resolved cryptocurrency-based financial crime cases in the USA to date, exploring the impact of offence, defendant and evidence characteristics on the mode of disposition and penalties. The authors used bivariate analyses and logistic regression models to determine relationships among these variables.

Findings: The presence of individual defendants only (rather than a corporate defendant or combination thereof) and the use of only a cryptocurrency other than Bitcoin in committing a crime each made a case less likely to be resolved by dismissal, trial or summary or default judgement.

Originality/value: This paper is the first to examine variables contributing to financial crime prosecution outcomes and has implications for prosecutorial decision-making, resource allocation and the prevention and detection of financial offences involving cryptocurrencies.

Human detection of phishing emails

Zheng, S. and Becker, I. (2022). Presenting suspicious details in User-Facing e-mail headers does not improve phishing detection. In the *Proceedings of the Eighteenth Symposium on Usable Privacy and Security (SOUPS),* Boston, MA, U.S.

Phishing requires humans to fall for impersonated sources. Sender authenticity can often be inferred from e-mail header information commonly displayed by e-mail clients, such as sender and recipient details. People may be biased by convincing e-mail content and overlook these details, and subsequently fall for phishing. This study tests whether people are better at detecting phishing e-mails when they are only presented with user-facing e-mail headers, instead of full emails. Results from a representative sample show that most phishing e-mails were detected by less than 30% of the participants, regardless of which e-mail part was displayed. In fact, phishing detection was worst when only e-mail headers were provided. Thus, people still fall for phishing, because they do not recognize online impersonation tactics. No personal traits, e-mail characteristics, nor URL interactions reliably predicted phishing detection abilities. These findings highlight the need for novel approaches to help users with evaluating e-mail authenticity.

Teaching

The Centre's teaching offering 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.

Our teaching programme encourages students to think about the future crime implications of technological and other changes. Modules help reinforce external relationships. For instance, for one of the modules, students produce horizon scanning posters which are presented annually at the Home Office. This module 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.

Some of the topics that students have produced horizon scanning reports on include the threats associated with ChatGPT, autonomous vehicles, and drone swarms.

Photo: Dr Mariam Elgabry

PhD training

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 instil, 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.

Here **Mariam Elgabry,** a recent graduate from the programme, describes her experience:

"I had the privilege of pursuing my PhD at the Dawes Centre, which surpassed all my expectations. Being located at the heart of London, the Centre provided an ideal location for my research, which focused on the future of biotechnology crime. With a passion for real-world problem-solving, I was thrilled to find a department that prioritized practitioner-oriented research, enabling me to work with stakeholders such as the UK Home Office, London Metropolitan police, counter-terrorism units, and medical device regulatory bodies. This gave me an opportunity to see the impact of my research in real-time and collaborate with experts from different fields.

One of the most fulfilling experiences at the Dawes Centre was conducting fieldwork with biohackers and developing a framework for product design with crime science in mind. My work was recognized by the United Nations, and I was honoured to present my research at their forum. This also led to me being awarded prestigious fellowships at John's Hopkins, which allowed me to continue my research and collaborate with other experts in the field.

Starting my own venture using the skills and knowledge gained from my research at the Dawes Centre was an exciting opportunity to make a tangible impact in the world. I am proud to have published several papers and secured my first patent. Additionally, I was thrilled to receive speaking opportunities at conferences and to travel extensively.

The support and supervision I received from the faculty were exceptional. Despite the challenges of conducting PhD research, I had the flexibility to pursue my research in creative ways that worked best for me. The international peer group was equally supportive, and I made lifelong friends and colleagues who continue to inspire me.

Overall, I highly recommend the Dawes Centre to anyone looking for an interdisciplinary, supportive, and collaborative environment to pursue their PhD. The resources, support, and opportunities provided by the Centre are truly exceptional, and I am grateful for the role they played in shaping my career and life."

Best,
Dr. Mariam Elgabry

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 consultancies, 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 following briefings can be downloaded from the Centre's website:

- Older adults as victims of online financial crime
- Synthetic biology and future crime
- Cryptocurrencies and future crime
- AI-enabled future crime
- How secure is consumer IoT?
- Challenges of preventing counterfeit goods

The following policy report is also available:

- Network and Information Systems: Improving Implementation

Impact Highlights

Future Fraud conference

On 12 July 2022, the Centre organised and hosted an online conference on future fraud. The ongoing digital revolution is transforming the way we live, work and interact. But these same changes are opening up countless new ways for criminals to exploit vulnerabilities. New forms of online fraud – or old fraud enacted using new digital methods – are growing exponentially, from cryptocurrency scams to identity theft to tailored ransomware attacks. The problem will be exacerbated as we enter the new 'metaverse' era where we interact and carry out activities in virtual worlds. This free-to-attend event featured a range of speakers addressing current themes in this space. Industry and policy practitioners came together with academic speakers to examine this pervasive crime and how it will continue to evolve in the coming years.

