TU Delft

Delft University of Technology

# Computer science

Hartel, Pieter; Junger, Marianne

**DOI**
10.4324/9780203431405

**Publication date**
2018

**Document Version**
Final published version

**Published in**
Routledge Handbook of Crime Science

**Citation (APA)**
Hartel, P., & Junger, M. (2018). Computer science. In R. Wortley, A. Sidebottom, N. Tilley, & G. Laycock (Eds.), *Routledge Handbook of Crime Science* (1st ed., pp. 179-189). Routledge - Taylor & Francis Group. https://doi.org/10.4324/9780203431405

**Important note**
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

**Copyright**
Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

**Takedown policy**
Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

*This work is downloaded from Delft University of Technology.*
*For technical reasons the number of authors shown on this cover page is limited to a maximum of 10.*

# Routledge Handbook of Crime Science

*Edited by Richard Wortley, Aiden Sidebottom, Nick Tilley and Gloria Laycock*

First published 2019

ISBN: 978-0-415-82626-6 (hbk)
ISBN: 978-0-203-43140-5 (ebk)

12

## Computer science

*Pieter Hartel and Marianne Junger*

CC BY-NC-ND 4.0

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

# 12
# Computer science

*Pieter Hartel and Marianne Junger*

## Introduction

Marcus Felson and Mary Eckert, in their recent book *Crime and Everyday Life* (Felson and Eckert, 2016) describe how technology has influenced crime. When most people lived in 'the village' without the technology to venture far from home, villagers suffered crime from marauding bandits. The domestication of horses increased people's reach and created 'the town'. Horses and wagons became new tools and targets of crime. Then nautical technology created 'the convergent city', with ships providing new tools and the cargo the target. Then 'the divergent metropolis', arrived, thanks to modern transportation technology. Cars are not only an important target of crime but a powerful tool too.

We now live in 'the connected world', where computers and networks are both a target of crime as well as a powerful tool. A recent report from the UK National Crime Agency states that for the first time in history there is more recorded cyber-crime than traditional crime (NCA, 2016). Therefore students of crime need at least a basic understanding of the role that computers and networks play in the commission of crime, in the prevention of crime, and also in the study of crime. This chapter gives an introduction to these topics from the crime-science perspective, but we begin by giving three examples to illustrate the main point.

- Phishing is one of the most popular ways of using computers and networks in the commission of crime because the technology scales well. It is almost as easy to send one phishing email as to send millions. Even with a success rate as low as $10^{-5}$ phishing can be profitable (Milletary, 2013).
- Security cameras are ubiquitous in the UK and in many other countries. In a modern city with a good networking infrastructure, security cameras are a scalable technology. Therefore, it is possible to keep a watchful eye on many places of interest and indeed studies have shown that the technology can contribute to crime prevention (Welsh and Farrington, 2008).
- Computational social science is a field of study where the power of computers and networks is used to study social sciences. For example, a computer program can simulate behaviour predicted by a theory. If the results are not realistic, the theory is probably wrong.

This is usually a much cheaper way of refuting a theory than conducting an experiment (von der Heyde, Miebach, and Kluge, 2014; Rosoff, Cui, and John, 2014). Again the technology scales well.

In this chapter we will explore the relationship between crime and computers and networks by answering the following questions:

- Which techniques from computer science can be used to prevent crime?
- Which techniques from computer science can be used to study crime?

To address the first question we use the 25 techniques of situational crime prevention to provide a systematic assessment of how computer and network technology can be used to prevent crime. The second question will be addressed by discussing computer simulation methods in cases where real experiments with crime prevention would be too costly or impractical.

## Crime prevention

Borrowing from situational crime prevention, crime science offers five principles to prevent crime or to deter the offender.

1 Increase the effort needed for crime, for example better locks require more effort to pick, or better passwords require more effort to guess.
2 Increase the risks of crime, for example well-lit windows increase the risk of being caught during burglary, or an operator monitoring the network increases the risk of being caught during a hacking attempt.
3 Reduce the rewards of crime, for example marked parts of a stolen vehicle are harder to fence, or encrypted data is harder to sell.
4 Reduce provocations that invite criminal behaviour, for example rapid cleaning of graffiti discourages the application of more graffiti, or rapid restoration of defaced websites discourages repetition.
5 Remove excuses for criminal behaviour, for example many systems specify an acceptable use policy that informs users of what behaviour is acceptable.

For each of the five principles, five generic techniques of situational crime prevention have been developed. Together, they are known as the '25 techniques of situational crime prevention'.

We have found seven reviews in the literature that suggest how computers and networks can be used as a specific instance of the 25 generic techniques (Beebe and Rao, 2005; Brookson et al., 2007; Coles-Kemp and Theoharidou, 2010; Morris, 2004b; Newman and Clarke, 2003; Willison and Siponen, 2009; Reyns, 2010).

