Cyber-crime Science =
Crime Science + Information Security

Pieter Hartel, Marianne Junger, and Roel Wieringa
University of Twente

Version 0.19, 24th August, 2011

Abstract

Cyber-crime Science is an emerging area of study aiming to prevent cyber-crime by combining security protection techniques from Information Security with empirical research methods used in Crime Science. Information Security research has developed techniques for protecting the confidentiality, integrity, and availability of information assets but is less strong on the empirical study of the effectiveness of these techniques. Crime Science studies the effect of crime prevention techniques empirically in the real world, and proposes improvements to these techniques based on this. Combining both approaches, Cyber-crime Science transfers and further develops Information Security techniques to prevent cyber-crime, and empirically studies the effectiveness of these techniques in the real world. In this paper we review the main contributions of Crime Science as of today, illustrate its application to typical Information Security problems, namely phishing and on-line auction fraud, explore the interdisciplinary structure of Cyber-crime Science, and present an agenda for research in Cyber-crime Science in the form of a set of suggested research questions.

[C.2.0] Computer-communication networks General [Security and protection]

[K.4.1] Computers and society Public Policy Issues [Abuse and crime involving computers]

[K.6.5] Management of computing and information systems Security and Protection

1 Introduction

Crime Science has been developed as a reaction to the difficulty of traditional Criminology in effectively preventing and controlling crime. Criminology intends to explain the "why" of offending and usually investigates the behaviour of adolescents and its roots. Now we know that deeper, longer-term causes of crime cannot easily be changed and therefore, Criminology has had little impact on behaviour and on the prevention of crime [68, 141, 255]. Crime Science, in contrast is interested in explaining the short term causes of offending and the "how" of offending [70]. The focus of Crime Science is on the opportunity for crime. Crime Science relies on multidisciplinary, contextual, and evidence based research, directing towards practical solutions and prevention. This sets it apart from Criminology, which focuses on the criminal, his history, and transgenerational background, and on the long-term causes of criminal behaviour.[1]

In its short history, Crime Science has delivered on its promise of fast and effective scientific approach for the prevention of crime [175, 250, 284]. We can describe Crime Science by means of seven characteristics [250]:

1. In contrast to Criminology, Crime Science studies incidents, not persons. For example, Crime Science investigates when and were burglaries happen and not the personality of burglars or their family or school background. Crime Science does investigate, however, what the short-term motives are of burglars, such as: why an offender chooses a particular dwelling or a particular time to burgle or what to search for;

2. Crime Science in essence is a problem oriented scientific approach, and presents a model for finding ways to prevent concrete mishaps, disorders or crime. Similar contextual approaches exist in the study of accidents in medication [80, 104], in public health [253, 212], and personal safety [138, 214]. Crime Science is therefore outcome oriented, direct, and specific;

3. Crime Science research methods include target surveys, geographical surveys, and case studies that investigate how specific interventions affect crime;

4. Crime Science makes use of a conceptual framework consisting of, amongst others, the Rational Choice

[1] The term Crime Science was coined in the 1990s by the BBC broadcaster Nick Ross. The ten pioneers of Crime Science are Patricia and Paul Brantingham, Ronald Clarke, Paul Ekblom, Marcus Felson, Gloria Laycock, Ken Pease, Nick Ross, Nick Tilley, and Richard Wortley.

Perspective (RCP), the Routine Activity Approach (RAA), and Crime Pattern Theory (CPT) (see Section 3.1 for details);

5. By empirically investigating incidents, Crime Science tries to explain incidents by postulating rules and patterns that have led to these incidents, aspiring to understand how this knowledge can be used to prevent or control crime and disorder;

6. By definition Crime Science is a multidisciplinary field. The aim of Crime Science is to understand and prevent crime by whatever methods necessary, using methods from whatever discipline. For example, Crime Science makes use, amongst others, of knowledge and methods of Geography, Urban Development, Mathematics, Industrial Design, Construction Engineering, Medical Science, Economics, Computer Science, Psychology, Sociology, Criminology, Law, and Public Management;

7. Potential users come from a variety of fields: all professionals active in the field of crime prevention and disorder, such as police officers, policymakers, urban planners, managers, and architects are Crime Science users.

