



DAWES CENTRE FOR FUTURE CRIME AT UCL

ANNUAL REPORT

1 MARCH 2017 – 28 FEBRUARY 2018

Contents

- 1. Foreward by Professor Shane Johnson, Director**
- 2. Background to the centre**
- 3. Governance of the centre**
- 4. Summary of activities in the reporting period**
- 5. Research highlights**
 - **Completed projects**
 - **Current projects**
 - **PhD projects**
- 6. Teaching**
- 7. External engagement**
- 8. Publications**
- 9. Conclusion**

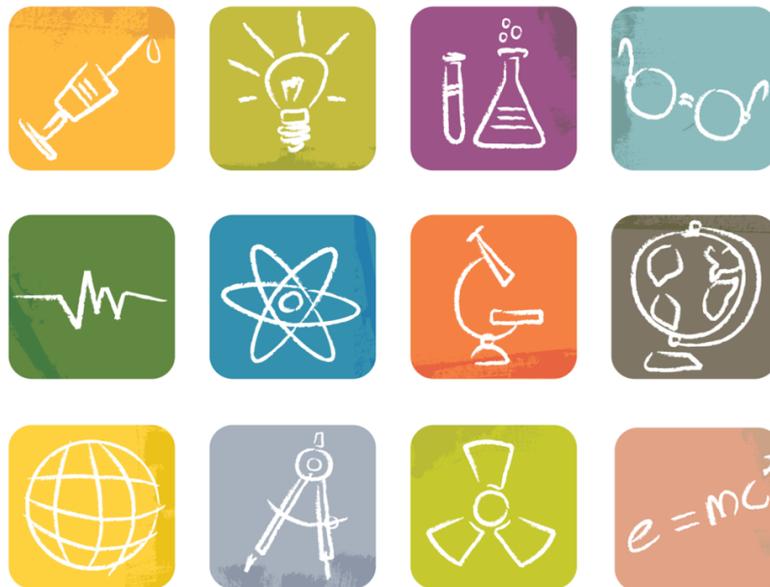
Foreward

Professor Shane Johnson, Director



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 2017 to 28 February 2018. 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 first full year of activity of the centre. In this period we have built up significant momentum, promoting our research and impact agenda, raising the profile of the Centre, and initiating exciting new research projects that address a variety of issues from a range of disciplinary perspectives. Engagement with the Centre, by academics, practitioners, or other stakeholders, has been welcome and significant. As we start to deliver outputs from the Centre's research, the participation of our network of stakeholders will become ever more important. We have found ourselves engaged in thought-provoking discussions with researchers from many disciplines including synthetic biology, materials discovery, and artificial intelligence, with half of the scoping studies we originally planned to fund already underway. We look forward to working with all of our partners in the coming year to realise the real-world impact of our work.



Background to the Centre

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

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



Key activities

Activities key to achieving the Centre's mission include:

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

Governance of the centre

The Centre is governed through three principal mechanisms:

The Executive Committee (EC)

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

- The Dawes Trust - Sir Stephen Lander, John Graham, and Stephen Webb,
- Independent advisors – Sir Richard Broadbent (Business Sector), Professor Andy Bell (Home Office Centre for Applied Science and Technology), and Simon Ruda (Behavioural Insights Team), and
- UCL - Professor Richard Wortley (Head of UCL Security and Crime Science and Committee Chair), Professor Nigel Titchener-Hooker (Dean of the Faculty of Engineering Sciences), and Professor Shane Johnson (Director of the Dawes Centre for Future Crime at UCL).

The Advisory Board (AB)

The AB comprises the following members.

Simon Parr QPM	Ex-Chief Constable Cambridge Police
Chris Rampton	Chief Technical Officer Centre for Applied Science and Technology (CAST).
Prof Dave Delpy	Chair of the UK Quantum Technology Strategic Advisory Board, former Chair of the Defence Scientific Advisory Council (DSAC) and former CEO of the Engineering and Physical Sciences Research Council.
Dr Emma Barrett	University of Manchester, Professor of Psychology, Security and Trust and strategic lead for Digital Trust and Security. Formerly a senior UK Government behavioural science adviser for national security. Associate of the Centre for Research and Evidence on Security Threats (CREST) at the University of Lancaster.
Dr Deeph Chana	Institute for Security Science & Technology, Imperial University. Previously a senior UK government science policy adviser on critical infrastructure security in Whitehall
Dan Greaves	Crime Director, UK Home Office

The Centre Management Team

This team comprises the Director, project manager, and Centre administrator.