The conference was divided into two key sessions:

- **Session 1 – "What more can governments do to combat future fraud?"**
- **Session 2 – "How will the metaverse enable new forms of fraud?"**

Talks and speakers included:

- *Behind the Criminal Economy: What money laundering myths and models tell us about our past, our present, and our future fight against economic crime by* Rian Matanky-Becker: Head of Economic Crime Policy and Engagement, HMRC
- *Examining people's ability to identify real and artificially synthesised faces by* Dr Sophie Nightingale: Dept of Psychology, Lancaster University
- *Developing Respectful and Capability-centred AI to Prevent Phone Call Fraud with Older Adults* by Dr Peter Novitzky: UCL Dept of Science, Technology, Engineering and Public Policy (STEaPP)
- *Detecting DeFi Securities Violations from Token Smart Contract Code by* Arianna Trozze: Consultant and UCL Cybersecurity Centre for Doctoral Training

External engagement

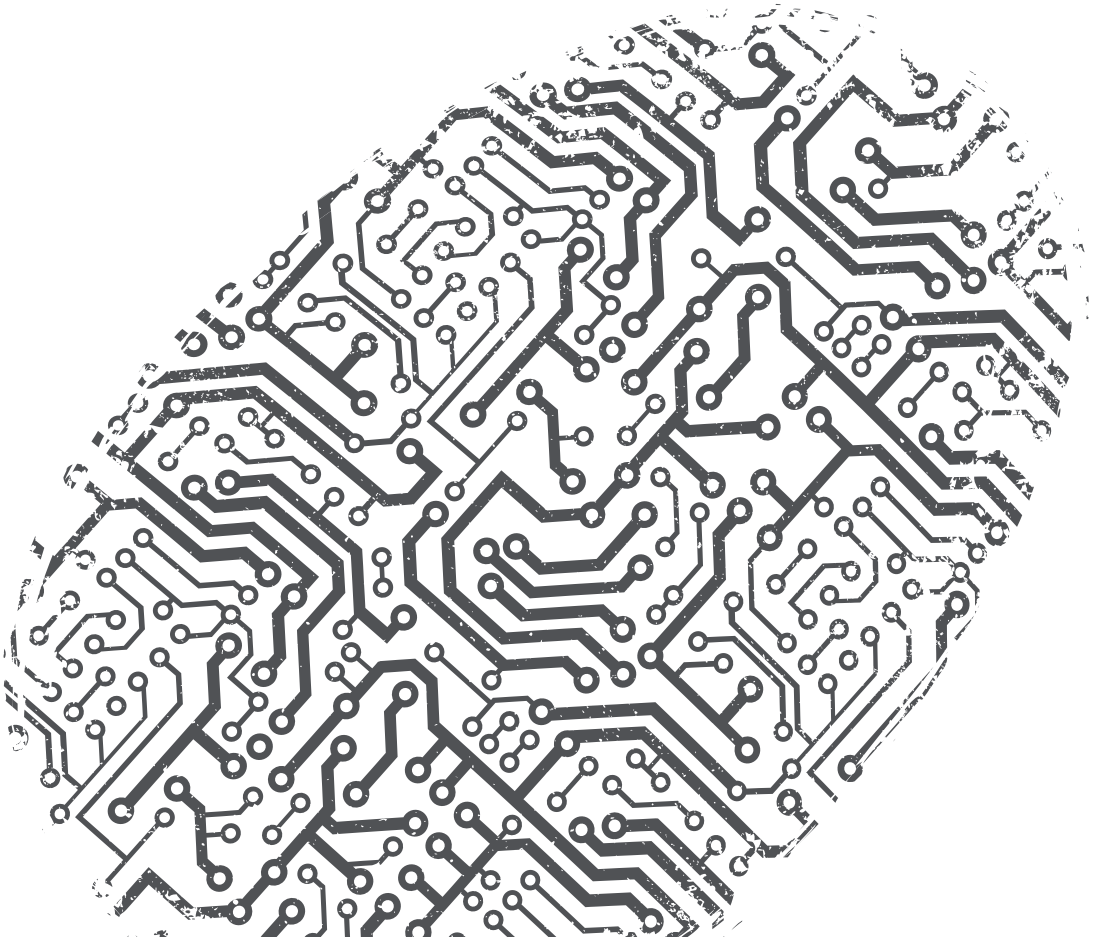
Engagement with other research centres and agencies continued to help the Centre better understand current initiatives in the future crime problems space and offers opportunities for collaboration. Engagement activities include stakeholder "sandpits" workshops, which are conducted as part of scoping research, seminars organised with and for the Home Office, stakeholder involvement in research projects, guest lectures on taught programmes, and input to PhD research.

