Future Crime

Shane D Johnson, Paul Ekblom, Gloria Laycock, Michael Frith, Nissy Sombatruang, Erwin Rosas Valdez

Johnson, S., Ekblom, P., Laycock, G., Frith, M., Sombatruang, N. and Rosas Valdez, E. (2019). 'Future crime' in R. Wortley, A. Sidebottom, N. Tilley and G. Laycock (Eds.), *Routledge Handbook of Crime Science* 428-446. Milton Park: Routledge.

INTRODUCTION (1)

The nature of crime is clearly changing. To illustrate, consider findings from the Crime Survey of England and Wales (ONS, 2016). For the first time, this sweep of the survey included questions about cyber crime. And while it only included questions about a handful of such offences, it suggested that at least half the crimes committed in the recall year, that were included in the survey[1], involved the misuse of computers. As much cyber crime will go unnoticed, and many types of online offending were not considered in the survey, this is likely to be an underestimate of the scale of offending. While many new forms of offending will be facilitated by the internet, new forms of crime opportunity will not be limited to the kinds of offending we commonly associate with the term cyber crime and it is hence important to think more broadly than this.

The Dawes Centre for Future Crime at UCL was established in October 2016 with the dual aim of identifying new forms of offending and developing informed strategies to address them. As part of the activity of the Centre, a scoping study was conducted to examine how developing technologies might create new opportunities for crime, or inform approaches to combat them. Three exercises were undertaken. The first involved a search of key science and technology publications to identify emerging technologies with potential implications for crime. The second involved a systematic review of research conducted across UCL – a multi-faculty university – for which the crime implications of developing technologies were explicitly discussed. The third focused on research conducted at UCL on developing technologies for which there were latent crime implications that had not been discussed by the authors.

In this chapter, we discuss the findings from these studies. This is intended to illustrate some of the emerging technologies that might facilitate new forms (or more likely methods) of offending and to

[1] It is important to note that not all crime is covered in the survey, including that against shops and other businesses.

highlight the diversity of academic disciplines and university departments that currently contribute to work in these areas , and will need to do so in the future. Many of the lines of enquiry that will be covered are rarely discussed in mainstream criminology journals, if at all. It is not our aim to explain why this is the case, but to highlight the need for a broader perspective and an explicitly multidisciplinary approach to research focused on offending if we are to address future and emerging crime threats.

Managing expectations (2)

Before proceeding it is worth noting that predicting the future is fraught with difficulty and subject to error, both in terms of trends that were not anticipated and false positives. For example, in 1957 Alex Lewyt, president of the Lewyt Vaccuum company apparently predicted that within ten years, nuclear powered vacuum cleaners would probably be a reality. As far as we are aware, this prediction did not come to pass. Accordingly, it is important to manage expectations. Equally, however, it is important to stress that without such exercises we risk repeating errors of the past. To elaborate, and as has been discussed elsewhere (Ekblom, 1997; Pease, 1997), where innovation and change are concerned, a common story has played out time and again. That is, when new technologies or services are introduced their benefits are reaped and uptake increases. However, as crime prevention is often overlooked, or inadequate attention given to it, there frequently follows a crime harvest, whereby offenders exploit the crime opportunities that the new product or service affords. Examples include vehicle crime (e.g. Laycock, 2004) and robbery at ATMs (Guerette and Clarke, 2003) in the 1980s, credit card theft in the 1990s (Levi, 2000), and mobile phone theft in the 2000s (Mailey et al., 2008). In all of these cases, criminals exploited vulnerabilities associated with these products and services and rates of crime increased. Each of these problems could have been anticipated but if they were, they were not addressed until after the crime problems emerged.

Another issue to raise at this point is that the aim of the work discussed in this chapter was to examine the future crime potential of a wide array of developing technologies, as opposed to a specific class of technology. As such, we do not report detailed analyses of background changes or other factors that would be considered in a PESTLE analysis, or the other types of horizon scanning exercises discussed in Chapter 29. Such exercises should be conducted for particular classes of technology, but they are not reported here. The final point to make is that the research reported here was completed at the beginning of 2017 and we live in a time of rapid technological change. As such, some of the technologies may have advanced substantially by the time this chapter is published or read.

The rest of the chapter is organised as follows. In the next section, we discuss how the theories that underpin much research in Crime Science (e.g. see Chapter 1; see also, Bruinsma and Johnson, 2018) can contribute to thinking about the future and how they were used to identify emerging technologies with potential crime implications. We go on to describe the methodology employed in our systematic review of research conducted at UCL and summarise key findings of the review. Then, we briefly discuss some of the developing technologies with implications for crime that were identified over the course of the project. We close by discussing crime prevention and the roles that different actors might play in preventing future crime.

LOOKING TO THE FUTURE THROUGH A CRIME SCIENCE LENS (1)

In this section, we briefly summarise some of the theoretical perspectives commonly used in Crime Science research that informed our scanning work. Most of these are discussed in more detail in other chapters of this book (including Chapter 1) and hence we highlight only their core features and how they can inform thinking about crime futures.

1. **Routine activity perspective** (Cohen and Felson 1979; Pease 1997; Felson and Eckert 2015) – is an ecological model of crime occurrence that considers how everyday routine activities bring together a likely (capable, motivated) offender, with a suitable target, absent capable guardians. A key aspect of the perspective is that changes to the activity of any one of these elements (not just offenders) can influence the likelihood of crime occurrence. Consequently, we can ask of any technological or social change, 'how might this innovation or change affect the routine activities of likely offenders, suitable targets and capable guardians to that bring them together or keep them apart?'.

2. **Rational choice perspective** – is a psychological/economic/opportunity model of offender decision-making (e.g. Cornish and Clarke 2017). It considers an offender's response to perceived risk, effort and reward from a contemplated criminal act, or wider criminal involvement choice, based on 'opportunity structure'. From this perspective, it is assumed that offenders will more likely engage in crime when they perceive the rewards to outweigh the risk and effort involved. We can ask, 'how might an innovation/change influence actual and/or perceived risk, effort and reward for a given opportunity or wider criminal involvement choice?'. We can also ask what new crime opportunities a particular technology might create.

3. **Crime pattern theory** – is traditionally a geographical approach to understanding offender activity spaces and movement patterns and how this shapes their perception and awareness of local environments and the crime opportunities they offer (e.g. Brantingham,

Brantingham and Andresen 2017). We can ask, 'how might innovation/change affect offenders' ability to move within, spot opportunities and get to know risks in their activity space?' We can also ask 'how might that activity space itself change with (for example) the introduction of new transit systems, the use of mobile navigation applications that direct people through areas they would otherwise not visit, or as a consequence of receiving data on the activity of places?' Further we might consider 'how might offenders develop activity spaces in virtual or other environments made accessible by new technology (e.g. unmanned aerial vehicles make airspace – and the third dimension – easily accessible to people)?'.

4. **Crime precipitators** – is a psychological approach that considers the role of factors in or near the immediate crime situation which influence the motivation/emotion of offenders, making their search for, or exploitation of, criminal opportunities more likely. For example, situational precipitators, such as environmental cues, events or influences can prompt, pressure, permit or provoke criminal behaviour (Wortley, 2008, 2017). We can ask, 'how might innovation/change influence the nature, strength and patterns in situational precipitators, or the susceptibility of offenders to them?'.