Table 12.1 compares the way in which the reviews suggest how computer science techniques can be used to prevent crime. We list 12 techniques that have been mentioned at least three times in the reviews and then describe them in some detail below. For the remaining techniques we refer the reader to the references provided.

1 A password or PIN code used to authenticate a user.
2 Encryption of data files to ensure that once encrypted, they can be read only when the correct decryption key is known.
3 A firewall that is used to stop potentially malicious connections to a computer or network.

*Table 12.1* The 25 generic techniques used to structure popular information security techniques (some definitions of acronyms follow)

| *Increase effort* | *Increase risks* | *Reduce rewards* | *Reduce provocation* | *Remove excuses* |
|---|---|---|---|---|
| **1 Harden target**<br>• Firewalls<br>• Vulnerability patches<br>• Encryption<br>• Antivirus<br>• ISP as a first line of defence<br>• IDS | **6 Extend guardianship**<br>• RFID | **11 Conceal targets**<br>• DMZ | **16 Reduce frustrations** | **21 Set rules**<br>• Educate end-users<br>• Provide a clear code of conduct |
| **2 Control access**<br>• Authentication using passwords, pins<br>• Caller-ID like technology for internet<br>• Logical: IDS<br>• Logical: Firewalls | **7 Natural surveillance**<br>• Report suspect email and information request to ISP | **12 Remove targets** | **17 Avoid disputes** | **22 Post instructions** |
| **3 Screen exits**<br>• IDS<br>• Antivirus<br>• Audit trail<br>• Audit trail<br>• Logical: Firewalls | **8 Reduce anonymity**<br>• RFID<br>• Caller-ID<br>• Audit trails | **13 Identify property**<br>• RFID | **18 Reduce arousal** | **23 Alert conscience**<br>• Public awareness on the consequences of crime<br>• Educate: 'copying software is stealing' |
| **4 Deflect offenders** | **9 Place Managers**<br>• IDS | **14 Disrupt markets**<br>• ISP should be keen to assist investigations | **19 Neutralise peer pressure** | **24 Assist compliance**<br>• Security education of staff |
| **5 Control facilitators**<br>• Caller-ID<br>• Make the ISP accountable for the traffic | **10 Formal surveillance**<br>• Auditing and trail reviews<br>• RFID<br>• Early warning systems of viruses and hacking attacks<br>• IDS | **15 Deny benefits**<br>• Encrypt valuable data | **20 Discourage imitation**<br>• Prompt software patching | **25 Control disinhibitors**<br>• Cyber-ethics education<br>• Campaign against hacker culture |

4 A de-militarised zone (DMZ) used to isolate the public web server of an organisation from the internal network.
5 An intrusion detection system (IDS) used to stop potentially malicious information being sent to a computer or network.
6 A virus scanner used to detect malicious code in the information being sent to a computer or network.
7 Prompt software patching to remove vulnerabilities as soon as a correction has been published.
8 A radio-frequency identification (RFID) tag used to provide information about the product to which it is attached.
9 The caller-ID feature of the telephone system used to inform the recipient of a telephone call who is calling.
10 An audit log used to collect relevant operational data that can be analysed when there is an incident.
11 An internet service provider (ISP) can assist its clients in using the information super highway responsibly.
12 User education, which is included in the list to emphasise that humans play an important role in crime prevention.

We will now discuss the 12 techniques in more detail.

*Passwords and PIN codes* are mentioned in all reviews, as these are standard tools. Unfortunately, a good password or PIN code is hard to remember so that as a result passwords and PIN codes that are currently in use are often weak (Anderson, 2008).

*Encryption* is seen by two reviews (Brookson et al., 2007; Morris, 2004b) as a means to harden targets and by the others (Beebe and Rao, 2005; Coles-Kemp and Theoharidou, 2010; Willison and Siponen, 2009; Newman and Clarke, 2003) as a means to deny benefits. The apparent ambiguity can be resolved if we take a crime specific example, such as stealing a laptop with full disk encryption. Disk encryption increases the efforts on the part of the offender because s/he will now have to break the disk encryption. If the offender is unable to break the disk encryption, the laptop will be worth less; hence encryption will also reduce rewards.

Spatial fragmentation is a target-hardening technique that can be used to prevent products from being lost or stolen. For example, an in-car entertainment system that consists of separate components built into various places into a car is harder to steal than a single component (Ekblom, 2008). Spatial fragmentation is more easily applied to a networked system, for example peer to peer systems usually apply spatial fragmentation to improve resilience, but the spatial fragmentation could be leveraged to prevent illegal downloading too. In a sense threshold cryptography is an instance of spatial fragmentation too. In $(n,t)$ threshold cryptography the decryption key is split into $n$ shares in such a way that decryption can only take place when the number of shares present during decryption equals or exceeds a previously determined threshold $t$.