The contribution of this paper is twofold: (1) to add Information Security to the already impressive list of disciplines that support Crime Science, and (2) to add Information Technology (IT) architects to the list of users of the results of Crime Science. Crime Science thus enhanced and used is called Cyber-crime Science in this paper.

To substantiate these contributions we seek to answer two questions:

- Which techniques from Information Security can be used to prevent and detect cyber-crime or crime in general?

- Can the empirical research methods of Crime Science be used to investigate the effectiveness of Information Security techniques?

Perhaps we should explain why we are interested in the effectiveness of Information Security. The reason is that even well intended security policies or mechanisms are ignored or simply too costly to implement. The classical example is the user who is forced to choose a strong password that he cannot remember. As a consequence the user writes the password on a yellow sticky and attaches it to his screen. Another example is given by Herley who estimates that the cost of Phishing is probably dwarfed by the burden on the users who are asked to comply with a variety of advice designed to stop phishing [143]. To make Information Security more effective, economic and human factors must be taken into account [197].

We will analyse the relation between Information Security and prevention of cyber-crime first, and then return to the seven items above to analyse the synthesis of Information Security and Crime Science into Cyber-crime Science.

In our analysis, we make a number of suggestions for future research that we will summarize at the end of this paper in the form of a research programme for Cyber-crime Science.

The plan of the paper is as follows. In Section 2, we introduce and discuss the definitions of the main concepts used in this paper. In Section 3 we review the theory and practise of Crime Science from an Information Security perspective. The last section concludes and sets the research agenda for the area of Cyber-crime Science.

The appendix provides supporting evidence for four basic observations on which the paper is built:

- There is hardly a published application of Crime Science to cyber-crime prevention in Computer Science (Appendix A);

- However, Crime Science can be used fruitfully to take preventive measures for cyber-crime, as illustrated via three case studies in Appendix B;

- The discipline of Information Security, like Crime Science, is supported by other disciplines, such as Economics and Law (Appendix C);

- Computer Science supports Social Science in general and Criminology in particular (Appendix D).

2 Definitions

We start with the definitions of a number of terms used throughout the paper.

Crime. There are two definitions of crime, providing a subjective and an objective view of crime. A subjectivist definition of crime is that it is an act of force or fraud undertaken in pursuit of self interest [128]. This is a subjectivist definition because it includes self-interest in the concept of crime. This is useful if we want to study behaviour that tends to be disapproved of by society because it is morally or legally wrong.

For the purpose of this paper we will however use an objectivist definition from criminal law [243]: A *crime* is behaviour that is commonly considered harmful to individuals and/or society.

Disorder. Crime Science does not limit itself to crime defined in the legal way, but is also interested in disorder. *Disorder* is a broader concept than crime and consists of observable physical and social cues that are commonly perceived to disturb the civil and unencumbered use of public space [220]. This includes crime, but it also includes for example cigarettes on the street, garbage, litter, empty bottles, and graffiti. Examples of social disorder are adults loitering or congregating, people drinking alcohol, and prostitution. Sampson and Raudenbush [220] argue that signs of disorder are commonly perceived as disturbing by all members of the public.

Crime Science. From the work of the ten pioneers of Crime Science, the following definition of Crime Science emerged [175, 213]: *Crime Science* is the application of the methods of Science to the prevention or detection of disorder, and in particular of crime.

Cyber-crime. Newman defines *cyber-crime* as behaviour in which computers or networks are a tool, a target, or a place of criminal activity [206]. This includes the subject of interest of Information Security, namely techniques to prevent or detect attacks on information assets, but it is broader because it also includes such topics as the use of computers to commit "traditional" crime.