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.

- Akartuna, E.A., Johnson, S.D. & Thornton, A.E. The money laundering and terrorist financing risks of new and disruptive technologies: a futures-oriented scoping review. *Secur J* (2022).
- Akartuna, E. A., Johnson, S. D., & Thornton, A. (2022). Preventing the money laundering and terrorist financing risks of emerging technologies: An international policy Delphi study. *Technological Forecasting and Social Change*, *179*, 121632.
- Elgabry, M., Nesbeth, D., Johnson, S., (2022), The Future of Biotechnology Crime: A Parallel Delphi Study with Non-Traditional Experts, *Futures*, 102970, ISSN 0016-3287.
- Elgabry, M., and Johnson, S.D. (2022). Review of security and privacy recommendations for non-mobile apps and app stores. Department for Digital, Culture, Media and Sport: London.
- Available at: https://www.gov.uk/government/publications/review-of-security-and-privacy-recommendations-for-non-mobile-apps-and-app-stores
- Eusebi, A., Vasek, M., Cockbain, E., & Mariconti, E. (2022, June). The ethics of going deep: Challenges in machine learning for sensitive security domains. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 533-537). IEEE.
- Frith, M. J., Bowers, K. J., & Johnson, S. D. (2022). Household occupancy and burglary: A case study using COVID-19 restrictions. *Journal of Criminal Justice*, 101996.
- C. Grasso, D. Ring, & L. Pasculli (eds.) (2022) Special issue 'Tax Evasion, Corruption and the Distortion of Justice'. 85(4) Law & Contemporary Problems.
- Johnson, S.D., Nikolovska, M. (2022) The Effect of COVID-19 Restrictions on Routine Activities and Online Crime. *Journal of Quantitative Criminology, advanced online access.*
- Mozes, M., Kleinberg, B. and Griffin, L., 2022, December. Identifying Human Strategies for Generating Word-Level Adversarial Examples. In *Findings of the Association for Computational Linguistics: EMNLP 2022* (pp. 6118-6126).
- Nikolovska, M., & Johnson, S.D. (2022). Covid-19 and Future Threats: A Law Enforcement Delphi Study. London: Dawes Centre for Future Crime at UCL
- L. Pasculli & B. Stanford (2023) 'Forma e flessibilità: la normalizzazione delle "sanzioni Magnitsky" nel rispetto della legalità negli U.S.A., in Canada, nel Regno Unito ed in Australia'. Translation by Giulio Vinciguerra. 1 Diritto Penale XXI Secolo 53-96
- L. Pasculli & S. MacLennan (2022) 'The Producers of Tax Abuse: The Corrupting Effects of Tax Law and Tax Reliefs in the U.K. Film Industry'. 85(4) Law & Contemporary Problems 101-136
- L. Pasculli & B. Stanford (2022) 'Form and Flexibility: The Normalisation of 'Magnitsky Sanctions' in the Face of the Rule of Law'. 15(1) The Hague Journal of the Rule of Law 109-142.
- Soldner, F., Kleinberg, B., & Johnson, S. D. (2022). Confounds and overestimations in fake review detection: Experimentally controlling for product-ownership and data-origin. *Plos one*, *17*(12), e0277869.
- 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.

- 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.
- Trozze, A., Kamps, J., Akartuna, E.A. et al. Cryptocurrencies and future financial crime. Crime Sci 11, 1 (2022).
- 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.
- Zheng, S. and Becker, I. 2022. Presenting suspicious details in User-Facing e-mail headers does not improve phishing detection. In Eighteenth Symposium on Usable Privacy and Security.