Summary of activities in the reporting period

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

Research activities include (for full details please see the **Research Highlights** sections):

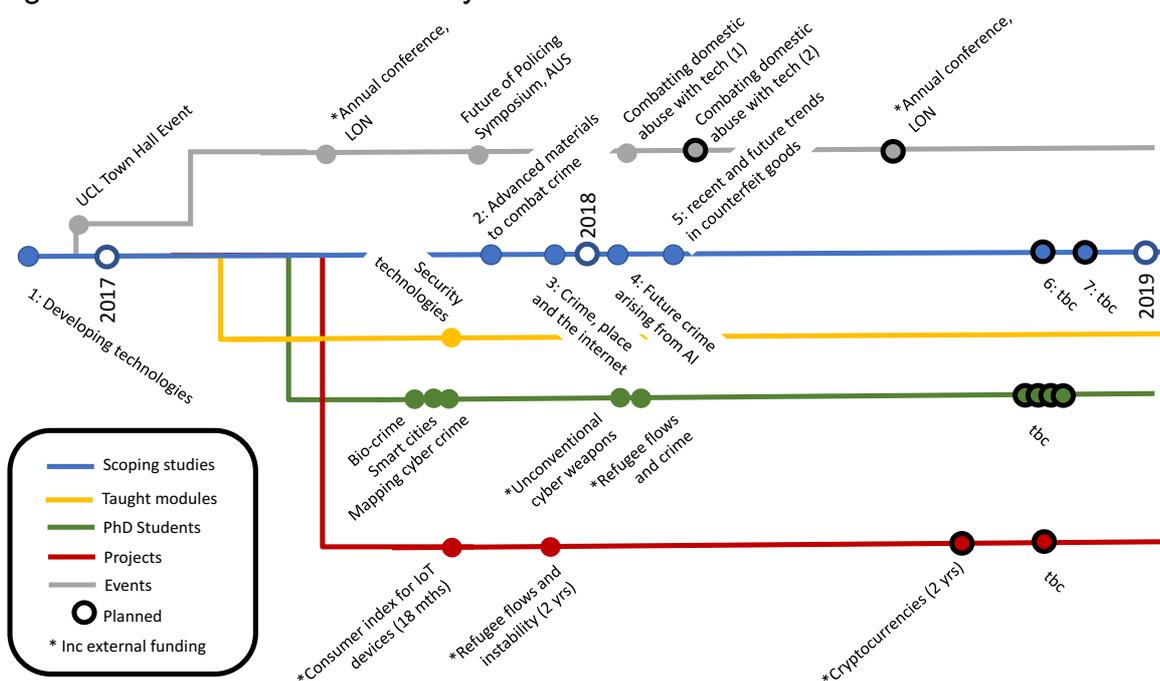
1. Completed projects – the first project of the Dawes Centre “Mapping the future: Scoping Study of Developing Technologies” was completed during this period. It identified a series of developing technologies, and mapped research at UCL on these topics.
2. Current projects – five new projects were initiated covering topics on crime and the Internet, the Internet of Things, counterfeit goods, amongst others.
3. PhD projects – each year we award a number of studentships for PhD research in areas of interest to the centre. This year PhD places were awarded for topics on bio-hacking, smart cities, cybercrime, and unconventional cyber weapons.

The year also saw us organise the first of a **series of conferences**, drawing in an impressive range of participants, including practitioners from the Home Office, National Crime Agency, and even the FBI.

We also launched the first of our taught modules, a new undergraduate module on Security Technologies, and developed a module on horizon scanning to be launched in the second term of the 2018 academic year. We summarise these modules in our **Teaching** section.

To provide a visual map of activity, Figure 1 below represents a “journey planner” to indicate the number and types of activity that are currently underway, along with their timing. These activities are described in more detail in the sections that follow.