5. **25 techniques of situational prevention** – is an extensive catalogue of practical techniques (e.g. Clarke and Eck 2003; www.popcenter.org/25techniques/) organised around various situational prevention principles relating to the above perspectives (risk, effort, reward to offender; excuses and provocations). We can ask, 'how might innovation/change enable or constrain the successful operation or implementation of each of these categories of preventive technique, or individual exemplars?'.

6. The **conjunction of criminal opportunity** (CCO: Ekblom 2011 and http://5isframework.wordpress.com) – is an integrated suite of 11 immediate causes of criminal events, and counterpart intervention principles; CCO merges situational prevention perspectives along with various offender-oriented approaches. These causes and interventions could change in the future and thus offer broad leads to systematically envisaging crime/security possibilities. We can ask, 'how might innovation/change affect each of these immediate causes of criminal events, and how they interact? And how might it affect the scope for intervention in those causes?'.

7. **Misdeeds and security framework** – is a 'think thief' approach to distinguishing several broad ways in which products, places, procedures and systems can feature in criminal action (Misappropriated, Mistreated, Mishandled, Misbegotten, Misused, Misbehaved with,

Mistaken) and security counterparts (See Ekblom, 2005, 2017). We can ask 'how might innovation/change enable or constrain Mistreatment, Misuse etc by offenders?'.

8. **Risk and protective factors** – frameworks such as CRAVED (Clarke 1999) have been developed to inform understanding of what makes a product "hot" (i.e. targets at high risk of theft/misappropriation). Hot products are considered to be those that are Concealable, Removable, Available, Valuable, Enjoyable, and Disposable and we can ask 'how might innovation/change affect these risk factors, or the capabilities/intent of offenders who might target them?'.

Identifying Developing Technologies of Interest (2)

The first part of the work involved the identification of developing technologies that might have crime implications. The aim of the exercise was not to develop a list for which there would be consensus across researchers, but to identify a broad list of developing technologies. To do this, the second author scanned key science and technology publications over a six-month period and considered articles through the lens of the perspectives described above. The Science Daily[2], BBC technology[3], and BBC science and environment web pages[4] were scanned on a near daily basis, while the *New Scientist* magazine was read on a weekly basis, and the UK Engineering and Physical Sciences Research Council (EPSRC) *Pioneer* magazine read every Quarter. The frequency of scanning reflected the rate of publication for these different sources.

Science Daily and the BBC websites produce daily-updated listings of science and technology news items and feature articles across the full spectrum of disciplines and domains, including relevant social sciences. Science Daily is based on edited publicity accompanying scientific journal articles supplied by source institutions, usually with links to the formal publications themselves. As such, it provides substantial coverage of current activity in the science and technology domains. New Scientist similarly provides links from both news items and specially commissioned feature articles which cover topics in depth and combine several sources.

To supplement this systematic search, sources including The Daily Telegraph, The Economist, The Independent, WIRED, and Nature were sampled on a more ad-hoc basis, sometimes in the process of following up source material from the news feeds. All of the articles surveyed were coded in a

2 www.sciencedaily.com

3 www.bbc.co.uk/news/technology

4 www.bbc.co.uk/news/science_and_environment

number of ways, but most importantly in terms of if they had potential crime and security implications. Inevitably, the approach taken was somewhat subjective since only one of the authors engaged in this task. However, the use of the above frameworks was intended to structure the process. The final outcome of this exercise was a set of keywords regarding developing technologies with implications for crime (available upon request) to inform a search for articles published by staff at UCL.

UCL SYSTEMATIC REVIEW (1)

As discussed above, two systematic searches of research published at UCL were conducted to identify (separately) work on developing technologies that explicitly discussed crime, and that which did not, but for which there may be crime/security implications in the future. To conduct the two searches, all research outputs published over the four-year period January 2013 to December 2016 listed in the UCL Research Publications Service [RPS] repository were extracted for analysis – a total of 89,299 items. Of these, 16,144 did not meet the inclusion criteria for the two literature searches and were removed during one of four stages of sifting. Details of the reasons for removing outputs are shown in Figure 1. In total, 73,155 outputs were eligible for further examination.

INSERT FIGURE 1 ABOUT HERE

Search 1: Research that explicitly mentions crime (2)

The titles, abstracts, keywords and notes of each of the 73,155 outputs described above were systematically searched to find outputs (that were directly) related to crime, using the following set of 16 keywords:

- aggress* (for aggression, aggressive etc.)
- assault
- burglar
- crime
- forensic
- malicious
- murder
- offend* (for offender, offending, etc.)
- police/policing
- rob/robber
- secur* (for secure, security etc.)
- theft
- threat
- victim
- violen* (for violence, violent, etc.)

Note that the character "*" is a wildcard, so that variants of the word stem searched for would be identified (e.g. offend* would identify terms such as offend, offender and offending).

Outputs that contained one or more of the keywords were identified as potentially relevant and inspected further. The term "disorder" was originally included as a keyword. However, pilot testing revealed that it identified a large number of outputs (3000+) that were unrelated to crime (e.g. articles concerned with topics such as psychological disorders but not crime). As such, this keyword was excluded.

In total, 1,839 outputs were identified that contained one or more of the crime keywords. Of these, 223 involved staff or students from the UCL Department of Security and Crime Science (DSCS). These were excluded from what follows – as we were primarily interested in articles published in other academic departments – and hence a total of 1,616 outputs remained.

The titles, abstracts and keywords for each of the remaining outputs were then reviewed by one of three research assistants (RAs) to assess its likely relevance. As with the previous exercise, this involved some degree of subjectivity (see below), but was completed using clear inclusion and exclusion criteria (available upon request). Chief amongst these was that the article should discuss a developing technology – defined as a new or in-development technology that has the potential to be involved in the commission, prevention or detection of crime in the next 5 years. Moreover, inter- and intra-rater exercises conducted for a sample of articles showed that the RAs' judgements were in close agreement – both with each other and with themselves at different stages of the review process. Following this exercise, a total of 274 articles were identified for the purposes of the review.

Figure 2 is a network graph that shows how research activity concerned with developing technology that has implications for crime (explicitly noted in the abstract, title or keywords) was distributed across UCL. Each green dot represents a research output, while each blue dot represents the academic department from which the lead author of the output is located. It is evident from Figure 2 that there are concentrations of activity within some UCL departments (and researchers within those departments). This is particularly the case for Computer Science, which is to be expected and welcomed, given that data from the CSEW suggest that at least half of all crime is now online. However, it is also clear that relevant research is conducted across a wide array of UCL departments, highlighting the fact that numerous disciplines can contribute to our understanding of crime and security, and that there is a need to break down disciplinary silos.

INSERT FIGURE 2 ABOUT HERE

Emerging Themes (3)

In this section, we draw out some of the general themes that emerged from the literature identified. These were identified through an iterative "thematic analysis" and represent a mixture of broad crime types (e.g. cybercrime), targets, techniques, technologies and approaches. The 274 outputs were grouped into 13 overall themes which are listed in Table 1, along with the number of outputs associated with each theme.

INSERT TABLE 1 ABOUT HERE

Of these, outputs were further classified as those that were rated to be of most relevance to the future crimes agenda. Forty-six articles met this criterion. Focusing on these outputs, Figure 3 shows the themes identified (green dots) and the home departments (blue dots) of the lead authors (some of which are labelled for the purposes of illustration). The nodes in the network are proportionately scaled to reflect the volume of outputs associated with a specific theme, and the number of outputs authored by staff in a particular department. The links between themes and departments are also proportionately shaded to indicate which departments contributed most to each theme. Again, a clear trend that emerges is that while there are concentrations of research activity for each theme in particular departments, work is conducted across a number of departments, highlighting the multidisciplinary nature of work on these issues.