*Firewalls* are mentioned in four reviews (Beebe and Rao, 2005; Brookson et al., 2007; Morris, 2004b; Newman and Clarke, 2003) as a specific technique for target hardening. One review (Coles-Kemp and Theoharidou, 2010) proposes firewalls as a technique for access control and screening exits. Screening exits is an interesting application, as it is as relevant to prevent offenders from getting information out of an organisation as it is to prevent offenders from getting into the organisation in the first place.

A *DMZ* is mentioned by three reviews (Brookson et al., 2007; Beebe and Rao, 2005; Coles-Kemp and Theoharidou, 2010) as a method for target concealment, typically the internal network of an organisation.

An *IDS* is mentioned in five reviews (Morris, 2004b; Brookson et al., 2007; Willison and Siponen, 2009), but in two different ways: as a form of formal surveillance (Coles-Kemp and Theoharidou, 2010; Willison and Siponen, 2009), and as an example of utilising place managers (Brookson et al., 2007). The difference between the two generic techniques is best explained in the physical world: formal surveillance is carried out by specially appointed personnel, whereas place managers could be colleagues watching each other. An IDS can also be used for access control (Coles-Kemp and Theoharidou, 2010), target hardening (Morris, 2004b), and screening exits (Beebe and Rao, 2005).

A *virus scanner* is mentioned as a measure for target hardening (Brookson et al., 2007), and formal surveillance (Morris, 2004b).

*Prompt software patching* is mentioned in four reviews. Software patching is a standard method for target hardening (Beebe and Rao, 2005; Morris, 2004b), but it can be used to discourage imitation (Willison and Siponen, 2009; Coles-Kemp and Theoharidou, 2010), since hackers, who often use each other's exploits, cannot do so if a vulnerability is patched.

*RFID* tags are mentioned in one review (Brookson et al., 2007), but in three different capacities: (1) to extend guardianship to reflect the idea that the tag can be used to raise the alarm in the case of shoplifting; (2) to reduce anonymity since tagged goods can be used to trace the person carrying the goods; (3) to enable formal surveillance, since tagged goods make it easier to recognise shoplifters. RFID tags can be thought of as a technique to identify property. RFID tags can be used for all of the 25 generic techniques.

*Caller-ID* is mentioned in two reviews (Brookson et al., 2007; Morris, 2004b) as an effective technique to control access, reduce anonymity, and to control facilitators. In the real world, caller-ID has reduced the number of nuisance calls in the telephone network (Clarke, 1990). This suggests that a fruitful line of research would be to look for similar, effective techniques for the internet. We have found two relevant papers. The first approach, called IPclip (Widiger et al., 2008), requires hardware support and changes to the way that an ISP operates. The second approach, called Clue (Afanasyev et al., 2011), adds identification information in software. As long as offenders use their own PCs to approach their victim, both IPclip and Clue could be effective. However, since offenders prefer to use hijacked computers rather than their own, the trace from the victim to the offending PC will end at the hijacked PC and not at the offenders PC, thus defeating the objective of the two techniques that have been published thus far.

An *audit trail* is mentioned by several reviews (Beebe and Rao, 2005; Brookson et al., 2007; Coles-Kemp and Theoharidou, 2010; Morris, 2004b; Newman and Clarke, 2003) as a tool to investigate the sequence of events leading up to an incident. An audit trail does not prevent crime per se, but the fact that all actions are logged can be used as a deterrent (Newman and Clarke, 2003).

The *ISP* should be more active in the prevention of crime. This conclusion is shared by all reviews. We have also found suggestions in the related work to empower the ISP. For example some years ago only 5 per cent of all downloads were paid for (Kennedy, 2009), which caused a serious problem for the music industry. Kennedy describes two approaches where the ISP can play a key role. For example, using bandwidth for illegal downloads reduces bandwidth for legal use of the network. A typical ISP would block or throttle bit-torrent traffic, when it is responsible for illegal downloads. This would be an instance of the generic technique of control facilitators. Reducing the potential for illegal downloads automatically increases the available bandwidth for legal use. Whether this is an appropriate solution is open to debate, as bit torrent also has legal uses. There is also a fundamental issue here in the sense that an ISP blockade goes against the principle of net neutrality (van Schewick and Farber, 2009). ISP blocking can even help the offender rather than preventing crime: Clayton (2005) describes how a major

ISP implemented a system for blocking content (child pornography), which leaked the list of blocked sites. The blocking system could then be used by the offenders as an 'oracle' to discover which sites were on the black list, so that they could take evasive action. The main conclusion of Clayton's paper is that a 'fit and forget' approach to designing internet-based crime prevention is doomed to failure; instead the potential targets are engaged in a perpetual arms race with the offenders.

