Chapter 12

Designing systems against crime

Introducing leaky systems[1]

Aiden Sidebottom and Nick Tilley

Introduction

Crime is known to concentrate in various ways. A small number of offenders are typically responsible for the majority of crimes committed (Budd *et al.*, 2005; Farrington and West, 1993; Wolfgang *et al.*, 1972). Some victims are repeatedly victimised, thereby experiencing a disproportionate amount of crime (Pease, 1998; Farrell, 2016). So-called crime 'hot spots' denote particular places with comparatively high levels of crime (Sherman *et al.*, 1989; Weisburd and Green, 1995). Products exhibit differential theft rates (Clarke, 1999). Crime is unevenly distributed over time (Felson and Poulsen, 2003). And, as Eck *et al.* (2007) demonstrate, when analysing the distribution of crime across a population of similar facilities such as bars, airports and hospitals, the bulk of offences concentrate on the risky few.

Immutable laws are seldom discussed outside the natural sciences. Yet such is the regularity with which crime is found to concentrate, the term 'law' has gradually been mooted. Weisburd (2015) refers to the *law of crime concentration at place* to describe how crime typically clusters in small geographic units (such as blocks and street corners). Similarly Wilcox and Eck (2011) talk of the *iron law of troublesome places* when referring to the recurrent finding that 'a small proportion of facilities produce a much larger proportion of the crimes' (p. 476). In sum, where crime is abundant, concentration is expected.

That crime is highly concentrated has important implications for crime prevention. Most obviously, it offers an efficient way of focusing preventive resources where crime is highest. Second, comparisons of high and low crime places, people and possessions can yield insights into the determinants of crime, which in turn can inform short-, medium- and long-term preventive responses. Third, identifying crime concentrations draws attention to those whose actions (or inactions) might help reduce crime, be that the manager of a bar or the handler of a persistent offender. 'Levers' might then be applied to encourage relevant parties to take greater responsibility for preventing problems (Scott, 2005).

In this chapter we propose a new form of crime concentration: that which emerges unintentionally from variations in intentionally produced regulations, policies and procedures. The less-than-perfect umbrella term used here to capture this source of concentration is 'system'. 'System' refers for present purposes to any set of organised or consciously developed habitual human behaviours.[2] *System* attributes are intentionally and knowingly created, even though they may produce unintended consequences.

The same objective may be pursued with different system attributes that bring with them different unintended consequences.

We are surrounded by systems. Many contemporary systems are largely or wholly electronic. For most people they are an important and common feature of daily life, be it for educational, recreational or vocations purposes. Most businesses and organisations are similarly reliant on various systems. It is hard to conceive of a world without systems: births and deaths could not be logged, governments could not collect taxes, vehicles could not be registered, patients could not be treated and so on. Examples of systems often used in everyday life include:

- banking systems
- navigational systems (such as GIS software)
- vehicle registration systems
- postal systems
- health care systems
- educational systems
- welfare payment systems
- criminal justice systems
- taxation systems
- financial control systems
- public transport systems
- retail stock control systems
- social networking systems (such as Facebook and Twitter)
- online auction systems (such as eBay and Gumtree).

There is much unsystematic behaviour that is relevant to crime opportunities and crime patterns, for example holidaymaking, pub-going, clubbing and so on. Such activities will be relevant to the production of crime patterns but are not 'systematic', as defined here, since they are not intentionally orchestrated or planned. Vulnerable, carefree and careless holidaymakers, unknowing about the riskiness of areas they visit, for instance, comprise easy crime targets, and their patterned victimisation is a predictable consequence of behaviours that individual holidaymakers engage in. What we have here is just the result of aggregates of individual choices that collectively constitute observably structured, but unplanned patterns of behaviour. This is not to say that these unstructured patterns are beyond engineering. Incentives of various sorts, taxes, signs, information and exhortation can all be used to try to manipulate unplanned patterns of behaviour in ways that reduce opportunities for crime. Yet such action is after the event and contrasts with the humanly designed systems of behaviour focused on in this chapter. This chapter is not, thus, concerned with patterned crime related behaviour as an emergent unintended consequence of aggregated individual actions. Rather its focus is on patterned unintended crime consequences of systems that that are purposively designed, even though the design may not be directed at crime.

Our argument in this chapter is that for any class of system developed to serve the same purpose, there is often variation in its design. Variation in system design can make some systems more criminogenic than others. Thus, as Eck and colleagues (2007) demonstrate for populations of homogeneous facilities, our hypothesis is that across a class of systems with the same purpose, a select few will account for much of the total

crime experienced. We call these 'leaky systems'.[3] If evidence were found to support this hypothesis, then the frequency of crime occurrence per system when plotted against crime rank would conform to the widely observed J-curve. How variations in system design might inadvertently produce crime is a neglected topic in the crime analysis literature. We know of no empirical examples investigating crime distributions across systems, as defined herein. As with other forms of crime concentration, we believe this might be a fruitful object of enquiry. Moreover, from a prevention perspective, it may usefully encourage others to think crime in the design of new systems (Pease, 1997; Ekblom, 2016).

The remainder of this chapter is as follows. In the next section we suggest nine ways in which the configuration of systems might facilitate crime. This is followed by some examples where the design of systems has produced reductions in crime. We then turn our attention to the main subject of this chapter: the distribution of crime across similar systems. We present a case study of the frequency of online romance scams across dating websites, taken here to be an example of a purposively designed system. We conclude by discussing the link between systems, places and crime concentrations.

How systems unintentionally create crime

There are several ways in which systems can be conducive to crime. What links the following examples is that in each case the specific system was well-intentioned: it was developed to meet specific needs or to serve specific purposes.

Systems can furnish rewards for crime

Systems can provide incentives for criminal behaviour. Variations in levels of excise duty on different sides of borders has for hundreds of years provided rich rewards for smuggling goods. Here, it is not a single system but the presence of more than one with different rates and scope to traffic between them that create the widely exploited crime opportunity.

Systems can make crime easy

The development of some systems unintentionally facilitates crime. Take fuel drive-offs. The method by which petrol is dispensed at service stations in some countries (such as the UK) makes driving off without payment easy. Customers serve themselves, there are no pump attendants, garage staff remain inside the service station building, payment is supposedly made after the tank is filled and means of escape are at hand (see La Vigne, 1994; Tilley, 2005).

Systems can make crime less risky

Financial accounting systems invariably involve some degree of independent monitoring to check for suspicious or fraudulent activity. The risk of fraud being detected is therefore influenced, in part, by the extent and/or thoroughness of such auditing. A system of accounting that does not routinely include independent expert audits, for reasons of cost, efficiency and so forth, would lower the risk of illegal behaviours being

discovered. A recent high-profile example is the parliamentary expenses scandal that was exposed in Britain in 2009. The publication of parliamentarians' allowances and expenses revealed widespread abuse in the form of false or excessive expense claims, carried out on the assumption that claims were rarely if ever queried.