INSERT FIGURE 3 ABOUT HERE

It is beyond the scope of the current chapter to discuss each of the themes identified and the research associated with them. Instead, we offer a brief discussion of some of these to illustrate the type of work underway and how the technology might create new crime opportunities or ways to address them.

A total of 127 outputs were identified as being relevant to the theme of cyber security, including 26 that were assessed as being highly relevant to the future crimes agenda. These can be further divided into sub-categories to include research that has examined privacy and two-step authentication systems for government services (Brandao et al., 2015), the security of cloud computing (Jeuk et al., 2013), the application of cryptography to secure phone calls (Murdoch, 2016), the security of cryptocurrencies such as Bitcoin (e.g. Courtois et al., 2016) methods for quickly updating the security of networked computers (e.g. Forrester et al., 2016), the security of web browsers (e.g. Yang et al., 2013), patterns of contagion in cyber attacks (Pym et al., 2016)[5], and the security of 5G networks (Wang et al., 2015).

5 Interestingly, this research employs statistical models that have been used to study the near repeat phenomenon in the context of urban crime (e.g. Mohler et al., 2010).

Many of these topics reflect emerging technologies associated with online activity that have the potential to be transformational in the future and to affect people's routine activities and hence opportunities for crime. Considering money, for example, cryptocurrencies such as Bitcoin have been used by criminals on the Darknet for some time due to the fact that they are pseudonymous and have no central controller, which provides benefits to those who wish to conceal their identity and deal in illegal products or services. However, cryptocurrencies are increasingly used by legitimate businesses such as Microsoft, and travel companies such as Expedia[6], not to mention smaller businesses in urban settings. As their legitimate use increases, this may create new opportunities for offending. When introduced, 5G technology will lead to (for example) massive increases in the bandwidth available for internet connected devices. Other research concerned with online activity discussed the trade-offs between the usability of online security techniques and the security they afford (Sasse and Smith, 2016) and why online security warnings fail (Sasse, 2015).

A second theme that emerged concerned scanning technologies. This included research concerned with automated methods of analysing x-ray images of cargo (Jaccard et al., 2016; Rogers et al., 2016) to verify the content of containers, and a novel system for detecting illicit drugs in fast-parcel environments (Drakos, 2015,). Other work involved the use of nanomaterials for the detection of illicit materials such as explosives (Peveler, 2015), and electromagnetic imaging systems for detecting materials through metallic enclosures (Darrer et al., 2016). Like most of the cyber crime examples above, the research associated with this theme has developed in response to the crime opportunities afforded by changes, in this case changes to the way in which goods are moved. For example, the growth in online shopping and increased competition in the delivery sector has created an environment of large volumes of "fast" parcels which, while convenient for consumers, create new opportunities for crime and challenges for law enforcement as checking the volumes of parcels now delivered throughout the world is an immense challenge.

Search 2: Research with latent crime implications (2)

The aim of the second search was to identify research on developing technologies that might have implications for crime in the future, but for which these implications are not acknowledged–at least not in the title, abstracts, keywords or notes of the articles. The absence of a discussion of crime in these articles is to be expected as the researchers who undertook the studies generally work in other disciplines, and crime will be but one of many practical implications of their work. The aim of the research was thus to tease out some of these implications.

6 https://www.expedia.com/Checkout/BitcoinTermsAndConditions

As with the first exercise, we systematically searched the 73,155 outputs described above. This time, however, we searched the articles using the set of 76 technology-related keywords identified as part of our first strand of work. As with the crime keyword search, some of the keywords initially used led to the identification of a large number of outputs (1000+) that pilot testing (of a sample of around 5% of them) suggested were entirely unrelated to crime. These keywords[7] were therefore excluded. In addition, outputs that had been identified in the crime keyword search were excluded from what follows to avoid duplication.

In total 3,251 outputs were identified that contained one or more of the technology-related keywords. As with the first search, each of the outputs was reviewed by one of the RAs and retained or discarded according to whether it met our inclusion criteria[8]. A total of 304 publications remained after completion of this exercise.

Figure 4 shows how research activity of this kind is distributed across UCL. In this case, because of the focus of the keyword search, the network graph includes outputs from the Department of Security and Crime Science (SCS) as well as other UCL departments. There are some similarities between Figures 2 and 4. That is, activity is concentrated in some departments but is also clearly evident across the university. However, there are differences. For example, the Department of Electronic and Electrical Engineering features more prominently in Figure 4 than Figure 2 (accounting for 77 and 17 outputs across the two figures, respectively). Moreover, the Departments of Pharmaceutics and Materials and Tissue feature in Figure 4 but not its counterpart. The number of relevant outputs identified as being of particular relevance also tended to be higher per department for this search than the earlier one. One interpretation of this is that going forwards, research on crime will need to become increasingly multidisciplinary.

INSERT FIGURE 4 ABOUT HERE

Emerging Themes (3)

An iterative "thematic analysis" of the 304 outputs revealed a total of 18 "overall" themes of research. These are shown in Figure 5 (green dots) along with the home departments (blue dots) of the lead authors.

7 Specifically, "optic" and "brain AND (reading OR control)" which led to the identification of articles concerned with topics such as eye conditions and scans of abnormal brain functionality, respectively.

8 To be included, the main criteria articles needed to address was that they were concerned with a developing technology, have plausible implications for crime, and for the application of the research to be plausibly realised within the next 5 years.

INSERT FIGURE 5 ABOUT HERE

In Table 2, we provide a further synthesis of topics and highlight ten example areas that were perceived by the authors of this chapter as being particularly relevant, either because they might facilitate crime or help to prevent it. It is beyond the scope of this chapter to discuss each theme in detail and hence their identification is simply intended to illustrate the diversity of issues and some of the implications. With this in mind, in each case we do provide a pen picture to illustrate some of the issues. To supplement this, we take two related themes and elaborate on these a little.

INSERT TABLE 2 ABOUT HERE

Smart Technology (3)

As discussed in Chapter 20 , smart technology (also called the Internet of Things, IoT) refers to products which are internet connected, incorporate sensors, and may have actuators that can make physical changes to the environment within which they are located. Such devices are often designed with the goal of improving people's quality of life and domestic examples can range from smart watches/activity trackers, to health monitors (e.g. heart-rate monitors), to internet connected fridges, to smart energy meters, to home security systems. Most devices collect and transmit data, which could include indicators of health, physical activity or other forms of data. As such, the security of these technologies is important as they may store and/or transmit sensitive information such as people's daily routines, leaving them vulnerable to crime. Unfortunately, at present the security of many such devices is notoriously weak (e.g. DCMS, 2018). As the number of devices increases – industry experts estimate that by 2020 there will be around 20 billion devices (e.g. Gartner, no date) – so too will the opportunity for criminal activity that exploits them.

Insecurities in the IoT pose substantial risks to national infrastructure, and these were discussed in Chapter 20. Considering the risks posed by the IoT from a routine activity perspective, devices can send and receive data about people's movements and actions. Such data might be exploited by offenders to commit crimes such as burglary and other offences for which guardianship is an important deterrent, or it may facilitate domestic abuse in which coercive control and stalking play an important role (e.g. Dragiewicz et al., 2018). In terms of crime opportunity more generally, the proliferation of devices in people's homes and critical infrastructure suggests that the potential for their exploitation is huge and the implications alarming.