It is possible that in the future, cyber-crime will turn out to be nothing special. Something similar has happened before, with the introduction of new technology: The industrial revolution urbanised crime, which the law enforcement of the day was unable to cope with [45]. This eventually led to the introduction of the modern police force. It is possible that the information revolution will have an effect on law enforcement too. However, before cyber-crime is subsumed by the definition of crime, there are some challenges to be met. For example Locard's exchange principle, which is the foundation of Forensics, does not seem to apply to cyber-crime scene investigation [142, Chapter 10].

Information Security. Finally, to complete our set of definitions we will use the following definition from the US Code Title 44 Chapter 35, subchapter III, §3542: *Information Security* is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.

2.1 Analysing the definitions

Based on the definitions of cyber-crime and Information Security above we can see that there is overlap between cyber-crime and Information Security. If a cyber-crime occurs, then, by the definition above, computers or networks must have been used as a tool, a target, or a place of criminal activity. Since the only purpose of computers and networks is the manipulation of information, the occurrence of a cyber-crime is usually related to a breach of Information Security. By a breach of Information Security we understand either breaking a security mechanism or violating a security policy. For example, acts such as cyber-bullying and cyber-stalking would normally be forbidden by the security policy of an Internet Service Provider (ISP), hence we can speak of a breach of Information Security. Cyber-bullying and cyber-stalking are a form of disorder. All common forms of cyber-crime, i.e. cyber-trespass, cyber-deceptions and thefts, cyber-pornography, and cyber-violence [287] typically involve a breach of Information Security.

Despite this overlap between cyber-crime and Information Security, there are also differences. To improve our understanding we will analyse these differences. First, there are cyber-crimes that do not involve a breach of Information Security.

A good example is blue box phone fraud [97], which used to work as follows. First, the offender dials a low tariff local number, then activates the blue box, and finally selects a high tariff long distance number. The call is charged at the low tariff, thus defrauding the telephone company by the difference between the two tariffs. The fraud exploits a fundamental design problem of the phone system of the 1950's, which assumed that callers would never generate signalling information in the voice channel, thus allowing the phone system to carry voice and signalling on the same channel. The current phone systems use out-of-band signalling to render blue boxes inoperative. US Code Title 18, Part I, Chapter 63, §1343 "Fraud by wire, radio, or television" from 1958 imposes a maximum fine of US $ 1,000 on blue box fraud.

One could say that while one discipline supporting Cyber-crime Science (i.e. Information Security) failed to act, another discipline supporting Cyber-crime Science (i.e. the Law) did act. Blue box fraud therefore falls within the broad interpretation of Cyber-crime Science. There are more examples of this kind, but we believe that the innovative character of the example suggests that the blue box category of incidents are eventually subsumed by Information Security. Anticipating this development, we give a broad interpretation to Cyber-crime Science so as to include cases like blue box fraud.

Second, there are breaches of Information Security that are not crimes. For example, suppose that a boss shares his username and password with his secretary so that she can deal with his email during his holidays. In this case the boss has violated a security policy, and has thus breached Information Security. An honest secretary will not misuse the trust placed in her, but even if she does commit minor offenses, the principle of "de minimis non curat lex" (i.e. the law does not deal with trifles) ensures that the legal system ignores those events. In any case, this is a case of mild disorder that falls under the province of Crime Science, and hence, in this example, of Cyber-crime Science.

Returning to cyber-crime that involves a breach of Information Security, we should note that computers and networks themselves can be criminogenic, meaning that they can provide new opportunities for crime, that do not exist without computers or networks, and which Information Security seeks to prevent. Already in 1982, Jay Becker, then head of the US National Centre for computer crime data hypothesised that "Environment, not personality seems the most useful factor in predicting and preventing computer crime" [19]. In the Crime Science literature, the environment that Becker refers to is called the "opportunity structure". We have not found a follow up on Becker's work in literature on Information Security. We believe this to be due to the fact that only now, the state of the art in Crime Science is sufficiently developed to start testing Becker's hypothesis.