Systems can facilitate crime planning

Where there are predictable systems, risks, rewards, effort and the tools needed for offending can all, in principle, be gauged in advance. Take robbery. Regular security patrols can better be avoided than random ones. Regular patterns of cash delivery can better be targeted than random ones. Standard staffing patterns can inform plans about needs for weapons or numbers of offenders, although in practice much planning of robbery seems at best rudimentary (Matthews, 2002).

Systems can disinhibit and provoke crime

Those who might not otherwise be intending to commit crimes may be disinhibited and provoked by virtue of systems in place. Take late-night city centre violence. Happy-hour drinks promotions in bars can create a supply of disinhibited drunks, who are liable to be violent and to be victims of violence (see Homel *et al.*, 1997). Specified closing times and restricted transport systems can create large numbers competing for means to get home late at night, provoking friction and potential clashes between disinhibited groups trying to access buses and taxis.

Systems can generate need

Though need and relative deprivation may drive some crime, which may thereby be a function of broader economic systems,[4] there are more immediate ways in which systems can create needs that in turn facilitate crime. Take electricity and gas cash-prepayment meter breaks, which became an increasing problem in Britain in the 1980s (see Hill, 1986). Meter breaks were found to take place disproportionately in relatively poor areas, and at mid-week (Hill, 1986; Forrester *et al.*, 1988, 1990). Systems for social security payments to all be on the same day each week may reduce the scope for mutual borrowing when money runs out, creating patterns of need that may be met by meter breaks the day before welfare payments are made.

Systems can create crime networks

Provisions for young offenders or those at risk of offending can bring them together. This may be the case for motor projects for those involved on the fringes of vehicle crime and also for holiday play-schemes in high crime neighbourhoods. In particular if sent home at the same time these groups can crystallise. Local authority housing allocation systems can likewise unintentionally lead to concentrations of networked offenders in particular areas (Bottoms *et al.*, 1992).

Systems can teach crime

To commit many crimes techniques have to be learned. Take drug-related rapes. Internet websites that are designed to allow potential victims to recognise when they might be at risk and the precautions that they can take also indicate the properties of specific drugs and the methods that can be used to take advantage of suitable victims. Likewise, reports on the Internet, in newspapers or on television, of offences and the easy ways in which they can be committed can all transmit information about crime techniques (see Matthews, 2002). One example relates to the slashing of curtains to curtain-sided trucks parked overnight at service areas. A description of the modus operandi and the names and addresses of a gang of offenders who had been convicted were published by the police on the Internet. Following this there was an explosive growth in the number of similar incidents (Tilley, 2005).

Systems can legitimatise crime

The routine non-enforcement of rules can lead to their perceived illegitimacy (see Sherman, 1990). Take littering. There is little or no enforcement of the law surrounding the dropping of litter. It then becomes widespread and quite normal. This process of growth in crime and disorder is at the heart of the Broken Windows theory (Wilson and Kelling, 1982), support for which comes from several artful experiments by Keizer *et al.* (2008).

How systems intentionally reduce crime

In the previous section we suggested some of the ways in which purposively designed systems might unintentionally facilitate crime. This section describes a variety of ways in which system design can reduce crime. Our list is not exhaustive. Our intention is simply to illustrate the different ways in which system design might affect crime. Examples include system modifications that have been introduced specifically to address crime problems as well as system changes introduced for non-crime reasons which nonetheless prompted unintended crime reducing effects.

Systems can make crime more risky

There are several examples of system changes that have been introduced with a view to increasing the risk or perceived risk to the prospective offender. An Australian one relates to the introduction of random breath-testing in New South Wales as a means of reducing drunk-driving and the casualties that are associated with it. Homel (1993) found that this system of enforcement in relation to driving under the influence of alcohol, when accompanied with growing public intolerance of drinking and driving, produced a substantial and sustained fall in the numbers of people killed through drink-driving incidents.

Mayhew *et al.* (1989) discuss an interesting case where a change in regulation brought with it an unintended crime reduction. They describe the fall in thefts of motorcycles that followed when wearing motorcycle helmets became compulsory in Germany, and when the regulation was also conscientiously enforced. In these circumstances, unless the prospective offender happened to be carrying a helmet or came prepared to commit the

theft by carrying one, he or she faced substantial risks of being caught driving off (helmetless) on a stolen motorcycle.

A more recent example concerns the reduction in metal thefts in England and Wales which coincided with changes to the system through which scrap metal is bought and sold. Levels of metal theft have increased significantly in the past decade, a period over which most other forms of acquisitive crime have recorded large reductions. Increases in metal theft have been shown to be strongly associated with global increases in the price of metal (Sidebottom *et al.*, 2011, 2014). Most stolen metals (such as copper cabling or lead roof tiles) hold little inherent value to the offender. Profit is realised on disposing them for cash. In England and Wales, the central means through which metal is bought and sold is through scrap metal dealerships, a process that traditionally was largely cash based and involved little if any paperwork, thereby presenting minimal risks of detection for metal thieves. In response to the growing problem of metal theft, cashless trading for scrap metal was introduced in December 2012, followed subsequently by a tougher licensing scheme. The rationale was that legitimate sellers of scrap metal would not be deterred by the new requirement to provide their (bank) details in order to dispose (and financially benefit) from the sale of metal. By contrast, those seeking to profit from the sale of illegally sourced metal would be reluctant to provide their details and, facing the prospect of possessing metal that they can no longer sell, would refrain from stealing metals. Invoking the 25 techniques of situational crime prevention (Cornish and Clarke, 2003), removing the ease with which scrap metal could be sold anonymously increased the risk that illegal activity might be detected. Several sources of evidence suggest that this system change contributed to the reductions in metal theft that occurred in England and Wales around 2012 (see Morgan *et al.*, 2015).

Systems can make crime more difficult

Across a wide range of problems system modification appears to be possible to make crime more difficult.

The first example, from Sweden, relates to cheque frauds in the 1970s (Knuttson and Kuhlhorn, 1997). The problem was one of cheque books being obtained illicitly and then individual cheques being presented fraudulently. This generated a large number of crime incidents per cheque book used. Each incident typically involved only a small sum of money: less than 300 Swedish Kroner (then around US$60). The reason for the high numbers of low-value cheque crimes was that the bank guaranteed payments below 500 Kroner and at less than 300 Kroner the recipient was not even required to obtain any evidence of the identity of the person paying by cheque. The system-change response was withdrawal of the bank guarantee and a requirement that evidence of the identity of the person paying the cheque be obtained in all cases, regardless of the amount payable. This was instituted in July 1971. Figure 12.1 shows the pattern of all reported cheque crime in Sweden from 1965 to 1978. It appears that an immediate, dramatic and sustained fall took place following the change in system.