On a more positive note, researchers (Hunter, 2016) at UCL have looked at the possibility of developing automated persuasion systems (APS) that would run on mobile devices to encourage behaviour change in individuals. Part of the appeal is that as such devices become ever more

pervasive so too does the opportunity to engage people with APS to affect their behaviour – in other words, the solution can scale up in step with the problem. In the context of crime, the authors discuss possible applications for the prevention of anti-social behaviour to include violence, sexism and trolling. Similarly, work by Lathia et al. (2013) has looked at how smartphones can unobtrusively sense human behaviour and how this might be applied to monitor and change it (through feedback). Extrapolating from these papers, an interesting application would be in the prevention of high harm crimes such as domestic abuse. For instance, for offenders wanting to desist from behaviours such as stalking, smart sensing could be used to detect when an offender is at risk of committing abuse and an APS used to discourage this.

A different possible application comes from an anecdotal example of a case of domestic abuse9. During the incident, the abuser accused the victim of calling the Sherriff's office. Accidentally, their home smart speaker misheard his accusation, believing him to ask *it* to call the Sheriff's office. It did so, and officers were promptly dispatched to deal with the incident. We might ask whether such technology be used in this kind of capacity in the future to prevent crime or detect offenders? In considering such questions, due care and attention does, of course, need to be given to ethical implications, and to opportunities to abuse such safeguarding. For example, while the type of artificial intelligence employed in such systems is advancing, there have already been demonstrations of how – through what are known as adversarial perturbations – these systems can be tricked in ways that would be impossible for a human to detect (e.g. Carlini and Wagner, 2018).

Smart Cities (3)

A related theme concerns Smart Cities. The smart city concept takes the beneficial principles of smart devices to apply them at scale to make the running of cities more efficient, and in many cases more sustainable. Smart connectivity has the potential to impact on all aspects of city functioning, and cities around the world are already trialling smart technology to include everything from smart bins to smart traffic management.

In the smart city, transportation too is likely to change significantly both for service providers and ordinary citizens. For example, already we are seeing the emergence of Mobility as a Service (MaaS), which may ultimately reduce or eliminate the need for (most) individuals to own their own vehicles. The operating model of MaaS is to provide users with transportation for whole (door-to-door) journeys specified via a mobile phone application. Parts of the journey may involve rail, parts

9 https://www.independent.co.uk/life-style/gadgets-and-tech/news/man-beat-girlfriend-murder-threat-alexa-gadget-call-police-google-home-bernalillo-county-sheriff-new-a7835366.html. Last accessed 25 June 2018.

might involve taxis, or driving a rental car (according to the user's preferences), with the service seamlessly (in theory at least) providing the user with access to an efficient combination of various forms of transport, none of which the user needs to own. While such services will have enormous benefits for the environment and people's mobility, some thought should go into how they will impact on our routine activities and if these changes are likely to create or disrupt opportunities for crime.

A perhaps more obvious concern regarding Smart Cities is their resilience to attack. In 2017, we saw that the operation of one-third of hospital trusts in the UK was adversely affected following cyber attacks in the form of *wannacry* (e.g. Ehrenfeld, 2017; Mayor, 2018). Wannacry is a type of ransomware that in this case was used by offenders to take over hospital systems and encrypt patient data making it unavailable to hospital staff, until ransoms were paid. In many cases, the attacks resulted in significant disruptions to patient treatment and care. This type of offending was (in part) made possible by the existence of cryptocurrencies, which are a form of non-fiat currency underpinned by a blockchain. While cryptocurrencies have many positive aspects (e.g. Brito and Castillo, 2013), they are transacted pseudonymously, which means offenders using them can conceal their identity in ways that they cannot so easily do using more traditional banking systems (but see, Meiklejohn et al., 2013). The use of cryptocurrencies in this context serves to highlight the importance of how *convergences* of technology – as opposed to single technologies – can make crime more likely: that is, while hospitals may have been vulnerable to attack before, absent cryptocurrencies, it would have been difficult for offenders to extract ransoms at scale and with such little effort. In the language of the rational choice perspective, these technologies have tipped the balance of risk, effort and reward, creating new crime opportunities that are attractive to offenders.

As with wearable devices, Smart Cities do of course offer considerable potential for law enforcement and the prevention of crime more generally. For example, at present, law enforcement agencies take advantage of sensors in the environment in the form of CCTV cameras. These can provide surveillance capabilities to help in the detection or prevention of crime (Welsh and Farrington, 2009). The camera streams that are currently routinely available to the police are limited to those on their networks. However, as more cameras become internet connected, so too does the potential network of cameras that could easily be used to prevent crime. This raises the question of how the other sensors that might form part of Smart City infrastructure could inform law enforcement activity? This will require careful consideration to avoid an Orwellian nightmare, but if done in an ethically appropriate manner that is seen as legitimate by the public who the police serve, and with suitable checks and balances, the opportunities to protect our cities are substantial.

Issues of provenance and verification will, of course, be important too as the potential to interfere with, or inject data into networks will offer further opportunities for crime.

DISCUSSION (1)

In scanning the literature, we employed a range of theoretical frameworks such as the routine activity and rational choice perspectives to inform our thinking. In doing so, we identified various ways in which developing technologies might increase opportunities for crime. Of course, these approaches also provide a framework for thinking about what to do about the types of problems identified. Perhaps the most obvious is the application of situational crime prevention (e.g. Clarke, 1995). Initially developed to address everyday urban crime problems such as burglary and theft, it has since been developed for the application to acts of terrorism (e.g. Clarke and Newman, 2006) and cyber crime (Newman and Clarke, 2013). In summary form, as discussed in chapter 1, the approach currently comprises 25 techniques intended to increase the effort (e.g. car immobilisers), increase the risks (e.g. CCTV on public transport), reduce the rewards (e.g. graffiti cleaning), reduce provocations (e.g. separate enclosures for rival teams at football stadia), or remove excuses (e.g. breathalyzers in pubs) for crime (Clarke and Eck 2003; www.popcenter.org/25techniques/). In thinking about what to do about emerging crime problems, or how to enhance existing approaches to crime prevention with developing technologies, this would seem like a good place to start and researchers are encouraged to do so.

The problem analysis triangle (Scott et al., 2008; see also chapter 1), related to routine activities, also provides a framework for thinking about how to address future crime problems and, in particular, who might need to be engaged to address them. As discussed in elsewhere in this book and the introduction to this chapter, the roles of the victim, offender and capable guardians are central to the routine activity perspective – crime is less likely in the presence of the latter and (generally impossible in) the absence of the former.

Guardians can take many forms, and include anyone or anything whose presence can deter crime. In considering new and emerging crime, we may need to think carefully about this role. The police will undoubtedly always play a role, but they will not have the capability to address all future crime issues and nor will they be best placed to do so. Cyber crime provides a contemporary example for thinking about the changing shape of guardianship. In this context, guardians would include anti-virus software and home routers – the latter providing a gateway between home networks and the

internet. Anti-virus software is imperfect and is generally of little value against zero day attacks (when virus or malware patterns are unknown), but it does serve a guardian function by protecting against those infections that *are* known. What of routers? Are these as secure as they could be? In considering this question, Szewczyk and Macdonald (2017) suggest that the architects of router communication technology overlooked one thing – security. They thus acted as what are referred to as crime promoters in the conjunction of criminal opportunity framework described above. This refers to people, organisations or designers who inadvertently, carelessly or deliberately increase the likelihood of crimes committed by other people, e.g. by supplying vulnerable targets or useful resources for offending. Thinking about crime promoters draws explicit attention to how developing technologies, goods and service might contribute to future crime problems and emphasises the role that those other than the police might play in making crime more or less likely. Returning to the example of routers, as with many products and services, Szewczyk and Macdonald (2017) suggest that a focus on function took primacy over security. This will need addressing going forwards, but similar thinking will be required for new technologies.