Figure 1 – Dawes Centre Journey Planner



Research highlights

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

Projects will generally comprise two phases:



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



The aim of **Phase 2** projects is to complete original research intended to address a specific future crime problem, or to develop existing research to reach a technology readiness level suitable for deployment.

Research Highlights: Completed projects

Mapping the future: Scoping Study of Developing Technologies

Research

The discipline-based organisation of university departments means that science and engineering developments tend to be taken forward with scant regard to their social consequences in general or crime and security consequences, in particular. Project 1 comprised a series of work packages intended to produce a catalogue of emerging work in the science and engineering disciplines with implications for crime and security¹ and from this to inform recommendations for future investment by the Centre.

The first work package involved scanning key science/technology/engineering materials, including science newsfeeds and magazines, to identify developments in the broader scientific community that might inform the work of the Centre. Over a six-month period, items published on the Science Daily and BBC technology websites were read on a near-daily basis, and those published in the New Scientist on a weekly basis. Additional [ad-hoc] searches of 18 other publication sources including WIRED, Police Professional, and NESTA were also conducted. Articles identified were coded along several dimensions to tease out, for example, the potential crime and security implications of the work. This led to the identification of a set of developing technologies for prioritisation.

The second workpackage involved systematically searching the titles and abstracts of all papers published by UCL staff over the last four-years to identify work concerned either with crime and security, or the developing technologies identified in the first workpackage. These exercises were used to map out research activity at UCL with implications for the work of the Centre, and to identify key academics involved in these areas of work with whom discussions could be held to explore the implications of their research and potential scoping studies that might be conducted.

Lead investigators: [Professor Paul Ekblom](#), [Professor Shane Johnson](#), [Professor Gloria Laycock](#) (in alphabetical order)

Project findings

A series of developing technologies were identified, and research at UCL on these topics was summarized and mapped. A top-ten list of topic areas was produced, the contents of which are summarised below, to provide suggestions for projects that might be funded by the Centre over the next 12 months. The table provides a brief description of the technologies of interest, and the reason for their selection, along with an indication of the time horizon over which the technologies might impact upon crime (its commission or prevention).

¹ We use the word 'crime' henceforward but mean this to include volume crime, terrorism, organised crime and disorder.

Likely Time Horizon

Current to near term



Current to medium term

Near to medium term

Medium to long term

Long term



Phase 1 Scoping study

Phase 2 project

PhD student

Topic
<p>1. Crime, place and the Internet  </p> <p>In cities, analysis shows that crime clusters spatially. This has informed successful crime prevention. Can cyber-crime prevention be enhanced through similar insight?</p>
<p>2. Radar and scanning </p> <p>Advances in sensor technology increase what (e.g. counterfeit drugs) can be detected, advances in Artificial Intelligence (AI) can increase speed and coverage.</p>
<p>3. Social networks and monitoring technology</p> <p>Advances in mobile technology and sensing enable people's physical and online activity to be tracked and correlated in real-time. This could be used for criminal purposes, but could also be used to "nudge" positive behaviour, or scan for emerging problems.</p>
<p>4. IoT – Industrial and domestic devices/autonomous vehicles, smart cities  </p> <p>Electronic devices are increasingly internet enabled which presents opportunities to enhance people's quality of life but also risks increasing criminal activity.</p>
<p>5. Smart technology and artificial intelligence  </p> <p>Advances enable artificial systems to learn rather than follow instructions. This revolution, along with the proliferation of "smart devices" which enable sensing at low cost (e.g. Amazon Alexa) dramatically increases their potential for positive and criminal applications.</p>
<p>6. Wireless technology</p> <p>Next generation wireless technologies (e.g. 5G) are intended to enable faster data transfer, minimise energy consumption and allow wireless energy transfer. Ambient signals can also be used to detect and track activity in enclosed spaces.</p>
<p>7. Nano materials </p> <p>Nano materials (including Graphene) have tiny components. Their structural properties enable the manufacture of lightweight, resilient materials with embedded sensors. Such materials have clear implications for combating crime.</p>
<p>8. Synthetic biology including CRISPR </p> <p>CRISPR allows DNA editing and the manipulation of biological circuits. Current applications are in medicine and crops, possible applications include DNA as a storage medium. Potential implications are profound. Example crimes include gene doping, and narcotic crop mutation, while genetic tagging may help track and prevent the theft of industrial material</p>
<p>9. Blockchain</p> <p>The blockchain is an electronic, open, distributed ledger system used to verify and record transactions securely. It may fundamentally change economic and other transaction-based systems (e.g. the Land Registry), making them more secure. However, vulnerabilities might be exploited.</p>
<p>10. Quantum computing</p> <p>Quantum computing would enable complex computations (currently intractable) to be completed efficiently. Effects would be pervasive as current methods of encryption (which secure the internet) would be threatened. Quantum cryptography would address this.</p>