Becker's paper [19] is the earliest reference in the Computer Science literature that mentions the word criminogenic. Here we give some examples of more recent papers that focus on the criminogenic properties of computers and networks. Marshall and Tompsett [187] describe how in one major benefit fraud identities were created using aggregators like `http://www.192.com/`. The Internet is replete with identity information, making life easy for the scammers [205]. McCarty [189] describes how "carders" (i.e. offenders that specialise in offenses with credit cards) use Internet Relay Chat (IRC) channels to conduct their illegitimate business. McEwen [191] shows how criminogenic the mobile phone is in the drug trade. The concept of a "burner" is interesting, i.e. a mobile phone that is thrown away after having been used in drug trafficking. Slay and Turnbull [232] describe how in the early days of Wireless Local Area Network (WLAN), people were negligent about security, such that others could use their access point for criminal purposes. The paper reports on cases of WLAN access point owners who got into trouble because of their negligence. Some offenders were caught because they did not think about hiding their actions. Computers and networks thus provide opportunity for crime and Information Security in general seeks to prevent these opportunities.

Summarizing, all breaches of Information Security are examples of crime or disorder and hence examples of cyber-crime in the broad sense. While there are some examples of cyber-crime that do not involve breaches of Information Security such examples are not the focus of this paper. In the rest of this paper, we explore how the synthesis of Information Security research with Crime Science research can enrich both fields.

2.2 Cyber-crime Science

Cyber-crime Science combines the methodology of Crime Science with the technology of Information Security. To clarify what we mean by this, we refine the seven characteristics of Crime Science into the characteristics of Cyber-crime Science, by adding the Information Security perspective.

1. Like Crime Science, Information Security is not interested in the personality of the offender, but is interested in the incidents, such as violated security policies, broken security protocols, hacked web sites, guessed passwords, cloned smart cards etc. In this respect, Cyber-crime Science and Information Security research are similar;

2. Like Crime Science, Information Security is problem-oriented and focuses on ways to prevent concrete incidents (such as hacking a web site). Information Security is "crime" specific. For example, all well designed security protocols make specific assumptions about the power of the attacker and the threat model (i.e. the list of possible attacks that are being considered). By aiming to prevent or detect specific outcomes, Information Security research is outcome-oriented. Here too Cyber-crime Science and Information Security research are similar;

3. However, unlike Crime Science, Information Security research does not normally study the outcome of Information Security breaches empirically. Applying the empirical research methods of Crime Science to study the effects of Information Security techniques in practice should contribute to making the use of these techniques more effective. This is an enrichment of Information Security research that is illustrated by the Case studies of Appendix B;

4. At this moment Information Security research does not have a conceptual framework for criminal or disorderly behaviour like that of Crime Science. We will show in Section 3.1 that the conceptual framework of Crime Science provides useful guidance for Information Security. The Rational Choice Perspective is also fundamental to the Economics of Information Security and Privacy; we will review this fundament in Appendix C.1. There is a role for the Routine Activity Approach [287, 150] and Crime Pattern Theory too, but there is a difference between cyber-crime and traditional crime that has influence on the conceptual framework of Crime Science: the notions of time and space in the physical world are different from those in cyber-space. We believe that further research is needed to refine a number of existing theories to cyber-crime. This is a significant further development, which is part of our research agenda;

5. Unlike Crime Science, Information Security research does not investigate incidents to identify rules and patterns of human behaviour that explain the occurrence of these incidents. Rather, Information Security develops new techniques to prevent and detect security breaches, and investigates the properties of these techniques, aspiring to understand how they work in practice and how they can be improved

further. This can enrich the proposals to prevent cyber-crime based on empirical research of incidents in Crime Science;

6. Like Crime Science, Information Security is a multidisciplinary field. Information Security is intimately related to Mathematics, but also Physics [26], Law [240], Economics [11], and Psychology [223]. Our proposed discipline of Cyber-crime Science relates Crime Science to Information Security. As far as we can see, Information Security does not link to Geography, which is an area of future research;

7. Like Crime Science, potential users of Information Security come from a variety of fields, such as the security industry, the police, governments, and businesses.