The routine activity perspective has developed over time to incorporate other actors whose influence can affect the likelihood of crime occurrence. These include place managers (e.g. Madenson and Eck, 2018) who are responsible for the way in which particular facilities are managed, the polices that are practised, and the extent to which staff and those who use the facilities comply with them. In the context of future crime, we can ask what role place managers can play in reducing the likelihood that offenders will exploit new crime opportunities. This might include, for example, ensuring that managers of community synthetic biology laboratories[10] (See Table 2) set and enforce clear rules to ensure that those who use them do not engage in criminal activity.

The role of place managers may, however, need some rethinking in the context of smart cities. For example, as our environments become more automated and self-organising, will the role of individuals as place managers slowly (or rapidly) decline? While such futures may seem a long way off, consider that in shops, self-service checkouts have existed for some time. This removes a form of guardianship and perhaps it is not surprising that the evidence (e.g. Taylor, 2016) suggests their introduction has been accompanied by an increase in shop theft. Consider further that Amazon GO (in Seattle) and AliBaba (in China) are already testing the next generation of shopping environments in which customers (who register for the service via a smartphone application) do not even need to use a checkout but can, in the case of Amazon GO, simply pick up items and leave the store, with their accounts being charged automatically.

[10] https://www.nature.com/scitable/blog/bio2.0/synthetic_biology_at_home

If the role of people as place managers does decline, attention will need to be given to how the role that they have fulfilled to date can be incorporated into smart systems of place management. If it does not, consideration will need to be given as to how place managers can and should exert an influence over smart systems to make crime less likely. It seems probable that – at least in the near future - some environments will become increasingly automated, while others will continue to be managed by people. If this is the case, then both issues will need consideration. In the last resort, human managers will be needed to cope with the adaptive nature of offenders when this exceeds the capability of any automated security system (e.g. Ekblom, 2017).

Another important type of actor that forms part of the Problem Analysis Triangle is the handler - a person who can directly influence the activity of a likely offender. Handlers usually have some form of emotional attachment to an offender such as a parent, friend or sibling (e.g. Sampson et al., 2010). Guardians, handlers and place managers are all forms of controllers (e.g. Sampson et al., 2010), and each can influence the likelihood of crime by protecting victims, discouraging offenders from offending and by making places safer, respectively. A further iteration of these ideas (e.g. Sampson et al., 2010) identifies *super controllers* as a set of actors who have a more indirect influence on the crime equation but who can have a broader impact on incentivising or enforcing approaches to crime prevention. These include regulators, the media and mass markets. Super controllers can exert their influence on all actors in a variety of ways. For instance, regulators can set standards for the manufacture of products or services to make them less criminogenic and enforce compliance with these standards. Apropos future and emerging crime, consider that at present, there is no regulation regarding the security standards that consumer IoT devices should meet. As such, many devices have little to know security making them vulnerable to attack and criminal exploitation[11]. In most countries, regulations exist to ensure that vehicles are road worthy and safe to drive, and hence we might ask why similar regulation does not exist for IoT and similar products. Efforts are now underway by a number of governments (e.g. DCMS, 2018) to address this problem but this will take time and we have already seen criminal exploitation of the insecurities that these devices possess. The action is hopefully not too late, but it certainly could have started sooner. When considering developing technologies, or new services, it therefore seems important to consider the role that super controllers can and should play in ensuring that (at least) those that will become ubiquitous do not facilitate crime and are secure by design (for an extended discussion

11 For examples, see https://krebsonsecurity.com/tag/iot/; https://krebsonsecurity.com/2017/10/reaper-calm-before-the-iot-security-storm/; https://arstechnica.com/information-technology/2016/01/how-to-search-the-internet-of-things-for-photos-of-sleeping-babies/

of such issues, see Clarke, 2005). The challenge is to find ways to turn them from potential crime promoters, into active and competent crime preventers.

Regulation will not always be the answer, but super controllers will still have a role to play. To take an example, consider vehicle crime in the UK in the 1990s. At that time, the theft of vehicles was soaring, which was unsurprising since vehicle security was woefully inadequate, despite calls for this to be addressed. To encourage industry to respond, the UK Home Office published the Car Theft index (see Laycock, 2003), which provided consumers with information on the rate at which different makes and models of vehicles were stolen (given the number that were on the road in the UK). Simple in its construction, it had the potential to influence both consumer choice and the industry who, presumably, would want to avoid reputational damage. Its publication was one of the factors that led to the industry quickly improving vehicle security, and it serves as an example of how super controllers can exert an influence using data and evidence (plus consumer and reputational pressure) as opposed to legislation.

In this chapter, we focused on how developing technologies might generate new opportunities for the commission or prevention of crime. However, technology is not the only thing that will influence the shape of crime in the future. Broader policy changes, societal preferences, and demographic change (to name a few) can all act as externalities that have the potential to influence future crime patterns. If we are to anticipate future crime opportunities and address them, all of these changes will need consideration, as will their convergence with changes in technology. As discussed throughout this chapter and the introduction to this handbook, identifying these influences, understanding them and finding solutions to the problems that may follow will require a multidisciplinary approach, as embodied by the aspiration of Crime Science.

References

Brantingham, P.J., Brantingham, P. L. and Andresen, M. (2017). 'The geometry of crime and crime pattern theory.' In R. Wortley and M. Townsley (eds) *Environmental Criminology and Crime Analysis* (2nd edition). London: Routledge.

Brandão, L. T., Christin, N., & Danezis, G. (2015). Toward mending two nation-scale brokered identification systems. *Proceedings on Privacy Enhancing Technologies*, *2015*(2), 135-155.

Brito, J., & Castillo, A. (2013). *Bitcoin: A primer for policymakers*. Mercatus Center at George Mason University.

Carlini, N., & Wagner, D. (2018). Audio Adversarial Examples: Targeted Attacks on Speech-to-Text. *arXiv preprint arXiv:1801.01944*.

Clarke, R. V., & Newman, G. R. (2005). Security coding of electronic products. *CRIME PREVENTION STUDIES*, *18*, 231.

Clarke, R. V. (1995). Situational crime prevention. *Crime and justice*, *19*, 91-150.

Clarke, R. (1999). *Hot Products: Understanding, Anticipating and Reducing Demand for Stolen Goods*. Police Research Series Paper 112. London: Home Office.

Clarke, R. V. G., & Newman, G. R. (2006). *Outsmarting the terrorists*. Greenwood Publishing Group.

Cohen, L. and Felson, M. (1979). 'Social change and crime rate changes: a routine activities approach.' *American Sociological Review*, 44, 588—608.

Cornish, D. and Clarke, R. (2017). 'The Rational Choice perspective.' In R. Wortley and M. Townsley (eds) *Environmental Criminology and Crime Analysis* (2nd edition). London: Routledge.

Courtois, N. T., Valsorda, F., & Emirdag, P. (2014). Private Key Recovery Combination Attacks: On Extreme Fragility of Popular Bitcoin Key Management, Wallet and Cold Storage Solutions in Presence of Poor RNG Events.