The above table indicates the types of research projects the Centre is now funding and the broad topics on which they focus. Other projects will be initiated over the coming year.

Research Highlights: Current projects

Crime, place and the Internet

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

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

Lead investigator(s): [Dr Toby Davies](#), [Dr Gianluca Stringhini](#)

Advanced Materials to Combat Crime

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

This project will consider the potential of various advanced material technologies to combat crime. The intention is to work out what applications are desirable, over what timescales their production is plausible, and what is required to make the exploitation of advanced materials for combatting crime feasible. Part of this scoping study involves the identification of current approaches used by law enforcement, and the discussion of these with relevant stakeholders and industrial partners to identify user-need, potential developments and the likely timescales and costs required for production.

Lead Investigator(s): [Dr Kwang-Leong Choy](#)

Future Crime opportunities arising from Artificial Intelligence (AI)

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

- Identity Forgery – AI methods can generate speech in a target’s voice given a sample and couple it with synthesized video of them speaking. A senior citizen could be tricked into making financial transfers over video skype by an apparent trusted party.
- AI Snooping: Phones, PCs, TVs and Home Hubs provide the sensors for audio snooping inside homes. Speech Recognition can sift the resulting data for exploitable fragments (e.g. passwords or bank details, affairs being admitted to).
- Driverless Weapons: The driverless truck is close to the ideal urban attack robot for terrorists. GPS guidance could bring it to target, and Machine Vision could target pedestrians.

On the flip side, AI has potential for crime prevention. Most developed is Machine Perception in, for example, vehicle tracking, person recognition, and X-ray threat detection. However, all Deep Learnt vision systems so far studied are capable of being fooled by an adversary who has prior access to the software. This is achieved, not by hacking it, but by using AI methods to find its hidden weaknesses – minute *adversarial perturbations* of the input to the system that tip it into giving the wrong output. Understanding whether a



particular security-critical system is vulnerable, and addressing the weakness by, for example, ensuring the software is not physically present in purchasable security scanners (but instead runs from a remote server which is not accessible by an adversary) can guard against a lurking problem. This project seeks to examine the future crime potential of AI, and provide a basic taxonomy graded on scales of criminal profit, public harm, victim harm, effort, difficulty, and technology readiness.

Lead investigator(s): [Dr Lewis Griffin](#)

Scoping study on recent and future trends in counterfeit goods

Counterfeit products are big business, with an estimated value of half a trillion US dollars per year, and they can cause serious harms, including poor treatment of life threatening diseases, impaired pest control for food crops, and brand damage, to mention just a few. Counterfeiters have become increasingly proficient at producing authentic-looking products and/or packaging, honing their methods to the point where their products pass visual

inspection – the first line of defence. Thus, there is a growing need for fast analytical methods to test the chemical composition of the contents of such products. This project will carry out a scoping study to examine current and future trends in counterfeiting and to evaluate the technology that might be used to identify counterfeit goods.

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

Lead investigator(s): [Prof Robert Speller](#), [Richard Lacey](#) (Home Office CAST)

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

Internet enabled devices, including smart televisions, security cameras and thermostats, are now commonly found around the home. Devices such as these have enormous potential to transform society, but they also provide opportunities for crime. For example, some devices (including ‘security’ cameras) lack basic password functionality or allow the use of default passwords that can easily be guessed or even found on forums. Such vulnerabilities have been exploited to conduct Distributed Denial of Service (DDoS) attacks, which are used to overwhelm a website or online service, making it unavailable. One such attack, which took place in 2016, knocked Twitter, Netflix and the Guardian Newspaper offline for the best part of a day. Vulnerable Internet-enabled devices can also be targeted to steal personal information, including credit card details, and may facilitate a range of other crime types now and in the future.