Systems can make crime less rewarding

The most celebrated case of system design to deny rewards probably relates to the rapid removal of graffiti. Sloan Howitt and Kelling (1997) describe the issue of graffiti on

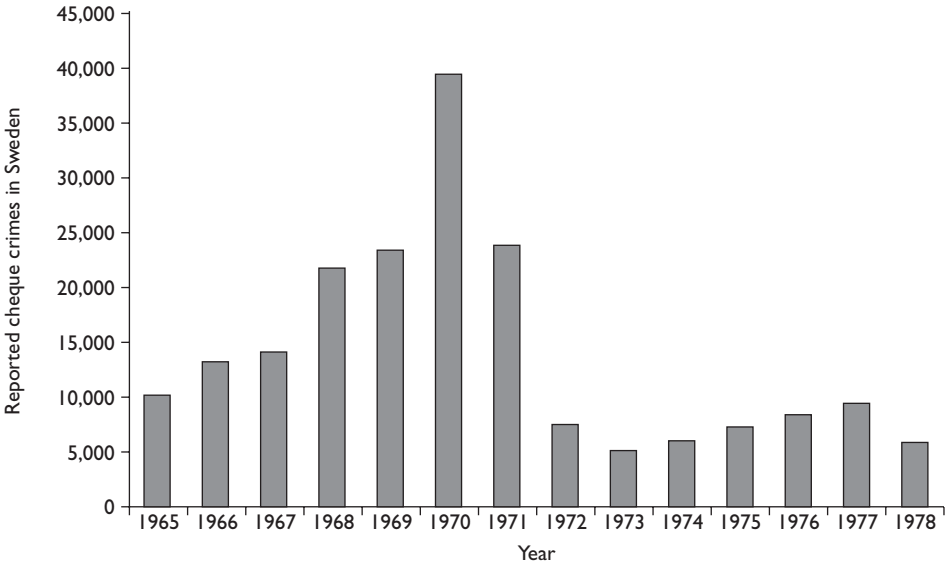

Figure 12.1 Reported cheque crimes in Sweden, 1965–1978.

New York subway trains. It had been a persistent and knotty problem, involving multiple offences. Though each was trivial in itself, collectively they impacted significantly on the quality of life of millions of New Yorkers. They started from the premise that graffiti artists get their crime rewards from seeing the results of their labours on display. The system development that eventually cracked the problem was the quick withdrawal from service of cars covered in graffiti, so that images could seldom be seen publicly. The reward that motivated the offender was removed. The New York City Transit Authority strategy was to clean a car and then ensure that it never again went into service with graffiti on it. Over a period of five years (1984–1989) all cars became free from graffiti, and new graffiti more or less stopped appearing. The cleaning was backed by enforcement with police riding clean cars, and targeting efforts at detection of repeat offenders who were recognisable from their graffiti tags. However, as the cleaning regime developed numbers of arrests for graffiti/vandalism actually fell. Those for felonies went down from 237 in 1984 to 114 in 1988, whilst those for misdemeanours declined from 2,681 to 974 over the same period.

Systems can reduce crime provocation

The apparently 'mindless' violence and disorder that is found in some entertainment and city centre areas late at night may be reduced by a number of system changes. A notable example involved reducing the widespread availability of cheap alcohol through special promotions. Special promotions with cut price drinks can lead to the congregation of large numbers of easily provoked inebriates, who are apt to confront one another violently as well as to behave in disorderly ways. A major demonstration project addressing this problem was undertaken in 1993 in Surfers Paradise, at the heart of the Gold Coast region in Queensland, Australia (Homel *et al.*, 1997).

In the small Central Business District of Surfers Paradise, there were 187 licensed premises and 22 nightclubs. Numbers of violent and disorderly incidents were rising, the reputation of the area was suffering, and some businesses were leaving as a consequence. Competition between bars led to drinks promotions providing cheap liquor and cost-minimising methods of management. A Venue Management Task Group devised a checklist for assessing the policies at each individual bar, covering:

1. discounting, including 'happy hours' and other binge drinking incentives;
2. pricing practices for low and standard alcohol beers;
3. information for staff about serving underage and intoxicated customers;
4. information given to customers, promoting the bar and its use;
5. under age policies about admission and serving those under age;
6. low and non-alcoholic drink availability;
7. instructions about response to and serving practices for those who are intoxicated;
8. times and ranges of food available;
9. entertainment used to promote the bar, and clientele targeted – from all-male to mixed;
10. transport provision;
11. the size of glasses and jugs used to serve alcohol;
12. policies relating to staff drinking, during and outside working hours;
13. strategies to deal with problem, drinking customers;
14. extent and nature of community and stakeholder group involvement;
15. personnel practices, including preferred staff style, recruitment, management, etc.;
16. security style, recruitment and training.

Out of these assessments came individual 'Model House Policies' for each licensee. The issues were discussed collectively by bar owners, who shared a sense of responsibility for their practices and recognised that they needed to change. A common Code of Practice emerged, which was eventually agreed by all but one licensee.

Adherence to the Code of Practice was monitored. Breaches were reported, for example with free drinks offers, 'specials' for alcohol sales or overcrowding. They were then discussed informally with the licensee – though it became apparent that informal mutual pressure needed to be backed with action by formal police and licensing authorities.

The overall changes in management practices were striking. There were statistically significant changes in all but two of the 16 areas of assessment listed above (staff drinking and personnel were the exceptions). There appeared to be real changes in management policies and procedures. Various outcome data suggested that there was also a substantial drop in violence and disorder. For example, the numbers of incidents recorded by security companies fell at a growing rate: from 235 to 192 incidents for January to March in 1992 and 1993 respectively (–18 per cent); from 215 to 115 for April to July (–47 per cent); and from 241 to 50 for August to November (–79 per cent). Bars were evidently managed in ways producing less drunkenness and less provocation, leading to fewer problems of violence and disorder.

Systems can remind potential offenders of rules

The infraction of formal rules constitutes crimes and misdemeanours. Such transgressions, however, often also involve forms of denial by offenders, so called 'techniques of neutralisation' (Sykes and Matza, 1957). Rule reminders prompt potential offenders, at the point of offending, to be aware that they are about to undertake a breach.

One example relates to the fraudulent return of goods to shops in exchange for cash. This is made easier where there are 'no questions' returns policies in place. Challinger (1997) discusses ways in which rule reminders were used by the retailer Coles Myer in Australia to reduce fraudulent returns. Measures included:

1 signs informing customers that proof of purchase would be required;
2 a requirement that proof of purchase be presented when goods were returned; and
3 where there was no proof of purchase

- a requirement of proof of personal identity when the goods were returned,
- a requirement for a handwritten and signed statement giving identity, address and details of the purchase,
- beyond specified sums, refunds by cheque only, and
- reimbursement to the alleged purchaser who paid by cheque only once the cheque had cleared.

There was scope for flexibility in the application of this policy, for example when known and long-term customers were concerned.

Across the company's 500 supermarkets, 391 discount stores and 70 department stores Challinger reports an indexed fall from 100 to 17 in the number of detected fraudulent returns and a fall from 100 to 37 in the dollar value following the system changes. He reports the largest reductions in the discount stores and lowest in supermarkets, reflecting the different types of good sold in each store format.

Systems can deny resources for crime

Offending often calls for resources. However much someone may want to commit a crime, if they lack the wherewithal to do so the offence will not take place (Ekblom and Tilley, 2000).