The Morris reports (Morris, 2004a, 2004b) contain suggestions for empowering the ISP. The Morris panels (2004b) would like to see the ISP as a first line of defence (i.e. target hardening) to assist consumers in keeping their computers clean and healthy. The services provided by the ISP can also be seen as a tool for the offender to reach his or her targets. In this sense, making the ISP more accountable for what goes on in its network can be seen as an instance of the control facilitator's generic technique. Finally, the ISP could advertise that it is proactive in preventing crime, and that the ISP will cooperate closely with the police wherever possible. This falls into the generic technique of alert conscience.

*Education* of offenders, targets, and guardians is considered useful by all reviews to remove excuses. Brookson et al. (2007) believe that if we alert their consciences potential offenders might be discouraged from engaging in software and content piracy. In the context of their work on insiders, Willison and Siponen (2009) suggest that the education of staff might assist compliance with company policies. The Morris (2004b) report asserts that customer security education for e-banking, for example using the five 'golden rules' of e-banking, is a specific case of set rules. Finally, using education to control disinhibitors merits a little digression. Before the internet went commercial in the early 1990s some users adhered to the 'hacker's ethic' which held that information should be free (Furnell et al., 1999). When the internet opened for business, new information was made available that is clearly not free. However the hackers' ethic is still with us today, which is a disinhibitor for good behaviour (Newman and Clarke, 2003). Education would be appropriate to explain the difference between information that is free and information that is not.

Having established how useful it is to adopt the systematic approach of crime science to information security, we now turn our attention to the converse, discussing the use of computer science techniques for the study of crime.

## Crime simulation

Science uses computers to collect and analyse experimental and simulated data, using networks to collaborate. For example the high-energy physics community was the first non-military user of the internet and thanks to the computers and networks e-science is flourishing today (Craddock et al., 2008). The development of computational social science follows the lead of natural science. For example Lazer et al. (2009) observe that what we all do in our everyday life leaves traces on the internet, thus providing a source of information that can be mined and analysed. Privacy concerns limit the data available to researchers, but there is hope that these problems can be resolved (Kenneally and Claffy, 2010).

Crime science is a member of the computational social-science family because the analysis of crime data is an important aspect of crime science. However, this is not all. Crime science emphasises that each new idea for the prevention of crime must be properly evaluated, preferably in a well-designed experiment or else in a quasi-experiment or a well-designed time-series analysis. Unfortunately, there are practical limitations to what can be achieved in a real-life experiment.

Firstly, some experiments are just too costly. For example if we believe that changing the street pattern of a city might reduce crime, then it will be hard to convince the

authorities to change the street pattern just for a scientific experiment (Brantingham and Brantingham, 1993).

Secondly, crime data contains systematic errors. Sometimes, neither the offender, nor the target, or the police, have an interest in providing correct data (Gove et al., 1985; Langworthy, 1999; Thornberry and Krohn, 2000). For example, a repeat offender has a vested interest in keeping silent about his crimes, and the police might be interested in inflating the crime rate to ensure that the police force will receive more funding (Eck and Liu, 2008a). It is well known that police recording policies and practices have a strong impact on the officially registered volume of crime, particularly violent crime (Shepherd and Sivarajasingam, 2005; Wittebrood and Junger, 2002).

Computer-based simulated experiments can help to circumvent these problems (Groff and Mazerolle, 2008). For example, in a computer-based experiment we can change the map of a street pattern. We can also use a simulation-based experiment to fill the gaps in available crime data. However, in a computer-based experiment we do not have access to the actors involved, such as the offender, the target, or the capable guardian. Therefore, the behaviour of these actors must be modelled too. Modelling humans is hard, but in the study of crime we are primarily interested in behaviour that is believed to be represented by a number of relatively manageable perspectives, such as rational choice, routine activity, and crime pattern theory. These perspectives can be codified to a certain extent (Bosse et al., 2009b), thus endowing the actors in a simulation with behaviour relevant for a human actor. With a model of the actors and the relevant environment we can use a computer to simulate crime events.

We consider computer-based modelling and analysis of crime as part of crime science. However, the term 'computational criminology' is also being used; it seems to have been employed first by Patricia and Paul Brantingham (2005). We will now discuss the research of the main groups working on crime simulation.