Summarising, Cyber-crime Science and Information Security research can mutually enrich each other in the area of Cyber-crime Science.

An appropriate framework for this is the schema of empirical evaluation research presented by Pawson and Tilley [211]:

Context and Treatment causes Outcome.

- The context is the environment in which opportunities for crime exist;
- The treatment consists of the application of techniques aiming to prevent crime;
- The outcome is the result of applying the treatment in a specific, concrete context.

In the approach by Pawson and Tilley, empirical investigation of outcomes in Crime Science is done by case studies. The aim of these studies is to understand the specific mechanisms that in this concrete case have caused the treatment, which in this context to lead to this outcome. The ambition is to find generalisable, reusable knowledge by identifying generic mechanisms that can be predicted to occur in other cases too.

In Cyber-crime Science, this approach is combined with the approach of Information Security research to develop treatments, i.e. techniques to prevent or detect Information Security breaches. Cyber-crime Science studies the effect of these treatments in concrete cases using the research methods and conceptual framework of Crime Science and proposes improvements to these treatments based on the insights gained by this research.

3 Crime Science from an Information Security perspective

The components of Crime Science are:

1. A conceptual framework;
2. A set of opportunity-reducing techniques;
3. Knowledge about a body of evaluated practice;
4. Studies of displacement of crime and diffusion of benefits.

We summarize the prominent aspects of each of these in the following four sections, using examples from Information Security where possible.

3.1 Conceptual framework

Crime Science researchers have developed a conceptual framework that consists of three perspectives on the crime incident. These three perspectives operate at different levels, which, following Felson and Clarke [103], we will present top down:

- The Routine Activity Approach operates at the level of society or an organisation. The main question is how to discover and prevent opportunities for crime in the routine activities of potential offenders;
- Crime Pattern Theory operates at the level of everyday life of an individual offender, and his location. The main question is how to discover and prevent opportunities for crime in the daily commute and other patterns of movement of potential offenders;
- The Rational Choice Perspective operates at the level of a specific crime opportunity, focusing on the cost benefit tradeoffs presented by the opportunity. The main question is to measure and influence the cost benefit tradeoffs that underlie crime.

The three perspectives can be used to understand and explain opportunity for crime at each of these levels, and they can be used to design preventive measures that reduce this opportunity. We discuss the three perspectives in the next three sections, followed by a discussion of a closely related issue: Repeat Victimization.

3.1.1 Routine Activity Approach

The first perspective is RAA [75], which states that the opportunity for crime is likely to present itself during routine activities, when (1) a potential offender meets (2) a suitable target in the absence of (3) a capable guardian. We will discuss each of these three actors below, starting with the potential offender.

A potential offender is the main actor of crime. Some individuals in modern society are potential offenders [72, 128, 254]. For example when there is little supervision or likelihood of detection, people are vulnerable to temptations [102]. An important reason for Crime Science to stress prevention is that the reservoir of potential offenders is virtually unlimited.

An insider is privy to more information than an outsider and has thus better opportunities to commit a crime. The Information Security literature offerers several studies on insider threats, dating back to Dorothy Denning's seminal paper [84]. The idea of separating offenders into a more powerful class of insiders and a less powerful class of outsiders is in principle attractive, as one can focus effort on the class of offenders that are considered to pose the highest risk. Once the two classes of offenders are separated, one may try to refine the class of insiders into subclasses. For example Wood [283] theorises about certain characteristics of insiders, but without any empirical evidence, and Theoharidou et al [248] examine various social and criminological theories, including those discussed here, as a basis for containing the insider threat. Neumann [204] provides an older but still valid overview of the challenges of preventing insider attacks. Finally Caputo et al [57] describe an experiment in the spirit of Crime Science where in a randomized controlled trial the difference between benign and malicious insiders is studied.