The most obvious denial of resource for offending occurs where there are restrictions on the sale of firearms, most particularly handguns. Handguns are clearly very useful in the commission of many serious crimes, including murder, robbery and rape. Where they, and ammunition for them, can readily be purchased then certain types of offending are facilitated. In the United States, although the crime rates for most offences are lower than those in the United Kingdom, a major exception relates to gun-related homicide. Although the statutory controls relating to firearms availability in the UK is far from perfect, the widespread use of replicas and air weapons (Schneider *et al.*, 2004; Morrison and O'Donnell, 1996; Wheal and Tilley, 2009) suggests that offenders are not easily able to obtain 'real' guns. Where such substitutes are used, the potential for injury during the conduct of the offence is much lower.

In the United States, the ready availability and increasing power, capacity and speed of handguns (specifically semi-automatics) can be used to explain rises in handgun

related homicides from the mid-1980s to the early 1990s and control over their supply in some measure explains their subsequent decline (Wintermute, 2000). Control over supply was achieved partly by police operations but more significantly by the Bureau of Alcohol, Tobacco and Firearms (ATF), which tightened the oversight of federally licensed dealers (including for example substantial checks on new applicants), leading to a reduction from 287,000 licensees in 1993 to 86,180 in 1999. Local jurisdictions added further controls. Wintermute gives the example of Oakland California, where the number of licence holders fell from 57 to seven in 1997 following the introduction of screening and background checks. Additional controls were also made on buyers, with checks before sales to them could be completed. A host of systems have been put in place, at least in some parts of the United States, reducing the supply of firearms as crime resources (see Cook and Goss, 2014).

Variations and concentrations: on the distribution of online romance frauds across dating websites

The preceding two sections described how different systems might facilitate or inhibit crime. Our focus now turns more fully to variation *within* sets of systems intended to meet some similar need or purpose. We contend that this variation might be associated with different crime risks, which in turn might inform ways in which particular systems might be configured to reduce crime opportunities. To examine this conjecture, we next focus on a specific type of crime associated with a particular set of systems, namely romance scams linked to online dating websites.

Online or Internet dating denotes 'the practice of using … web sites for the purpose of finding short- or long-term romantic partners' (Toma, 2015).[5] This typically involves users composing a profile that describes themselves and their relationship preferences, which is then used to connect the user to prospective partners. As Toma (2015) reports, different sites employ different matching procedures. Some sites allow users to perform key word searches to generate a list of prospective partners who exhibit sought-after characteristics (e.g. Match.com). Other sites use matching algorithms to identify those whose profiles suggest compatibility (e.g. eHarmony.com). Some use a combination of both (e.g. OKCupid.com).

The past decade has witnessed an explosion in the frequency and use of online dating sites. Accurately estimating the number of dating websites is challenging; new sites appear with such regularity that previous estimates are quickly rendered obsolete. This notwithstanding, recent reports suggest there were 1,400 online dating sites in 2009 in North America alone (Rege, 2009). In terms of dating website users, a large nationally representative survey (n = 19,131) found that just over one-third of marriages that took place between 2005 and 2012 in the United States originated online (Cacioppo *et al.*, 2013). Online dating evidently is no longer a niche activity. What was once stigmatised as a refuge for the undateables and a 'crutch for the desperate' (Toma, 2015, p. 2) is now a common and accepted feature of contemporary relationships.

The phenomenon of online dating has prompted a diverse range of scholarly activity. For example, research has investigated the differences between online and offline romantic unions (Finkel *et al.*, 2012), whether particular types of people are more likely to use dating websites (Sautter *et al.*, 2010), the extent and patterns of deception in online dating profiles (Toma *et al.*, 2008) and whether relationships that start online are

more 'successful' than relationships originating offline (Cacioppo *et al.*, 2013). From a criminological perspective, research has also considered the crime implications associated with the increased popularity of online dating. Such research is timely. Crime is known to follow opportunity (Felson and Clarke, 1998). Consequently, increases in the prevalence of online dating may generate increases in the number of crime opportunities associated with this activity, most notably online dating scams.

Online dating scams are a type of fraud. Individuals form romantic relationships through online dating sites under false pretences, for the purposes of defrauding victims for financial gain. Huang *et al.* (2015) identify several features that distinguish online dating scams from other types of Internet fraud (such as advanced fee fraud):[6] (1) victim–offender interaction usually takes the form of personalised messages rather than automatically generated messages which are circulated in bulk; (2) online dating scams often display a longer time course than other types of fraud since the fraudster must garner sufficient trust and confidence in the victim for them to part with their money. This sometimes involves face-to-face contact. And (3) online dating sites are purposively designed to connect individuals. Consequently the notion of unsolicited messages, which forms the basis of many anti-spam systems, is inapplicable.

Determining the true extent of online dating scams is challenging. The crime is novel, believed to have originated in the mid-2000s (Buchanan and Whitty, 2014). Questions on individuals' experience of online crime in general and romance scams in particular have only recently begun to feature in standard victimisation surveys (such as the Crime Survey of England and Wales). Extrapolating survey results from a nationally representative sample of adults in Britain in 2011 (n = 2,028), Whitty and Buchanan (2012) estimate that approximately 230,000 individuals experienced some form of online romance fraud by 2011. Figures on the number of dating scams reported to the Fraud Authority in England and Wales indicate a 34 per cent increase between 2014 and 2015 (from 2,040 offences to 2,736). These counts of crime are likely to be an underestimate, however. Button and colleagues (2014) suggest many online frauds are not reported to the authorities owing to victim embarrassment, and uncertainty about what constitutes online fraud and to whom such crimes should be reported.

An archetypal online romance scam is as follows (see Rege, 2009). Using an Internet dating site, the fraudster contacts the potential victim. An online conversation ensues, initially through the dating site and in some cases then moving to personal email or instant messaging applications. This conversation may take place over many months, in which time the fraudster seeks to establish a level of trust with the victim. Once established, the fraudster reports experiencing some unexpected event such as being robbed or receiving a hefty medical bill. A request for money is then lodged to help deal with the aftermath of such an event. Payment by the victim often prompts further requests for money.

The problem of online dating scams is understudied, likely owing to the aforementioned lack of relevant data. That research which is available has tended to concentrate on identifying the different types and processes of romance scams (e.g. Huang *et al.*, 2015), the attributes and behaviours that might increase someone's likelihood of victimisation (Buchanan and Whitty, 2014) and the costs and consequences of experiencing online romance scams (Whitty and Buchanan, 2015). Routine activity theory (Cohen and Felson, 1979) suggests that crime events occur when motivated offenders encounter suitable victims in places where guardianship is insufficient. Eck (2003)

arranged these core elements of crime – offender, victim, place – into the crime triangle, emphasising that crime can be prevented by blocking these three elements from converging in time and space. Research has recently demonstrated that the routine activity approach, initially proposed to explain the rate and distribution of common crime types (such as robbery), is also applicable to the generation and distribution of cybercrimes (see e.g. Reyns *et al.*, 2011). However, in the context of cyber-based systems, the term 'place', with its connotations of physical space, may be misleading. It fails to capture trans-locational *system* sources of vulnerability (such as a lack of guardianship) where the crime may be experienced by a victim at a particular place but is enabled by 'leakiness' in the system. Where this is the case, just as managers might usefully be mobilised to reduce crime opportunities at places, so too might system owners be prompted to do the same for crime opportunities generated by leaky systems (for a related discussion see Eck and Clarke, 2003).