Darrer, B. J., Watson, J. C., Bartlett, P. A., & Renzoni, F. (2015). Electromagnetic imaging through thick metallic enclosures. *AIP Advances*, *5*(8), 087143.

Dragiewicz, M., Burgess, J., Matamoros-Fernández, A., Salter, M., Suzor, N. P., Woodlock, D., & Harris, B. (2018). Technology facilitated coercive control: domestic violence and the competing roles of digital media platforms. *Feminist Media Studies*, 1-17.

Drakos, I. (2015). *Optimisation of illicit drug detection using X-ray diffraction: Drug Identification using Low Angle X-ray scatter–DILAX III* (Doctoral dissertation, UCL (University College London)).

Ehrenfeld, J. M. (2017). Wannacry, cybersecurity and health information technology: A time to act. *Journal of medical systems*, *41*(7), 104.

Ekblom, P. (1997). Gearing up against crime: A dynamic framework to help designers keep up with the adaptive criminal in a changing world. *International Journal of Risk Security and Crime Prevention*, *2*, 249-266.

Ekblom, P. (2005). How to police the future: scanning for scientific and technological innovations which generate potential threats and opportunities in crime, policing and crime reduction. In M. Smith and N. Tilley (Eds.) *Crime Science: New Approaches to Preventing and Detecting Crime*. Cullompton: Willan.

Ekblom, P. (2011). *Crime Prevention, Security and Community Safety Using the 5Is Framework*. Basingstoke: Palgrave Macmillan.

Ekblom, P. (2017). 'Technology, opportunity, crime and crime prevention – current and evolutionary perspectives' in B. Leclerc and E. Savona (Eds.) *Crime Prevention in the 21st Century*. New York: Springer.

Felson, M. & Eckert, M. (2015). *Crime and Everyday Life* (5th edition). London: Sage.

Foerster, K. T., Schmid, S., & Vissicchio, S. (2016). Survey of consistent network updates. *arXiv preprint arXiv:1609.02305*.

Hunter, A. (2016, January). Computational Persuasion with Applications in Behaviour Change. In the annual proceedings of *Computational Models of Argument,* pp. 5-18.

Jaccard, N., Rogers, T. W., Morton, E. J., & Griffin, L. D. (2016, May). Tackling the X-ray cargo inspection challenge using machine learning. In *Anomaly Detection and Imaging with X-Rays (ADIX)* (Vol. 9847, p. 98470N). International Society for Optics and Photonics.

Jeuk, S., Zhou, S., & Rio, M. (2013, May). Tenant-id: Tagging tenant assets in cloud environments. In *Cluster, Cloud and Grid Computing (CCGrid), 2013 13th IEEE/ACM International Symposium on* (pp. 642-647). IEEE.

Lathia, N., Pejovic, V., Rachuri, K. K., Mascolo, C., Musolesi, M., & Rentfrow, P. J. (2013). Smartphones for large-scale behavior change interventions. *IEEE Pervasive Computing*, *12*(3), 66-73.

Levi, M. (2000). *The Prevention of Plastic and Cheque Fraud: A Briefing Paper*. London: Home Office.

Mailley, J., Garcia, R., Whitehead, S., & Farrell, G. (2008). Phone theft index. *Security Journal*, *21*(3), 212-227.

Mayor, S. (2018). Sixty seconds on... the WannaCry cyberattack. British Medical Journal 361:k1750.

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013, October). A fistful of bitcoins: characterizing payments among men with no names. In *Proceedings of the 2013 conference on Internet measurement conference* (pp. 127-140). ACM.

Murdoch, S. J. (2016). Insecure by design: Protocols for encrypted phone calls. *Computer*, *49*(3), 25-33.

Newman, G. R., & Clarke, R. V. (2013). *Superhighway robbery*. Routledge.

Office for National Statistics (2017). Crime Survey in England and Wales. Office for National Statistics. Available online at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmar2017#what-is-happening-to-trends-in-crime

Pease, K. (1997). Predicting the Future: the Roles of Routine Activity and Rational Choice Theory. In Newman, G., Clarke, R.V.G. and Shosham, S.G. (eds.) *Rational choice and situational crime prevention: Theoretical foundations*. Aldershot: Dartmouth.

Peveler, W. J. R. (2015). *Development of nanomaterial based sensors for the detection of explosives* (Doctoral dissertation, UCL (University College London)).

Pym, D. J., Williams, J., Ioannidis, C., Gheyas, I. A., & Baldwin, A. (2012, June). Contagion in Cybersecurity Attacks. In *11th Annual Workshop on the Economics of Information Security*.

Rogers, T. W., Jaccard, N., Morton, E. J., & Griffin, L. D. (2017). Automated x-ray image analysis for cargo security: Critical review and future promise. *Journal of X-ray science and technology*, *25*(1), 33-56.

Sampson, R., Eck, J. E., & Dunham, J. (2010). Super controllers and crime prevention: A routine activity explanation of crime prevention success and failure. *Security Journal*, *23*(1), 37-51.

Sasse, A. (2015). Scaring and bullying people into security won't work. *IEEE Security & Privacy*, *13*(3), 80-83.

Sasse, M. A., & Smith, M. (2016). The Security-Usability Tradeoff Myth. *IEEE Security & Privacy*, *14*(5), 11-13.

Scott, M., Eck, J.E., Knutson, J. and Goldstein, H. (2008) Problem-oriented policing and environmental criminol- ogy. In: R. Wortley and L. Mazerolle (eds.) *Environmental Criminology and Crime Analysis*. Cullompton, UK: Willan Publishing, pp. 221–246.

Taylor, E. (2016). Supermarket self-checkouts and retail theft: The curious case of the SWIPERS. *Criminology & Criminal Justice*, *16*(5), 552-567.

Welsh, B. C., & Farrington, D. P. (2009). Public area CCTV and crime prevention: an updated systematic review and meta-analysis. *Justice Quarterly*, *26*(4), 716-745.

Wang, L., Wong, K. K., Elkashlan, M., Nallanathan, A., & Lambotharan, S. (2016). Secrecy and energy efficiency in massive MIMO aided heterogeneous C-RAN: A new look at interference. *IEEE Journal of Selected Topics in Signal Processing*, *10*(8), 1375-1389.

Wortley, R. (2017). 'Situational precipitators of crime.' In R. Wortley and M. Townsley (eds) *Environmental Criminology and Crime Analysis* (2nd edition). London: Routledge.