Conclusion

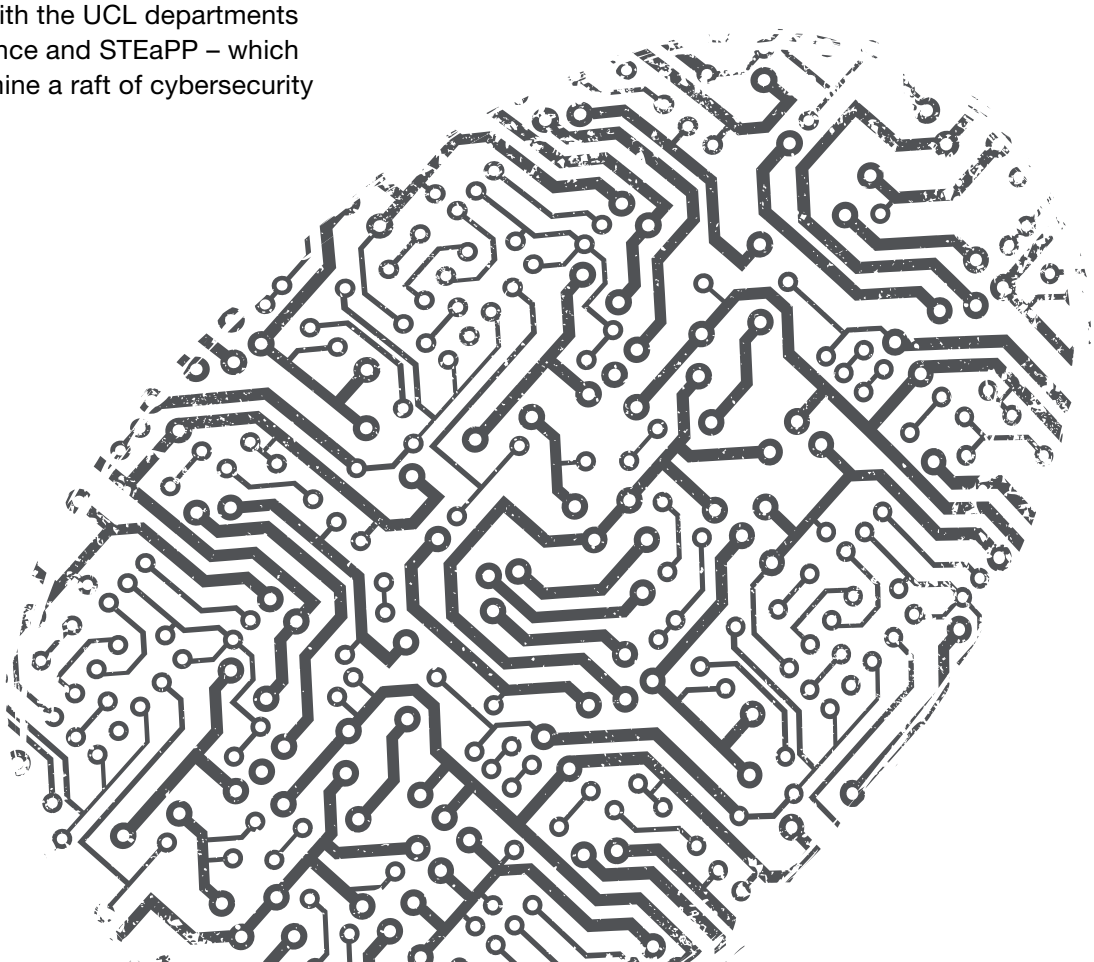
During the past twelve months the Dawes Centre has continued to build on earlier work, launching several new projects while bringing others to completion. The Centre is now well established in the UK and increasingly well known overseas.

There is an ever-growing appetite for the Centre's expertise. With cybercrime and other forms of tech-enabled crime continuing to be the drivers of law enforcement – and, increasingly, private sector – activity, the Dawes Centre is now being sought out and funded to complete a variety of projects. For instance, this past year saw us collaborate with several large private and public sector organisations (such as BP, Aston Martin and the Driving Standards Authority) to work on a scoping study examining "Crime enabled by Autonomous Vehicles". This groundbreaking work will be of widespread interest as autonomous vehicles become a reality on our streets in the coming decades.

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.

In the coming period the Centre will launch several new projects around understanding and addressing emerging fraud problems, including looking at how law enforcement use social media in relation to fraud, and what can be learned from posts from the public. The Centre's annual conference will return to a physical setting, in London. The theme will be "Organised crime: the present and the future."

The Ukraine war and economic uncertainty continue to create a turbulent environment, one in which crime and security issues remain prominent. Advances in generative AI have the potential to disrupt many aspects of our lives. As ever, criminals will seek to exploit societal vulnerabilities and technology, at the macro and micro levels. The Dawes Centre will continue to respond through the use of science and technology.



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 Pasculli (Deputy Director, started autumn 2022), Dr Manja Nikolovska (Researcher), Dr Nilufer Tuptuk (Lecturer), Mr Vaseem Khan (Project Manager).