Returning to online romance scams, existing research has thus concentrated on the 'offender' and 'victim' components of the crime triangle; little empirical research has investigated the specific cyber-spaces within which romance scams occur and, in particular, variation in crime across such cyber-spaces. This is the subject of the analysis that follows. In this instance the specific cyber-spaces to which we are referring are the online dating sites in which victims and offenders converge. Our question is whether online romance scams are unevenly distributed across online dating websites

Data

Data were acquired through a Freedom of Information request to the National Fraud Intelligence Bureau (NFIB) based at the City of London Police (UK). The NFIB was established in 2010 to gather intelligence on and combat fraud. Data were requested on all incidents of online romance fraud reported to the police in England and Wales from January 2013 to December 2014. Romance fraud is defined by the UK Home Office (2015) as an incident in which 'The intended victim is befriended on the Internet and eventually convinced to assist their new love financially by sending them money for a variety of emotive reasons.'

Across the study period, 6,171 incidents of online romance fraud were reported to the police. For the purposes of our analysis, we were only interested in those incidents where the victim reported a dating website on which they met the offender(s), which occurred in 2,909 cases (47 per cent of the original total reports). From this subset of incidents, cases were removed if (1) the stated website is not in fact a dating website, (2) the victim did not populate the report with correct website details or (3) information on the particular website was left blank. These deletions, which were performed by a member of the NFIB team, led to a final sample of 1,169 incidents (19 per cent of the original total cases). These incidents were then analysed using free text word searches to identify the name of the online dating website.

Before reporting our results, we acknowledge that we are unable to determine the impact of the aforementioned losses in data on the representativeness of our final sample. Moreover, it should be noted that providing information on the website on which victims experienced romance fraud is not mandatory. Consequently, victims may have omitted details either deliberately (e.g. out of embarrassment) or accidentally (e.g. due to mistakes made when reporting the incident). We also do not know whether victims on

certain dating websites are systematically more likely to report incidents of fraud than victims on other dating websites. For example, we might expect lower levels of reporting (or at least a failure to name the website) for dating sites that are specifically designed for individuals who are married or in a committed relationship. Although we cannot measure this using our data, it is noteworthy that dating websites that are synonymous with short-term dalliances and extra-marital liaisons did not feature in our sample. We might therefore infer that selective reporting is plausible. Finally, we do not have information on those dating websites where no reported incidents of romance fraud took place.

Results

Figure 12.2 shows the distribution of online romance fraud reports across 37 online dating websites. We see a classic J-curve. Simply put, most dating websites experience few romance frauds and a small number experience a lot. The site with the largest number of romance scams (n = 494) accounts for 42 per cent of all reported incidents of romance fraud across our sample of dating sites. The top five sites account for 78 per cent (n = 906) of all reported incidents. These sites are, however, deviations from the norm. The modal number of fraud incidents across the 37 dating sites is one (mean = 32; median = 6). To reiterate, this is the lowest possible modal score since our data did not include sites where no scams took place. This finding matches that of Eck *et al.* (2007): where data containing zero-crime sites were available, zero was the modal number.

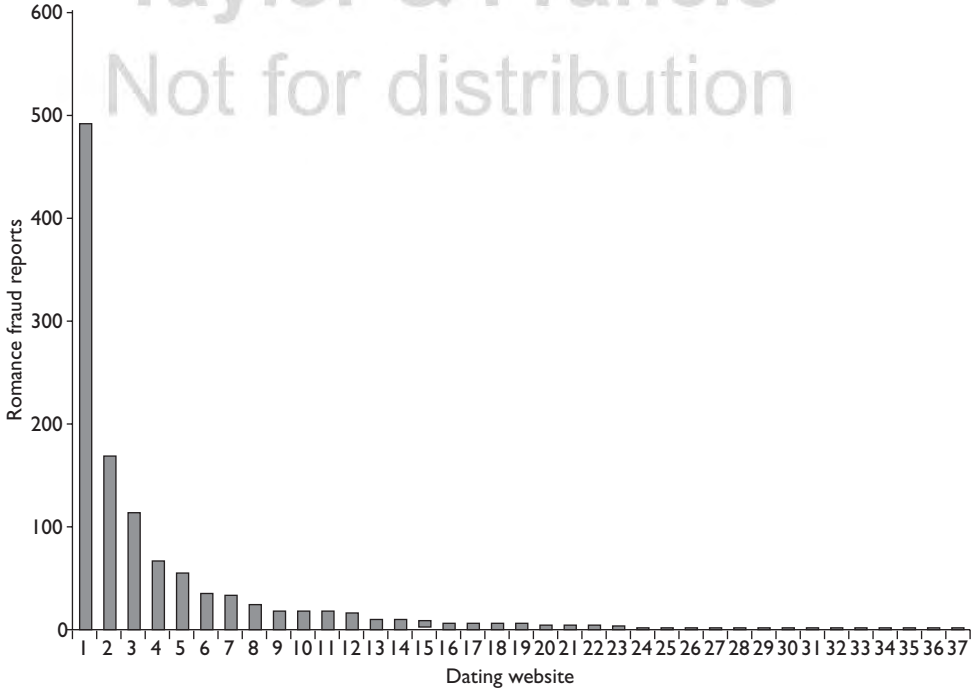

Figure 12.2 Online romance frauds by dating website.

Source: City of London Police recorded crime data, January 2013 to December 2014.

Eck *et al.* (2007) offer several explanations for why crime is unevenly distributed across sets of similar facilities. One explanation is that the ordering of facilities simply reflects the availability of crime targets, which in turn might be a consequence of variations in size. Take bars. More troublesome bars might be larger than less troublesome bars and thus higher counts of crime may be an artefact of more people (and crime targets) being present. To examine this requires the production of a crime rate rather than crime counts. The same explanation is applicable here. The ordering of dating sites on the x-axis of Figure 12.2 may reflect variations in the number of website users, site 1 having the largest user base, followed by site 2 and so on. To the best of our knowledge, there is no single data set containing the number of registered and/or active users per dating site (nor for that matter is there a database which contains all known dating websites). To determine whether the pattern observed in Figure 12.2 can be explained by variation in the number of users per site, we used information freely available at SimilarWeb – an IT company which collects and analyses web traffic – on the estimated number of visits to each site in May 2015 (the time of writing). We acknowledge that there are some limitations with our choice of denominator. The number of users in the selected month (May 2015) may not accurately reflect usage per website over the study period (January 2013 to December 2014). Moreover, we have no way of determining the proportion of registered users who were active over the study period and hence at risk of victimisation. Information was available for all but three of the dating sites in our sample.