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

*This project is co-funded by PETRAS, the Internet of Things hub, and we are working closely with DCMS on this research.

Lead investigator(s): [Dr John Blythe](#), [Professor Shane Johnson](#)

Refugee Flows and Instability

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

The research will employ deep case analyses and surveys of former Lebanese refugees from the Lebanese Civil War and current Syrian refugees in Lebanon, alongside rich data analyses of cross-national and subnational flows of refugees globally between 1990 and 2015. We will also integrate these scales via the development of an agent-based model of refugee flows and a series of protocols for forecasting flows and instability.

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

Lead investigator(s): [Dr Alex Braithwaite \(University of Arizona\)](#), [Dr Faten Ghosn \(University of Arizona\)](#), [Dr Toby Davies \(UCL\)](#), [Professor Shane Johnson \(UCL\)](#)

Research Highlights: PhD projects

Crime, place and the internet

In urban environments, crime is known to cluster in time and space. We are thus able to locate crime “hot-spots” and inform effective place-based crime prevention policies and strategies. However, cyberspace does not work in the same way as physical spaces. Measuring space-time clustering in cybercrime requires new means by which place, distance, size, and route can be conceptualised. The aim of this PhD research is to develop a framework that can be used to measure cyberspace and map it with reference to both the physical and virtual space. The project will demonstrate how the framework can be used to conduct space-time clustering analyses of cybercrime both in the physical and online space. The findings of this research are intended to inform, and provide the security industry and policy-makers with effective deployable solutions to targeting cybercrime.

Biocrime - are we prepared for it?

A new generation of criminals are becoming more ‘tech savvy’ than ever before. Advances in biology make technologies such as DNA sequencing and engineering publicly available and accessible, regardless of technical background, making potential illicit activities possible. The future challenge from the commercialisation of various biological techniques and the potential “bio-crimes” that will inevitably appear, must be understood in order to put security systems in place. This project will overview the technologies that may catalyse this paradigm shift. The social changes shaped from these technologies will then be explored to identify the new opportunities of offending they produce, referred to here as “bio-crime”. The aim is to determine how these emerging trends might best be identified at the earliest possible stage before they escalate. Data science techniques will be predominately used to predict how, when and what form these new opportunities will take.

Cybercrime risks to London’s future street infrastructure

Smart cities incorporate many technological advances. The intelligent devices within the street infrastructure risk being inherently insecure which provides the potential for cybercrime. The aim of the proposed research is to gather a holistic view of the overall smart street infrastructure operating model and its resilience to possible types of cyber-attack. The expected outcome of this research is an evaluation of possible gaps and risks to cyber security in the operational management of smart street infrastructure, using London as a case study in the first instance.

Unconventional cyberweapons

The threat landscape relating to cyberweapons and cyber warfare is increasingly dominated by vulnerabilities in Internet-connected devices, vehicles, implants, and infrastructure; industrial control systems; and widely-used protocols and applications. The incidence of such vulnerabilities being exploited by criminals, terrorists, and hostile states continues to increase, and the sophistication and ambition of threat actors is escalating rapidly.

Despite these developments, the current discourse on cyberweapons and cyber warfare tends to focus heavily on the implications for technical infrastructure, the economy, and wider issues such as policy and legislation, without considering the physical and psychological impacts on humans. This research will focus on several existing and new technologies from various disciplines which, when combined with traditional malware delivery, exploitation and control mechanisms, could enable attackers to cause direct physiological and psychological harm to humans. There are two major motivations for this; first, to demonstrate that such attacks are possible in order to inform tactical, policy, and legislative frameworks relating to cyberweapons; and second, to develop detection and countermeasure capabilities for these techniques, thereby providing responders and investigators with effective mitigation strategies, and reducing the threat posed by such unconventional attack techniques.