The main idea of crime simulations is to compute the steps leading to a crime event so that predictions about real crime and its prevention can be made. Agent-based simulations are commonly used (Eck and Liu, 2008a), since the behaviour of human actors can be codified by way of rules that determine the behaviour of the agents. The aim of a simulation is then to infer aggregate behaviour from the individual behaviour of crime agents. Epstein (1999) argues that the main reason why this works is that the principle of 'bounded rationality' (which is an aspect of RCP) is also the essence of generative simulation. Quoting Epstein (1999, p. 42): 'Situate an initial population of autonomous heterogeneous agents in a relevant spatial environment; allow them to interact according to simple local rules, and thereby generate – or grow– the macroscopic regularity from the bottom up'. The agents of crime include the offender, the target, and the capable guardian. The simple local rules are provided by the relevant perspective, for example bounded rationality restricts the decision of the offender agent to local knowledge, and ensures that the decision is a rational one taking account of risk. The rules for the offender steer the latter towards a state where the crime has been committed, whereas the target and the guardian try to avoid the crime. The fact that the offender and the target have opposing goals naturally leads to the suggestion that game theory could be a useful meta-theory. The spatial environment could be a geographical environment modelled by a geographical information system (GIS), or it could be a social network. The macroscopic regularity could be a statement such as: 'burglary is communicable', which means that the spreading of burglaries follows the same pattern as a communicable disease (Bowers et al., 2004).

The strength of generative simulation is that it can be used to discount inappropriate theories, since a simulation that does not generate the sought-after macroscopic regularity is probably based on a theory that does not apply (Birks et al., 2012). The limitation of generative

simulation is that there could be more than one theory that can grow the regularity, so generative simulation should not be interpreted as a proof that the theory is the best or only explanation of a certain macroscopic regularity.

Our primary interest is in the ability of generative crime simulation to answer what-if questions. For example, 'what would happen to crime rates if we change the layout of the street pattern?' If the simulation indicates that this would not be useful, then a costly empirical experiment can be avoided. To answer what-if questions we could vary the initial configuration or the rules of the agents. For example, the effect of increasing the number of capable guardians can be studied simply by increasing the number of agents playing the role of a capable guardian. However, in practice, the number of configurations that one can choose from is often huge, so skill and intuition are required to drive the simulations. As yet there is insufficient progress in the field to make simulated what-if experiments routine (Glässer and Vajihollahi, 2008).

Any simulation must ultimately be validated with real data (Berk, 2008). We have not found reports of such validations, presumably for reasons of cost, ethics, and privacy (Lazer et al., 2009).

We have found several strands of work in the literature on the generative simulation of crime. We differentiate related work on the way in which the macroscopic regularity is specified.

- Researchers at the Vrije Universiteit in Amsterdam use a logical approach to the specification of the macroscopic regularity, where a kind of model checking separates simulated behavioural traces that lead to crime from those that do not lead to crime (Bosse et al., 2007a, 2007b; Bosse and Gerritsen, 2008, 2009; Bosse et al., 2009b, 2009a; Bosse et al., 2009b).
- Researchers at Simon Fraser University in Vancouver use an interactive approach towards the detection of the macroscopic regularity, in the sense that successful simulations exhibit for example crime hotspots (Glässer et al., 2006; Glässer and Vajihollahi, 2008; Glässer et al., 2008; Brantingham et al., 2004, 2005). Crime Pattern Theory (Brantingham and Brantingham, 1993, 1995) forms the basis of the simulations; hence the focus is on the spatial and temporal behaviour of the offenders and their targets (Short et al., 2010).
- Researchers at the University of Cincinnati (Eck, 1998; Eck and Liu, 2008b, 2008a; Liu et al., 2005; Wang et al., 2008) and the University of Virginia in Charlottesville (Brown, 1998; Brown et al., 2000; Brown and Gunderson, 2001; Brown and Oxford, 2001; Gunderson and Brown, 2000; Gunderson, 2002; Lin and Brown, 2003, 2006; Porter and Brown, 2007; Xue and Brown, 2003, 2006) use statistical approaches towards the specification of the macroscopic regularity, such as clustering (Brown and Gunderson, 2001), and data association (Brown et al., 2000).

We found one proposal on agent-based simulation of cyber-crime. Gunderson and Brown (2000), from the University of Virginia propose using the same methods and tools that are used successfully to predict traditional crime, without elaborating what the notion of space in the cyber-world might be.

Computational social science is relatively young but has a lot to offer to social science in general and to crime science in particular.

## Conclusions

In conclusion, we found a considerable amount of work in the literature that suggests how crime-science methods can be used by computer scientists and vice versa. We have provided references to relevant related work, but space limitations preclude us from citing more than the tip of the proverbial iceberg.

## Acknowledgements

We are grateful to Ron Clarke, Hans Hendrickx, Ken Pease, Roel Wieringa, and the reviewers for their feedback on drafts of this chapter.

## References

Afanasyev, M., Kohno, T., Ma, J., Murphy, N., Savage, S., Snoeren, A. C., and Voelker, G. M. (2011). Privacy-preserving network forensics. *Communications of the ACM*, *54*(5): 78–87.