Figure 1: Sankey diagram showing the literature selection process and the inclusion and exclusion of research outputs

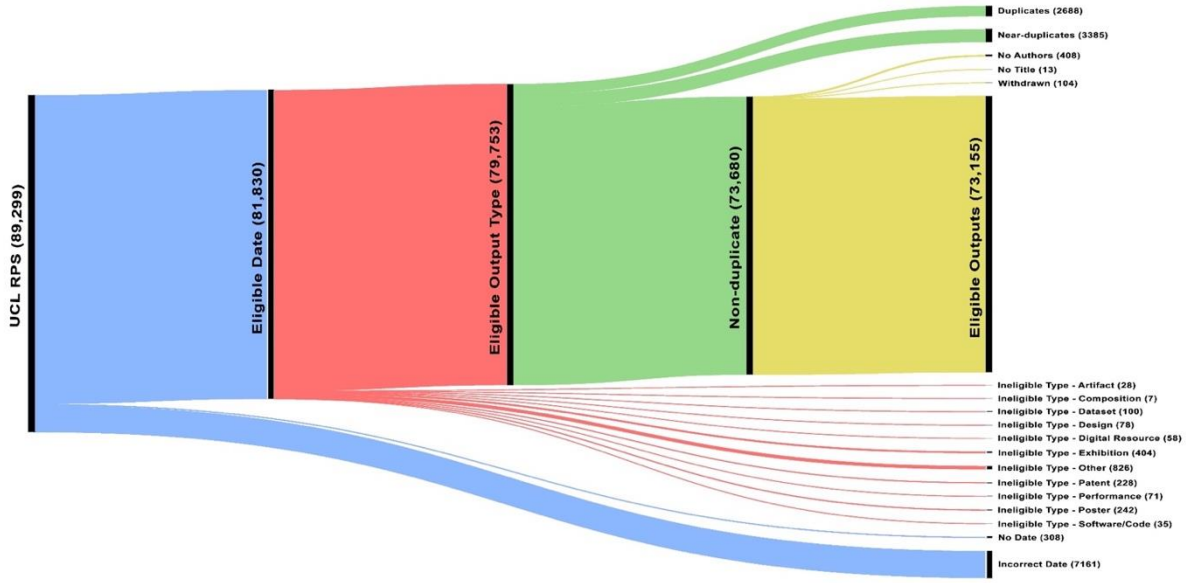

Figure 2: Network graph showing research activity concerned with crime and technology across UCL departments

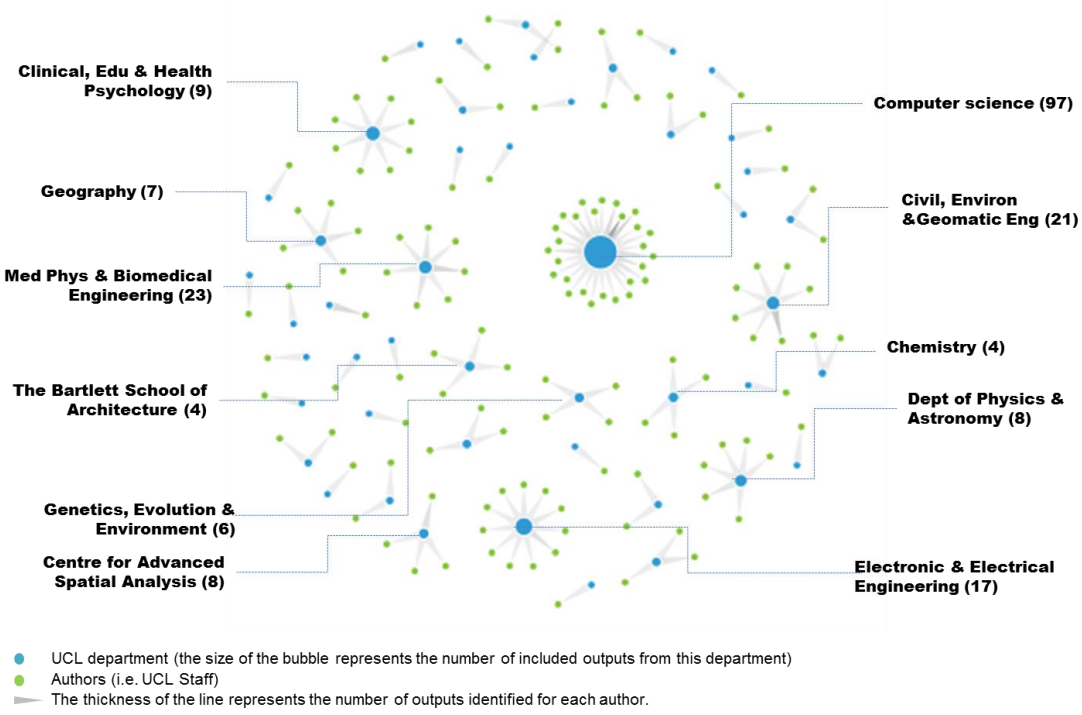

Figure 3: Network graph showing research activity by research themes and the UCL departments involved

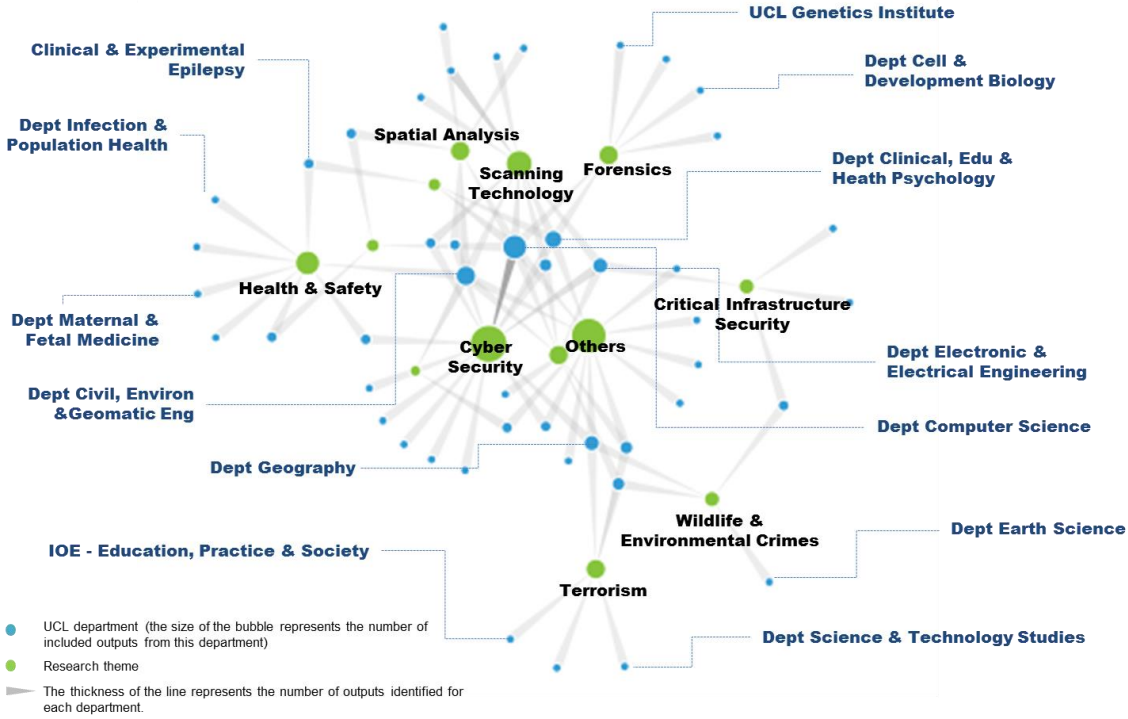

Figure 4 Network graph showing research activity concerned with developing technology with implications for crime across UCL departments