Teaching

Dissertation Research

In addition to PhD supervision, Centre staff supervise MSc student dissertations. In the 2016 academic year, MSc students completed research projects to include:

- the security of consumer Internet of Things devices for security cameras and popular devices,
- analyses of patterns of cybercrime using data collected for the Crime Survey of England and Wales,
- analyses of cybercrime victim reporting behaviour using data collected for the Crime Survey of England and Wales,
- an analysis of the theft of keyless cars in the West Midlands.

Security Technologies

In 2017, we launched the new *Security Technologies* undergraduate module. The course introduces students to the field of security technology and educates them in the fundamental scientific principles and processes, and associated mathematics underlying the operation of key domestic security technologies. These technologies include camera and video analytics; radio-frequency and biometric sensors; as well as X-ray scanners and other systems used for screening and threat detection. Students are also introduced to the concept of horizon scanning. This year's students produced horizon scanning papers on topics that included smart cities, drones, and the blockchain. Students are also required to produce a poster presentation. Next year, the poster session will be held at the Home Office in Marsham Street.

Horizon Scanning module

In the second term of the 2018 academic year, we will launch a new postgraduate module concerned with horizon scanning. This module will consider the changing nature of crime. It will begin with a discussion of how crime has evolved over time and the arms race in which offenders, law enforcement and others have been historically engaged. Cycles of innovation and how these might lead to new crime opportunities will be considered, as will the role of industry and other players in designing out crime. Methods of horizon scanning and associated methodologies will be discussed in general, followed by a focus on how such techniques can be applied in the context of crime, in particular.

External engagement

Part of the Centre's strategy is to engage with other research centres and agencies involved in work related to the aims of the Centre. The objectives of this activity include promoting the Centre, better understanding what the police and other agencies are doing about future crime problems (in terms of trying to identify or prevent them), identifying opportunities for collaboration, uncovering potential sources of additional funding, and locating those who might usefully contribute to the work of the Centre or inform the direction of our activity. For a number of reasons we will not detail the exact organisations with whom we are interacting, but they include representatives from the police, professional bodies, the private sector and Non-Government Organisations involved in crime prevention.



Publications

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

Linares, F.M., and **Johnson, S.D.** (2018). Cybercrime and Place: Applying Environmental Criminology to Crimes in Cyberspace. In G. Bruinsma and S.D. Johnson (Eds.) Oxford University Press Handbook of Environmental Criminology, New York: Oxford University Press.

- **Blythe, J., & Johnson, S.D.** (2018). The Consumer Security Index for IoT: A protocol for developing an index to improve consumer decision making and to incentivize greater security provision in IoT devices. *In proceedings of the Living in the Internet of Things: Cybersecurity of the IoT Conference. IET. London, UK.*
- Tanczer, L., **Blythe, J.**, Yahya, F., Brass, I., Elsdon, M., & Blackstock, J. (2018). Summary literature review of industry recommendations and international developments on IoT security. Report prepared for the Department for Digital, Culture, Media and Sport, HM Government, London. Available from [https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/686090/PETRAS Literature Review of Industry Recommendations and International Developments on IoT Security.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/686090/PETRAS_Literature_Review_of_Industry_Recommendations_and_International_Developments_on_IoT_Security.pdf).
- Our work on the Consumer Security Index for IoT is discussed in the Department for Culture, Media and Sport (DCMS) report Secure By Design: Improving the cyber security of consumer Internet of Things Report.²

²https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf

Conclusion

We have had a productive year. However, much more is planned for the year ahead. IBM estimate that 90% of all data ever created was produced in the last two years - we are witnessing a data explosion. To take advantage of this, we have appointed a new lecturer in data science (September 2018-), who will help to build our portfolio in this growing area of research, and explore how techniques such as machine learning can inform our understanding of new and emerging crime threats and how to combat them.

The coming year will see the first of our scoping study sandpits take place. The first two of these, concerned with advanced materials to combat crime, and recent and future trends in counterfeit goods, will take place in April and will involve a mix of academics, practitioners and other key stakeholders.

This year will also see us work more closely with the DCMS and industry to develop and propose a Consumer Security Index, or similar labelling scheme, for consumer IoT devices. With the sale of such devices increasing year-on-year, it is important that manufactureres are encouraged to make them secure by design, and that consumers are provided with information at the point of purchase to help them make informed decisions.

We look forward to working with all of partners in the year ahead.