Willison explores in a series of papers how Crime Science can be applied to computer assisted insider fraud. His first paper [276] describes the actions of Nick Leeson that lead to the collapse of Barings bank. The main conclusion is that lack of a capable guardian contributed to the collapse of the bank. A series of three papers [278, 279, 277] propose to perform risk assessment of information systems from the perspective of the insider/offender (instead of the more common perspective of the target). The papers do not offer an empirical validation of the idea. A series of two papers [280, 231] (and a paper by other authors [181]) frame software piracy in terms of a number of criminological theories (such as Differential Association Theory, and Neutralization Theory) that focus on the offender, thus falling beyond the scope of the present paper. The seventh paper [278] argues that situational crime prevention is more effective when the target and the offender share a common situation. For example if the offender and target are both employees of one organisation then a variety of instruments are available to the management of that organisation. Willison provides an example of a crime script for a typical insider fraud case such as that committed by Leeson. The last paper by Willison (with Siponen) [281] is a synthesis of earlier work.

We believe that the notion of an "insider" is becoming less and less useful for the simple reason that the boundaries that used to separate insiders from outsiders are gradually disappearing. We give three examples. First, organisations outsource a growing part of their business (for example sales and HRM). Second, organisations form strategic alliances with other organisations, such that employees from one organisation must have access to information from another. Third, cloud computing relieves an organisation of the need to look after its IT assets; instead the employees of the Cloud Service Provider (CSP) take charge. In the end the information that used to be accessible to the employees of one organisation is now accessible to a number of other organisations as well, thus turning more and more people into various degrees of "insider".

However, can we jettison the concept of the insider just like that? Again Crime Science comes to the rescue, in the person of Marcus Felson who proposed the concept of "specialised access" [102] to characterise the specific opportunity structure of white collar crime. Specialized access captures the difference between the opportunity that an employee of an organisation, or its strategic partners, or its oursourcees, or its CSP have as compared to any one else. A network of organisations is usually governed by a set of Service Level Agreement (SLA), which can be used as the legal basis needed to operationalise specialised access. What is missing is a technical notion of specialized access, which leads to the following suggestion for future research:

Question 1 *What is the merit of framing the insider problem as a problem of specialised access?*

A suitable target is something that might appeal to an offender [101]. Bread is rarely stolen in affluent countries, but cash is the "mother's milk" of crime in any country. Crime Scientists often describe suitable targets using checklists. For example Concealable, Removable, Available, Valuable, Enjoyable, and Disposable (CRAVED) is a simple to use checklist to determine which products might become hot [67]. The mobile phone is a perfect example of a CRAVED product [79], and so is the laptop [166]. Information (e.g. credit card data) can also be described in terms of CRAVED [207, Chapter 4].

Some targets, like marked car parts are unattractive to thieves because of the difficulty of fencing such parts. However, property marking schemes incur a certain cost, which depending on the popularity of the target may be hard to justify. Interestingly, information technology makes it possible to "mark" property even after it has been lost or stolen, thus avoiding the up front cost for property marking. For example a mobile phone can be disabled via the network, once it has been stolen [273]. Similarly, a laptop or mobile phone can be fitted with remote wipe technology [237], which allows the owner to erase the data on the device via the Internet. To an offender who is interested in the data, for example in the case of industrial espionage, remote wipe technology thus has the capability of reducing the suitability of the target. We have been unable to find studies that investigate the effect of remote wipe technology on the likelihood of theft of equipment fitted with that technology, thus leading to the following suggestion for future research:

Question 2 *What manipulations of stolen digital goods would be effective in deterring potential attackers of these assets?*

Routine Activity does not distinguish between different types of target. We have given some examples of property targets but targets can be personal too [75]. For example the victim of cyber-bullying is a personal target. Often the person standing between the offender and a property target becomes a personal target. Stajano and Wilson give a detailed account of classical scams showing how even vigilant people can become personal targets [235].

A capable guardian can be an effective deterrent for an offender, for example a security guard patrolling an underground station. The classical example of what happened when capable guardians were absent is the rise in day time residential burglaries in the US in the 1960s. This can be explained by considering that in the 1960s more and more women joined the labour force, leaving homes empty where previously they were occupied during daytime [75].