Anderson, R. J. (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems*. New York: John Wiley & Sons.

Beebe, N. L. and Rao, V. S. (2005). Using situational crime prevention theory to explain the effectiveness of information systems security. In *Conference on Protecting the Intangible Organizational Assets (SoftWars)*. Las Vegas, NV: The Information Institute.

Berk, R. (2008). How you can tell if the simulations in computational criminology are any good. *Journal of Experimental Criminology*, *4*(3): 289–308.

Birks, D., Townsley, M., and Stewart, A. (2012). Generative explanations of crime: using simulation to test criminological theory. *Criminology*, *50*(1): 221–254.

Bosse, T. and Gerritsen, C. (2008). Agent-based simulation of the spatial dynamics of crime: on the interplay between criminal hot spots and reputation. In *7th International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS)*, pp. 1129–1136. Estoril, Portugal: International Foundation for Autonomous Agents and Multiagent Systems.

Bosse, T. and Gerritsen, C. (2009). Comparing crime prevention strategies by agent-based simulation. In *IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technologies (WI-IAT)*, volume 2, pp. 491–496. Milan, Italy: IEEE.

Bosse, T., Gerritsen, C., and Treur, J. (2007a). Case analysis of criminal behaviour. In *20th International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems (IEA/AIE) – New Trends in Applied Artificial Intelligence*, volume 4570 of *LNCS*, pp. 621–632. Kyoto, Japan: Springer.

Bosse, T., Gerritsen, C., and Treur, J. (2007b). Cognitive and social simulation of criminal behaviour: the intermittent explosive disorder case. In *6th International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS)*, pp. 1–8. Honolulu, HI: ACM.

Bosse, T., Gerritsen, C., Klein, M. C. A., and Weerman, F. M. (2009a). Development and validation of an agent-based simulation model of juvenile delinquency. In *International Conference on Computational Science and Engineering (CSE)*, pp. 200–207. Vancouver, BC: IEEE.

Bosse, T., Gerritsen, C., and Treur, J. (2009b). Towards integration of biological, psychological and social aspects in agent-based simulation of violent offenders. *Simulation*, *85*(10): 635–660.

Bowers, K. J., Johnson, S. D., and Pease, K. (2004). Prospective hot-spotting – the future of crime mapping? *British Journal of Criminology*, *44*(5): 641–658.

Brantingham, P. L. and Brantingham, P. J. (1993). Environment, routine and situation: towards a pattern theory of crime. In Clarke, R. V. and Felson, M. (eds) *Routine Activity and Rational Choice*, volume Advances in Criminological Theory 5, pp. 259–294. Piscataway, NJ: Transaction Publishers.

Brantingham, P. L. and Brantingham, P. J. (1995). Criminality of place: crime generators and crime attractors. *European Journal on Criminal Policy and Research*, *3*(3): 5–26.

Brantingham, P. L., Brantingham, P. J., and Glässer, U. (2004). Computer simulation in criminal justice research. *Criminal Justice Matters*, *58*(1): 18–19.

Brantingham, P. L., Glässer, U., Kinney, B., Singh, K., and Vajihollahi, M. (2005). A computational model for simulating spatial aspects of crime in urban environments. In *International Conference on Systems, Man and Cybernetics*, volume 4, pp. 3667–3674. Waikoloa, HI: IEEE.

Brookson, C., Farrell, G., Mailley, J., Whitehead, S., and Zumerle, D. (2007). ICT product proofing against crime. *ETSI White Paper 5*. Sophia Antipolis, France: European Telecommunications Standards Institute

Brown, D. E. (1998). The regional crime analysis program (ReCAP): a framework for mining data to catch criminals. In *3rd IEEE International Conference on Systems, Man, and Cybernetics (ICSMC)*, pp. 2848–2853. San Diego, CA: IEEE.

Brown, D. E. and Gunderson, L. F. (2001). Using clustering to discover the preferences of computer criminals. *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, *31*(4): 311–318.

Brown, D. E. and Oxford, R. B. (2001). Data mining time series with applications to crime analysis. In *International Conference on Systems, Man and Cybernetics*, volume 3, pp. 1453–1458. Tucson, AZ: IEEE.

Brown, D. E., Gunderson, L. F., and Evans, M. H. (2000). Interactive analysis of computer crimes. *IEEE Computer*, *33*(8): 69–77.

Clarke, R. V. (1990). Deterring obscene phone callers: preliminary results of the New Jersey experience. *Security Journal*, *1*(3): 143–148.

Clayton, R. (2005). Failures in a hybrid content blocking system. In *5th International Workshop on Privacy Enhancing Technologies (PET)*, volume 3856 of LNCS, pp. 78–92. Cavtat, Croatia: Springer.