Figure 12.3 shows the distribution of online romance frauds per million visitors to each dating site. A Pearson correlation indicates that there is no statistically significant relationship between the count of reported romance scams and the rate per million site visitors ($r = -0.040$, $p > 0.05$).

We use the term 'leaky' to describe those dating websites within which crime is most heavily concentrated. We can speculate as to what might account for the highly skewed distribution of romance scams across dating sites. One explanation might relate to whether the dating site requires users to pay a fee to register. Entering payment details might act as a deterrent to those who register for dating sites with the intention of defrauding others. A second explanation relates to the systems within the systems, in this case how different sites seek to identify fraudulent activity. Huang *et al.* (2015) describe four methods used by online dating websites to detect romance fraud, based on the assumption that scam accounts display behaviours that are reliably different from that of most legitimate dating profiles. Different systems attempt to identify fraudulent activity by focusing on: (1) the behaviours or characteristics of an account (e.g. scam accounts are judged more likely to be involved in multiple conversations at a time), (2) IP addresses (e.g. multiple accounts to one IP address), (3) photographs (e.g. multiple accounts using the same profile picture) and (4) text-based indicators (e.g. words judged to be commonly associated with fraudulent activity) (Huang *et al.*, 2015). Regrettably, data were unavailable on the type(s) of scam detection system(s) used across the online dating sites included here, although it is expected that this might influence vulnerability to scammers.

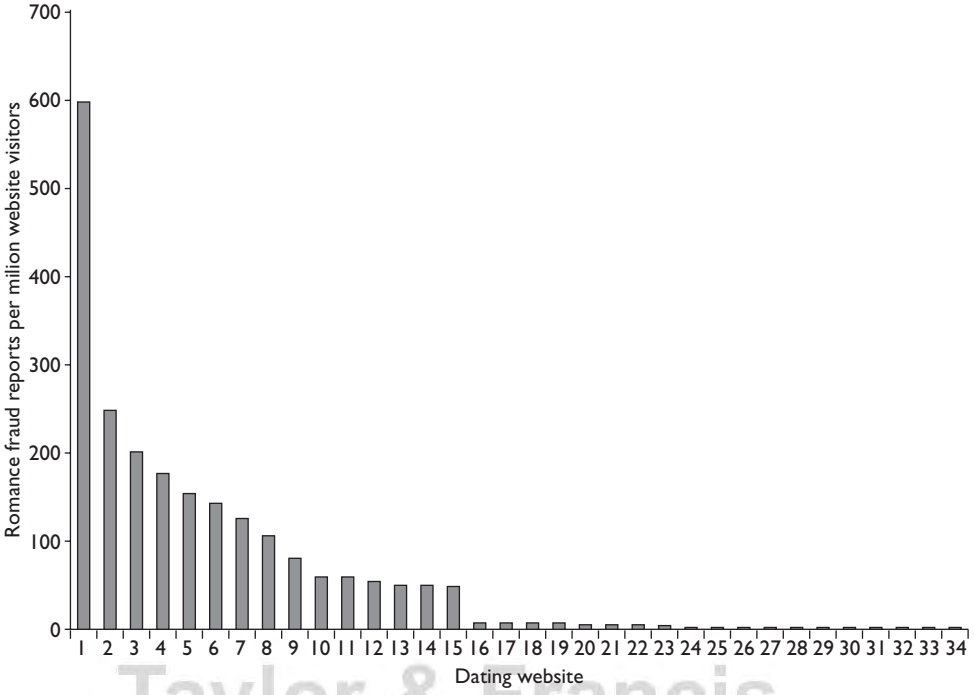

Figure 12.3 Online romance frauds per one million visitors to online dating website (January 2013 to December 2014).

Note
The numbers on the x-axis of Figure 12.3 do not correspond to the numbers on the x-axis of Figure 12.2.

The relationship between leaky systems, places and other types of crime concentration

In the latter part of this chapter we have focused on the problem of online romance scams to test the hypothesis that such offences are unevenly distributed across a set of systems intended to achieve broadly the same objectives. By definition, the systems analysed in this example – dating websites – are exclusively web based, with little connection to places. Our selection of an entirely web-based system should not, however, be interpreted as evidence that leaky systems have no relationship with place. On the contrary, there are several instances where systems and places interact. We referred to some previously, such as the concentrations of alcohol related violence around some bars as a consequence of their policies and practices (Homel *et al.*, 1997). Likewise school transit systems which routinely bring together large numbers of school children at specific locations (such as major transit hubs) may inadvertently produce convergent settings (Felson, 2003) which in turn might generate and radiate crime. Systems and places thus can, and often do, overlap. Yet despite these potential intersections between places and systems, in the case of online romance scams we would not necessarily expect the concentration associated with some dating websites to be expressed in associated concentrations of such scams on particular victims, places or products. We contend that leaky systems therefore comprise a distinct type of

crime concentration, albeit that we expect leaky systems often also to be interlinked with other forms of crime concentration.

In some cases where crime is geographically concentrated preventive efforts may be best targeted on the enabling system. For example, Graycar and Felson (2010) cite estimates that more than 70 per cent of Indonesia's total timber harvest is illegal (p. 81). They attribute this apparent concentration to 'weak governance', enabling rich pickings from 'bribery, graft, kickbacks, extortion, misappropriation, abuse of discretion, self-dealing, patronage, nepotism, favouritism, conflict of interest and political corruption' (p. 86), as value (and hence potential profit) is added to illegally sourced timber as it moves from forest to final consumer. Their situational crime prevention proposals are all system focused, and include:

> (1) Improve how timber is traced (increase risk); (2) Improve the timber labeling technology (increase effort); (3) Make vehicles more traceable (increase risk); (4) Enhance inventory control and chain of custody (reduce rewards); (5) Reduce official discretion (increase effort); (6) Reduce procedural complexity (remove excuses); and (7) Create simpler and more visible accounting formats and systems (increase risk).
>
> (p. 89)

Indonesia's timber trade comprises a leaky system, as we conceive it here, and Graycar and Felson's recommended preventive strategies are focused on plugging the leaks. The central thrust of this chapter is that comparisons across a set of systems intended to serve the same function might usefully shed light on the sources of such leaks, as well as assist in formulating methods to plug them. Continuing with Graycar and Felson's example, this would involve an assessment of different types of timber processing systems, and their relationship with timber theft. Presently systems-focused crime analysis of this sort is rare. We think it deserves more attention.

Conclusion

In this chapter we have argued that systems, broadly understood to include intentionally produced regulations, policies and procedures are important to the production and reduction of crime problems. Like other forms of crime concentration, we proposed that crime is unevenly distributed across particular classes of system intended to serve the same purpose, reflecting variations in opportunity as a function of different system designs. We provided evidence for this by examining the distribution of online romance scams by dating websites. Our results are consistent with expectation: a small number of dating websites were responsible for the vast majority of all online romance scams. We contend that similar concentration patterns might be observed in other system types, a pattern that we have called 'leaky systems'. That particular system designs are more susceptible to crime offers early opportunities to think crime and crime prevention rather than waiting for crime harvests to follow, just as is the case with new products or the design of new estates or buildings. Any new large-scale development – a town, housing estate, shopping complex, government organisation, business, hospital, airport, railway station, road network, holiday resort, library, university, entertainment centre, car park,

motorway service area, form of taxation, benefit entitlement – will potentially create crime opportunities, provocations and incentives. It makes sense to try to take account of this in the design of systems as well as of any physical space.