Deciding who could play the role of guardian in various forms of cyber-crime is not an easy question. For example, in the case of cyber-bullying, parents could monitor the Internet usage of their children, but this is more easily said than done [195]. Chua et al [64] suggest that the vigilantes in on-line auction communities such as eBay, who try to sabotage auctions of suspicious sellers, could be considered capable guardians. However, auction sites generally do not approve of the activities of the vigilantes, because it is undesirable that people take the law in their own hands [153].

Whether RAA works as well for cyber-crime as for traditional crime is an open question. On the one hand, Yar [287] suggests that in general the ideas apply, but that the differences between the Internet and the real world are significant, in particular there does not seem to be a useful notion of place on the Internet. We consider four possible alternatives for a notion of place, but this is by no means an exhaustive list:

Firstly, low level candidates such as the Media Access Control (MAC) address or the Internet Protocol (IP) address of a computer are probably not useful as location since both can be changed easily, for example using the Dynamic Host Configuration Protocol (DHCP).

Secondly, geographically based notions of place, such as the address of the ISP, the mobile base station of a mobile phone, or the wireless access point that an increasing number of Internet users go through might be useful. However it is normally not possible to retrieve such information without the cooperation of the relevant service provider. Such cooperation usually requires a court order, because the service provider naturally would try to protect the interests of its customers.

Thirdly, the Internet is a network that exhibits a certain structure that can in principle be exploited. For example the computers on the Internet as well as the World Wide Web form a clique [6], just like an Online Social Network (OSN). In an OSN a clique is a circle of friends or acquaintances from which offenders often choose their targets. Whether or not cliques play a similar role in cyber-crime is as yet unexplored.

Finally, Newman and Clarke [207] suggest focusing on a semantic notion of place, an example of which is provided by Holt and Bossler [150]. They report on an empirical test designed to explore the applicability of RAA to a specific form of cyber-crime: On-line harassment. A survey amongst 788 college students found that spending of time on the Internet does not necessarily increases the risk of victimization, unless time is spent in virtual meeting places such as chat rooms, where suitable targets are in contact with potential offenders. This suggests that virtual meeting places represent a suitable notion of place in the context of a particular form of on-line harassment.

It is possible to create a semantic notion of place on the Internet. Collaborative work systems typically do this to foster cooperation between workers but there are also systems that focus just on giving the illusion of physical presence, such as WebRogue [234]. This is a browser add-on that shows the visitor of a web page who else is visiting the same web page. Visitors may then choose to communicate via a chat system with another visitor, to give the illusion of physical presence. We have not found studies on the role that collaborative work systems or the more specialised systems such as WebRogue may play in cyber-crime, but see this as a fruitful avenue for further research.

Summarising, according to RAA, cyber-crime needs a potential offender, a suitable target, and the absence of a capable guardian. This suggests future research as follows:

Question 3 *How to measure and control proximity in the cyber-physical world?*

3.1.2 Crime Pattern Theory

CPT [37] assumes that offenders find opportunities for crime during the daily journey between home, work, and leisure. As a result, usually crime occurs in specific patterns and usually crime is concentrated at particular places, and at particular times, i.e. hotspots. Knowledge of such hotspots can be used to protect potential victims, since if we can predict where the hotspots are, and who is likely to be victimized, we can target the efforts of crime prevention more precisely and effectively [36]. For example town planners can use maps showing the incidence of crime to change street plans [38], and police resources can be deployed more effectively [34].

Traditional crime is generally serial crime because physical constraints make it difficult to commit more than one crime at once [45]. This means that normally a time and a geographical location can be associated with traditional crime, and that there is a one to one relationship between offender and target. Sometimes, the time or location of a crime is not accurately known. For example a burglary is usually discovered some time after it has taken place [4], but the location is accurately defined. With obscene phone calls, time is not normally the problem but location: the caller could make his calls from anywhere [65].