Coles-Kemp, L. and Theoharidou, M. (2010). Insider threat and information security management. In Probst, C. W., Hunker, J., Gollmann, D., and Bishop, M. (eds) *Insider Threats in Cyber Security*, volume Advances in Information Security 49, pp. 45–71. New York, Dordrecht, Heidelberg, London: Springer.

Craddock, T., Harwood, C. R., Hallinan, J., and Wipat, A. (2008). Opinion: e-science: relieving bottlenecks in large-scale genome analyses. *Nature Reviews Microbiology*, *6*: 948–954.

Eck, J. E. (1998). What do those dots mean? Mapping theories with data. In Weisburd, D. and McEwen, T. (eds) *Crime Mapping and Crime Prevention*, volume Crime Prevention Studies 8, pp. 379–406. Monsey, NY: Criminal Justice Press.

Eck, J. E. and Liu, L. (2008a). Contrasting simulated and empirical experiments in crime prevention. *Journal of Experimental Criminology*, *4*(3): 195–213.

Eck, J. E. and Liu, L. (2008b). Varieties of artificial crime analysis: purpose, structure, and evidence in crime simulations. In Liu, L. and Eck, J. E. (eds) *Artificial Crime Analysis Systems: Using Computer Simulations and Geographic Information Systems*, pp. 413–432. Hershey, PA: Information Science Reference.

Ekblom, P. (2008). Designing products against crime. In Wortley, R. and Mazerolle, L. (eds) *Environmental Criminology and Crime Analysis*, pp. 195–220. Uffculme, UK: Willan Publishing.

Epstein, J. M. (1999). Agent-based computational models and generative social science. *Complexity*, *4*(5): 4160.

Felson, M. and Eckert, M. (2016). *Crime and Everyday Life*, Fifth Edition. London: Sage publishing.

Furnell, S. M., Dowland, P. S., and Sanders, P. W. (1999). Dissecting the hacker manifesto information. *Management & Computer Security*, *7*(2): 69–75.

Glässer, U. and Vajihollahi, M. (2008). Computational modeling of criminal activity. In *1st European Conference on Intelligence and Security Informatics (EuroISI)*, volume 5376 of *LNCS*, pp. 39–50. Esbjerg, Denmark: Springer.

Glässer, U., Rastkar, S., and Vajihollahi, M. (2006). Computational modeling and experimental validation of aviation security procedures. In *International Conference on Intelligence and Security Informatics (ISI)*, volume 3975 of *LNCS*, pp. 420–431. San Diego, CA: IEEE.

Glässer, U., Rastkar, S., and Vajihollahi, M. (2008). Modeling and validation of aviation security. In *Intelligence and Security Informatics*, volume 135 of Studies in Computational Intelligence, pp. 337–355. Berlin: Springer.

Gove, W. R., Hughes, M., and Geerken, M. (1985). Are uniform crime reports a valid indicator of the index crimes – an affirmative answer with minor qualifications. *Criminology*, *23*(3): 451–502.

Groff, E. and Mazerolle, L. (2008). Simulated experiments and their potential role in criminology and criminal justice. *Journal of Experimental Criminology*, *4*(3): 187–193.

Gunderson, L. F. (2002). Using data mining and judgment analysis to construct a predictive model of crime. In *7th International Conference on Systems, Man and Cybernetics*, pp. 246–250. Yasmine Hammamet, Tunisia: IEEE.

Gunderson, L. F. and Brown, D. E. (2000). Using a multi-agent model to predict both physical and cyber criminal activity. In *International Conference on Systems, Man, and Cybernetics*, volume 4, pp. 2338–2343. Nashville, TN: IEEE.

Kenneally, E. E. and Claffy, K. (2010). Dialing privacy and utility: a proposed data-sharing framework to advance internet research. *IEEE Security & Privacy*, *8*(4): 31–39.

Kennedy, J. (2009). Digital music report 2009: new business models for a changing environment. IFPI. www.ifpi.org/content/library/DMR2009.pdf.

Langworthy, R. H. (1999). Measuring what matters: proceedings from the Policing Research Institute meetings. Washington, DC: National Institute of Justice, Office of Community Oriented Policing Services (COPS).

Lazer, D., Pentland, A., Adamic, L., Aral, S., Barabási, A.-L., Brewer, D., Christakis, N., Contractor, N., Fowler, J., Gutmann, M., Jebara, T., King, G., Macy, M., Roy, D., and Alstyne, M. V. (2009). Computational social science. *Science*, *323*(5915): 721–723.