Acknowledgements

We thank Ronald V. Clarke and John E. Eck for encouraging us to revise this chapter and for suggested the term 'leaky systems'. We also thank the NFIB at the City of London Police for responding to our Freedom of Information request and providing the data analysed here. Finally we are grateful to Rachel Armitage, Ronald V. Clarke, Ella Cockbain, John E. Eck and Gianluca Stringhini for commenting on earlier drafts of this chapter.

Notes

1 This chapter is a substantially revised version of N. Tilley (2005). Crime prevention and system design. In N. Tilley (ed.) *Handbook of Crime Prevention and Community Safety*. Cullompton, Devon: Willan.
2 *Consciously developed* habitual behaviour is distinguished from habitual behaviour that is reproduced without intention. It is a product of design, rather than instinct, affect or after-the-event reinforcement.
3 We thank Ronald V. Clarke for suggesting this phrase.
4 These bigger macro level systems are not considered in this chapter.
5 We recognise that Internet dating can also be facilitated via smartphone dating applications such as Tinder, Grindr and Happn. The focus of this chapter, however, is limited to dating websites.
6 Cross and Blackshaw (2015, p. 120) define advanced fee fraud as incidents 'where a person is asked to send a small amount of money with the promise of receiving a larger amount of money in the future, and is seen in the example of inheritance notifications, investment invitations, and employment opportunities'. So-called 419 scams are a common type of advanced fee fraud, '419' denoting the Nigerian Criminal Code which this scam violates.

References

Bottoms, A., Claytor, A. and Wiles, P. (1992). Housing markets and residential community crime careers: a case study from Sheffield. In D. Evans, N. Fyfe and D. Herbert (eds), *Crime, Policing and Place*. London: Routledge.

Buchanan, T. and Whitty, M.T. (2014). The online dating romance scam: causes and consequences of victimhood. *Psychology, Crime and Law*, 20(3): 261–283.

Budd, T., Sharp, C. and Mayhew, P. (2005). Offending in England and Wales: first results from the Crime and Justice Survey. Home Office Research Study 275, Home Office, London.

Burgess, S. (1999). Operation ACNE. Unpublished entry for 1999 Tilley Award for Problem Oriented Policing, Cumbria Constabulary.

Button, M., McNaughton Nicolls, C., Kerr, J. and Owen, R. (2014). Online frauds: learning from victims why they fall for these scams. *Australian and New Zealand Journal of Criminology*, 47: 391–408.

Cacioppo, J.T., Cacioppo, S., Gonzaga, G.C., Ogburn, E.L. and VanderWeele, T.J. (2013). Marital satisfaction and break-ups differ across on-line and off-line meeting venues. *Proceedings of the National Academy of Sciences*, 110(25): 10135–10140.

Challinger, D. (1997). Refund fraud in retail stores. In R.V. Clarke (ed.), *Situational Crime Prevention: Successful Case Studies*. New York: Harrow & Heston.

Clarke, R. (1999). Hot products: understanding, anticipating and reducing demand for stolen goods. Police Research Series Paper 112, Home Office; London.

Cohen, L.E. and Felson, M. (1979). Social change and crime rate trends: a routine activity approach. *American Sociological Review*, 44: 588–608.

Cook, P. and Goss, K. (2014). *The Gun Debate*. Oxford: Oxford University Press.

Cornish, D.B. and Clarke, R.V. (2003). Opportunities, precipitators and criminal decisions: a reply to Wortley's critique of situational crime prevention. In M.J. Smith and D.B. Cornish (eds), *Theory for Situational Crime Prevention*. Crime Prevention Studies, Vol. 16. Monsey, NY: Criminal Justice Press.

Cross, C. and Blackshaw, D. (2015). Improving the police response to online fraud. *Policing*, 9(2): 119–128.

Eck, J.E. (2003). Police problems: the complexity of problem theory, research and evaluation. In J. Knutsson (ed.), *Problem-Oriented Policing: From Innovation to Mainstream*. Monsey, NY: Criminal Justice Press.

Eck, J.E. and Clarke, R.V. (2003). Classifying common police problems: a routine activity approach. In M.J. Smith and D.B. Cornish (eds), *Theory for Situational Crime Prevention*. Crime Prevention Studies, Vol. 16. Monsey, NY: Criminal Justice Press.

Eck, J.E., Clarke, R.V. and Guerette, R. (2007). Risky facilities: crime concentration in homogenous sets of establishments and facilities. In G. Farrell, K.J. Bowers, S.D. Johnson and M. Townsley (eds), *Imagination for Crime Prevention: Essays in honour of Ken Pease*. Monsey, NY: Criminal Justice Press.

Ekblom, P. (2016). Crime prevention through product design. In N. Tilley and A. Sidebottom (eds), *Handbook of Crime Prevention and Community Safety* (2nd edition). Oxford: Routledge.

Ekblom, P. and Tilley, N. (2000). Going equipped: criminology, situational crime prevention and the resourceful offender. *British Journal of Criminology*, 40(3): 375–398.

Farrell, G. (2016). Repeat victimization. In N. Tilley and A. Sidebottom (eds), *Handbook of Crime Prevention and Community Safety* (2nd edition). Oxford: Routledge.

Farrington, D.P. and West, D.J. (1993). Criminal, penal and life histories of chronic offenders: risk and protective factors and early identification. *Criminal Behaviour and Mental Health*, 3(4): 492–523.

Felson, M. (1998). *Crime and Everyday Life* (2nd edition). Thousand Oaks, CA: Pine Forge Press.

Felson, M. (2003). The process of co-offending. In M.J. Smith and D.B. Cornish (eds), *Theory for Practice in Situational Crime Prevention*. Monsey, NY: Crime Prevention Studies.

Felson, M. and Clarke, R. (1998). *Opportunity Makes the Thief*. Police Research Series Paper 98, Home Office, London.

Felson, M. and Poulsen, E. (2003). Simple indicators of crime by time of day. *International Journal of Forecasting*, 19(4): 595–601.

Finkel, E.J., Eastwick, P.W., Karney, B.R., Reis, H.T. and Sprecher, S. (2012). Online dating: a critical analysis from the perspective of psychological science. *Psychological Science in the Public Interest*, 13: 3–66.

Forrester, D., Chatterton, M. and Pease, K. with the assistance of Robin Brown (1988). The Kirkholt Burglary Prevention Project, Rochdale. Crime Prevention Unit Paper 13, Home Office, London.

Forrester, D., Frenz, S., O'Connell, M. and Pease, K. (1990). The Kirkholt Burglary Prevention Project, Phase II. Crime Prevention Unit Paper 23, Home Office, London.