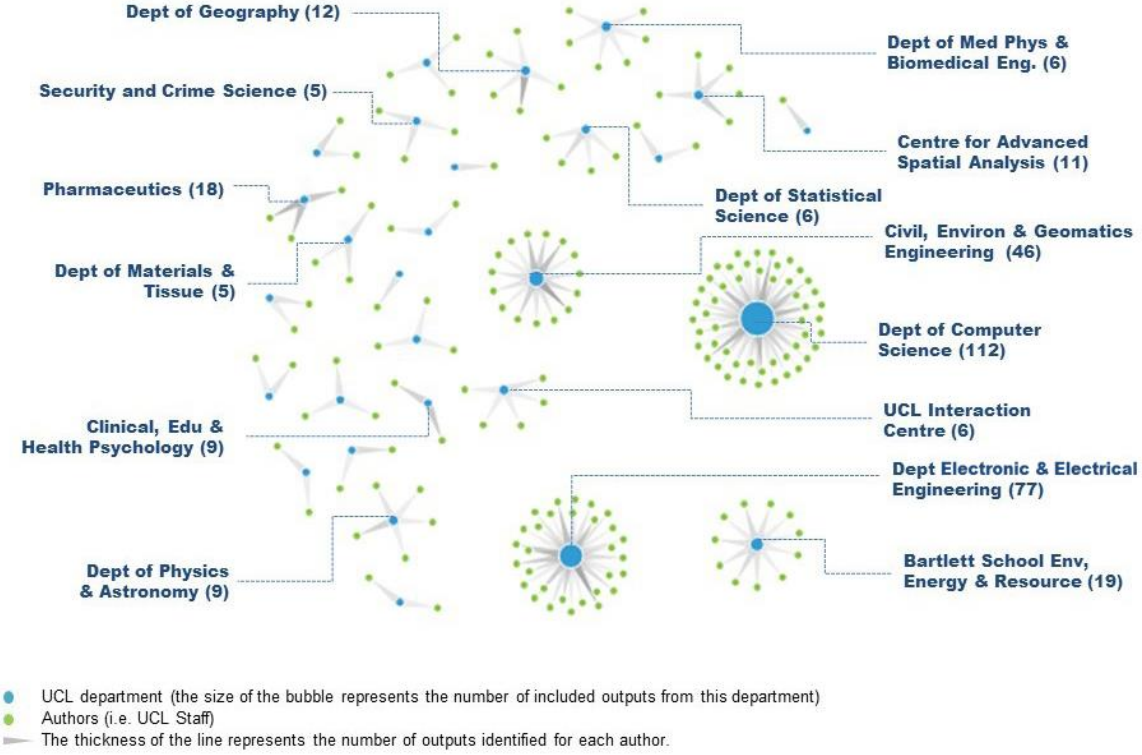

Figure 5 Network graph showing research activity by research themes and the UCL departments involved

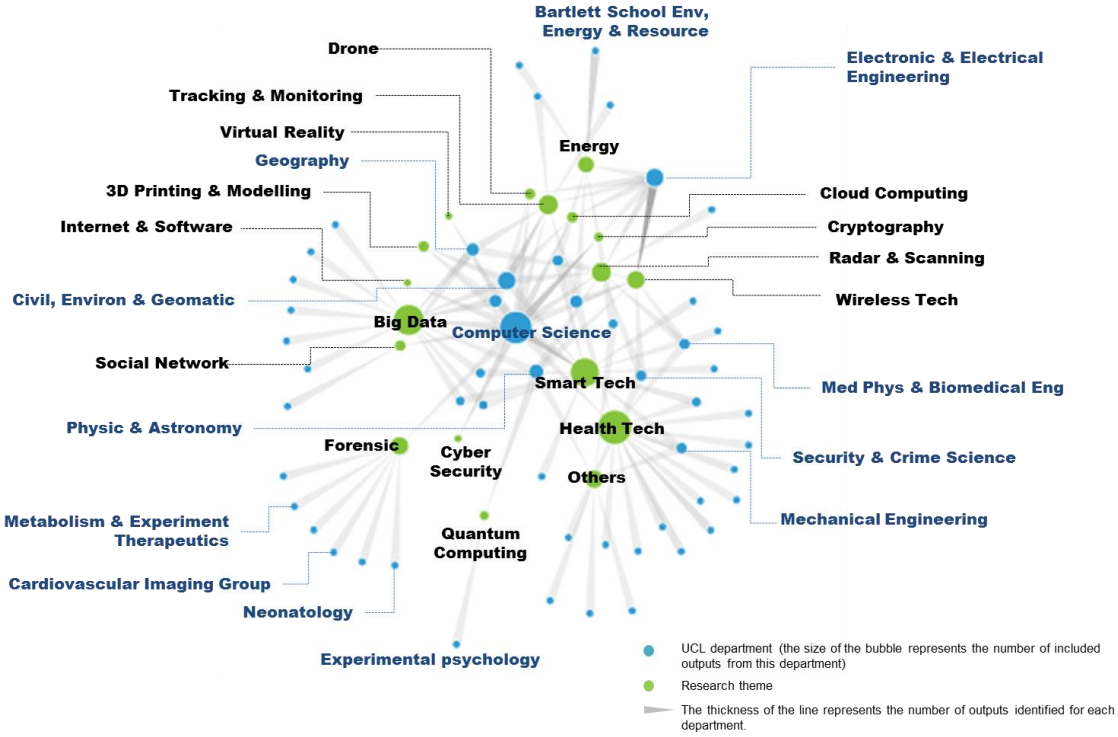

Table 1: The number of publications by theme

Theme	All Outputs	Highly Relevant Outputs
Cyber Security	127	26
Scanning Technology	29	9
Forensics	22	2
Other	15	3
Spatial Analysis	15	0
Policing	13	4
Health & Safety	10	0
Smart Technology	9	1
Wildlife & Environmental Crime	9	0
Terrorism	8	1
Critical infrastructure security	7	1
Neuroscience	5	0
Virtual Reality	5	0

Table 2 A sample of emerging technologies with implications for crime

Topics
1. Crime, place and the Internet In cities, analysis shows that crime clusters spatially, with around 20% of places accounting for 80% of problems. This has informed successful crime prevention. We can ask, while cyber crime does not occur at physical locations in the same way, does it cluster in other ways that might inform our understandig of (cyber) crime and its prevention?
2. Radar and scanning As legitimate parcels are moved with increasing speed to meet consumer demand (across and within country borders), this provides opportunties for the movement of illegal goods. Advances in sensor technology increase what (e.g. counterfeit drugs) can be detected in containers, parcels and so on, while advances in Artificial Intelligence (AI) can increase the speed with which data obtained from sensors can be analysed and made sense of. In concert, such technologies may play an important role in reducing the crime opportunities that fast parcels offer criminals.
3. Social networks and monitoring technology 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 (e.g. stalking), but could also be used to "nudge" positive behaviour, or scan for emerging problems.
4. Internet of Things – Industrial and domestic devices/autonomous vehicles, smart cities Electronic devices, buildings and other physical infrastructure are increasingly internet enabled. This presents opportunities to enhance people's quality of life, make our roads safer, and run our cities more efficiently and sustainably. However, absent adequate security, connected infrastrcture may be vulnerable to cyber attack.
5. Smart technology and artificial intelligence 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 (see below).
6. Wireless technology 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.
7. Nano materials Nano materials (including Graphene) have tiny components. Their structural properties enable the manufacture of lightweight, resilient materials which can have embedded sensors. Such materials, which can be manufactured to meet specific functional requirements, have clear implications for combating crime. Examples would include lightweight but superstrong protective clothing for police officers.
8. Synthetic biology including CRISPR 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. The 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.
9. Blockchain The blockchain is an electronic, open, distributed ledger system used to verify and record transactions securely. It is perhaps best known as being the technology that underpins cryptocurrencies to include Bitcoin. It may fundamentally change economic and other transaction-based systems (e.g. Land and property registration systems), making them more secure. It may also have application in securing evidence in (digital) investigations. However, vulnerabilities might be exploited and, as cryptocurrencies are pseudonymous, they can and have facilitated cybercrime.
10. Quantum computing 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.