Lin, S. and Brown, D. E. (2003). Criminal incident data association using the OLAP technology. In *First NSF/NIJ Symposium on Intelligence and Security Informatics (ISI)*, volume 2665 of *LNCS*, pp. 13–26. Tucson, AZ: Springer.

Lin, S. and Brown, D. E. (2006). An outlier-based data association method for linking criminal incidents. *Decision Support Systems*, *41*(3): 604–615.

Liu, L., Wang, X., Eck, J. E., and Liang, J. (2005). Simulating crime events and crime patterns in RA/CA model. In Wang, F. (ed.) *Geographic Information Systems and Crime Analysis*, pp. 197–231. London: Idea Group.

Milletary, J. (2013). Technical trends in phishing attacks. Technical publications, United States Computer Emergency Readiness Team (US-CERT). www.us-cert.gov/security-publications/technical-trends-phishing-attacks.

Morris, S. (2004a). The future of netcrime now: Part 1 threats and challenges. Online report 62/04. UK Home Office.

Morris, S. (2004b). The future of netcrime now: Part 2 responses. Online report 63/04. UK Home Office.

NCA (2016). Cyber Crime Assessment 2016. UK National Crime Agency. www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016.

Newman, G. R. and Clarke, R. V. (2003). *Superhighway Robbery: Preventing E-Commerce Crime* (Crime Science). Uffculme, UK: Willan Publishing.

Porter, M. D. and Brown, D. E. (2007). Detecting local regions of change in high-dimensional criminal or terrorist point processes. *Computational Statistics and Data Analysis*, *51*(5): 2753–2768.

Reyns, B. W. (2010). A situational crime prevention approach to cyberstalking victimization: Preventive tactics for internet users and online place managers. *Crime Prevention and Community Safety*, *12*(2): 99–118.

Rosoff, H., Cui, J., and John, R. (2014). Behavioral experiments exploring victims' response to cyber-based financial fraud and identity theft scenario simulations. In *10th Symposium On Usable Privacy and Security (SOUPS)*, pp. 175–186. Menlo Park, CA: USENIX Association.

Shepherd, J. and Sivarajasingam, V. (2005). Injury research explains conflicting violence trends. *Injury Prevention*, *11*(6): 324–325.

Short, M. B., Brantingham, P. J., Bertozzi, A. L., and Tita, G. E. (2010). Dissipation and displacement of hotspots in reaction-diffusion models of crime. *Proceedings of the National Academy of Sciences (PNAS)*, *107*(9): 3961–3965.

Thornberry, T. P. and Krohn, M. D. (2000). The self-report method for measuring delinquency and crime. In Duffee, D. (ed.) *Measurement and Analysis of Crime and Justice*, volume 4, pp. 33–84. Washington, DC: National Institute of Justice.

van Schewick, B. and Farber, D. (2009). Point/counterpoint network neutrality nuances. *Communications of the ACM*, *52*(2): 31–37.

von der Heyde, A., Miebach, J., and Kluge, A. (2014). Counterproductive work behaviour in a simulated production context: an exploratory study with personality traits as predictors of safety-related rule violations. *Journal of Ergonomics*, *4*(2): 1000130.

Wang, X., Liu, L., and Eck, J. E. (2008). Crime simulation using GIS and artificial intelligent agents. In Liu, L. and Eck, J. E. (eds) *Artificial Crime Analysis Systems: Using Computer Simulations and Geographic Information Systems*, pp. 209–225. Hershey, PA: Information Science Reference.

Welsh, B. and Farrington, D. (2008). Effects of improved street lighting on crime. *Campbell Systematic Reviews 13,* The Campbell Collaboration. https://campbellcollaboration.org/library/effects-of-improved-street-lighting-on-crime.

Widiger, H., Kubisch, S., Danielis, P., Schulz, J., Timmermann, D., Bahls, T., and Duchow, D. (2008). IPclip: an architecture to restore trust-by-wire in packet-switched networks. In *33rd IEEE Conference on Local Computer Networks (LCN)*, pp. 312–319. Montréal, QC: IEEE.

Willison, R. and Siponen, M. (2009). Overcoming the insider: reducing employee computer crime through situational crime prevention. *Communications of the ACM*, *52*(9): 133–137.

Wittebrood, K. and Junger, M. (2002). Trends in violent crime: a comparison between police statistics and victimization surveys. *Journal of Social Indicators Research*, *59*(2): 153–173.

Xue, Y. and Brown, D. E. (2003). Decision based spatial analysis of crime. In *First NSF/NIJ Symposium on Intelligence and Security Informatics (ISI)*, volume 2665 of *LNCS*, pp. 153–167. Tucson, AZ: Springer.

Xue, Y. and Brown, D. E. (2006). Spatial analysis with preference specification of latent decision makers for criminal event prediction. *Decision Support Systems*, *41*(3): 560–573.