Graycar, A. and Felson, M. (2010). Situational prevention of organised timber theft and related corruption. In K. Bullock, R.V. Clarke and N. Tilley (eds), *Situational Prevention of Organised Crimes*. Cullompton: Willan.

Hill, N. (1986). Prepayment coin meters: a target for burglary. Crime Prevention Unit Paper 6, Home Office, London.

Home Office (2015). *Home Office Counting Rules For Recorded Crime*. Accessed online, 17 March 2016 at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/421319/count-fraud-april-2015.pdf.

Homel, R. (1993). Drivers who drink and rational choice: random breath testing and the process of deterrence. In R.V. Clarke and M. Felson (eds), *Routine Activity and Rational Choice: Advances in Criminological Theory*, Vol. 5. New Brunswick, NJ: Transaction Press.

Homel, R., Hauritz, M., McIlwain, G., Wortley, R. and Carvolth, R. (1997). Preventing drunkenness and violence around nightclubs in a tourist resort. In R.V. Clarke (ed.), *Situational Crime Prevention: Successful Case Studies* (2nd edition). New York: Harrow & Heston.

Huang, J-M., Stringhini, G. and Yong, P. (2015). Quit playing games with my heart: understanding online dating scams. Proceedings of the 2015 Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA).

Keizer, K., Lindenberg, S. Steg, L. (2008). The spread of disorder. *Science*, 322(5908): 1681–1685.

Knuttson, J. and Kuhlhorn, E. (1997). Macro measures against crime: the example of check forgeries. In R.V. Clarke (ed.) *Situational Crime Prevention: Successful Case Studies* (2nd edition). New York: Harrow & Heston.

LaVigne, N. (1994). Gasoline drive-offs: designing a less convenient environment. In R.V. Clarke (ed.) *Crime Prevention Studies*, Vol. 2. Monsey, NY: Criminal Justice Press.

Matthews, R. (2002) *Armed robbery*. Cullompton: Willan.

Mayhew, P., Clarke, R. and Elliot, D. (1989). Motorcycle theft, helmet legislation and displacement. *Howard Journal*, 28: 1–8.

Morgan, N., Hoare, J. and Byron, C. (2015). An evaluation of government and law enforcement interventions aimed at reducing metal theft. Research Report 80, Home Office, London.

Morrison, S. and O'Donnell, I. (1996). An analysis of decision-making practices of armed robbers. In R. Homel (ed.) *The Politics and Practice of Situational Crime Prevention*. Crime Prevention Studies, Vol. 5. Monsey NY: Criminal Justice Press.

Pease, K. (1997). Predicting the future: the roles of routine activity and rational choice theory. In G. Newman, R. Clarke and S. Shoham (eds), *Rational Choice and Situational Crime Prevention*. Aldershot: Dartmouth.

Pease, K. (1998). Repeat victimisation: taking stock. Crime Detection and Prevention Paper Series Paper 90, Home Office, London.

Rege, A. (2009). What's love got to do with it? Exploring online dating scams and identity fraud. *International Journal of Cyber Criminology*, 3(2): 494–512.

Reyns, B.W., Henson, B. and Fisher, B.S. (2011). Being pursued online: applying cyber lifestyle-routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior*, 38(1): 1149–1169.

Sautter, J., Tippett, R.M. and Morgan, S.P. (2010). The social demography of Internet dating in the United States. *Social Science Quarterly*, 91: 554–575.

Schneider, J., Rowe, N., Forrest, S. and Tilley, N. (2004). Biting the bullet: gun crime in Greater Nottingham. Unpublished Report to Nottinghamshire Constabulary.

Scott, M. (2005). Shifting and sharing police responsibility to address public safety problems. In N. Tilley (ed.), *Handbook of Crime Prevention and Community Safety* (1st edition). Cullompton: Willan.

Sherman, L. (1990). Police crackdowns: initial and residual deterrence. In M. Tonry and N. Morris (eds), *Crime and Justice: A Review of Research*, Vol. 12. Chicago, IL: University of Chicago Press.

Sherman, L.W., Gartin, P.R. and Buerger, M.E. (1989). Hot spots of predatory crime: routine activities and the criminology of place. *Criminology*, 27: 27–56.

Sidebottom, A., Ashby, M. and Johnson, S.D. (2014). Copper cable theft: revisiting the price–theft hypothesis. *Journal of Research in Crime and Delinquency*, 51(5): 684–700.

Sidebottom, A., Belur, J., Bowers, K., Thompson, L. and Johnson, S.D. (2011). Theft in price-volatile markets: on the relationship between copper price and copper thefts. *Journal of Research in Crime and Delinquency*, 48: 396–418.

Sloan Howitt, M. and Kelling, G. (1997). Subway graffiti in New York City: 'getting up' vs. 'Meanin' it and cleanin' it'. In R.V. Clarke (ed.) *Situational Crime Prevention: Successful Case Studies* (2nd edition). New York: Harrow & Heston.

Sykes, G. and Matza, D. (1957) Techniques of neutralisation. *American Sociological Review*, 22: 664–670.

Tilley, N. (2005). Driving down crime at motorway service areas. In M. Smith and N. Tilley (eds), *Crime Science: New Approaches to Preventing and Detecting Crime*. Cullompton: Willan.

Toma, C.L. (2015). Online dating. *The International Encyclopedia of Interpersonal Communication*, 1–5. Accessed online, 1 December 2016 at: http://onlinelibrary.wiley.com/doi/10.1002/9781118540190.wbeic118/abstract.

Toma, C.L., Hancock, J.T. and Ellison, N.B. (2008). Separating fact from fiction: an examination of deceptive self-presentation in online dating profiles. *Personality and Social Psychology Bulletin*, 34: 1023–1036.

Weisburd, D. (2015). The 2014 Sutherland address: the law of concentration and the criminology of place. *Criminology*, 53: 133–157.

Weisburd, D. and Green, L. (1995). Policing drug hot Spots: the Jersey City DMA experiment. *Justice Quarterly*, 12: 711–736.

Wheal, H. and Tilley, N. (2009) Imitation gun law: an assessment. *Howard Journal*, 48(2): 172–183.

Whitty, M.T. and Buchanan, T. (2012). The online dating romance scam: a serious crime. *Cyberpsychology, Behavior, and Social Networking*, 15(3): 181–183.

Whitty, M.T. and Buchanan, T. (2015). The online dating romance scam: the psychological impact on victims – both financial and non-financial. *Criminology and Criminal Justice*, 1–19.

Wilcox, P. and Eck, J.E. (2011). Criminology of the unpopular: implications for policy aimed at payday lending facilities. *Criminology and Public Policy*, 10(2): 473–482.

Wilson, J. and Kelling, G. (1982). Broken windows. *Atlantic Monthly*, March, 29–38.

Wintermute, G. (2000) Guns and gun violence. In A. Blumstein and J. Wallman (eds), *The Crime Drop in America*. Cambridge: Cambridge University Press.

Wolfgang, M.E., Figlio, R.M. and Sellin, T. (1972). *Delinquency in a Birth Cohort*. Chicago, IL: University of Chicago Press.