By contrast, the notion of time (and location as explained above) in cyber-space is not well understood, and as a result there is no general notion of a cyber-crime hotspot. The only exception that we have found is formed by the chat rooms that are frequented by cyber-stalkers. This unfortunate situation is caused by the fact that computers and networks can automate aspects of human activity, including crime.

Leveraging the Internet, it is possible to commit several crimes at once at different places in the world. For example an offender can instruct thousands of computers in a collection of computers programmed to attack on a massive scale (BotNet) to attack web sites all over the world at the same time. One might argue that the Internet consists of interconnected computers, where hotspots in the sense of busy computers naturally arise, simply because some computers have more connections than others. However, we have not found any research investigating the activity of cyber-criminals on Internet hotspots.

If the offender can leverage the power of the Internet, then crime prevention should be able to do so too. We give two examples.

Firstly, there are various services trawling the Internet for credentials such as credit cards (for example `http://www.cardcops.com/` [108]), so that anyone concerned that his credit card may be stolen can consult a web site to check.

Secondly, all activity on the Internet leaves traces that can in principle be mined, like regular audit trails [259]. It is probably harder to collect traces in the real world than on the Internet, thus creating an advantage for cyber-crime prevention over traditional crime prevention.

However, collecting information that could eventually be used to prevent or detect cyber-crime would have privacy implications that will have to be dealt with appropriately. For example, one promising line of research allows the privacy of the persons to be revoked under well defined circumstances [147]. By way of conclusion we suggest for future research:

Question 4 *How can we monitor activity on the Internet to identify hotspots and still respect privacy?*

3.1.3 Rational Choice Perspective

RCP of human action is used in Economics [230], Psychology [256], and Sociology [76], but the roots are in the work of utilitarian philosophers such as Bentham and John Stuart Mill. It was adapted to the explanation of crime by Cornish and Clarke [79]. RCP says that behaviour is governed by its expected consequences. Translated to crime, this means that potential offenders make a judgment, weigh the costs and benefits, and commit a specific crime when the estimated benefits are greater than the costs. The choices are often based on bounded rationality, because human actors have limited knowledge, are limited in their ability to reason about all the possible consequences of an action, and are subject to the constraints of a given context (e.g. being drunk). Accordingly, a RCP of crime does not mean that offenders act wisely or are pursuing choices that are rational or beneficial in the long term. It means that, often quickly and under pressure, offenders attempt to decide, using their bounded rationality, how to act to maximize their profits, and to minimize their risks. They use the "fast and frugal heuristics" [117]. For example, burglars choose unoccupied houses, which have relatively easy access (the first or the last in a row), and which allow the offender to remain hidden [82]. Burglars are often more preoccupied by minimizing risk rather than increasing the rewards [82].

RCP has already provided guidance to researchers of Information Security researchers. We have discussed the work of Willison in Section 3.1.1, and we should also like to mention some case studies. For example Aytes and Connolly [16] present a survey of 167 college graduates showing that risky behaviour, such as sharing passwords, or opening suspect emails is a rational choice. Higgins [145] presents a survey of 318 college students showing that low self control, which is a factor that influences the rational choice people make, is linked to software piracy.

RCP has been applied in simulation by Social Scientists [98] and more specifically in crime simulations [186] (see Appendix D for details) as well as the study of the Economics of Information Security (see Appendix C.1 for details). While these are promising results, there is scope for more research into RCP on cyber-crime.

Summarising, RCP hypothesises that like traditional offenders, cyber-crime actors operate under bounded rationality too. This suggests the following topic for future research:

Question 5 *Which cost/benefit tradeoffs do cyber-criminals actually make?*

3.1.4 Repeat Victimization

Some criminals target the same victim repeatedly, which is referred to as Repeat Victimization [99]. For example, in the 1992 British crime Survey, 63% of all property crime was suffered by people who had already suffered a property crime recently, and 77% of all personal crime was suffered by people who had already suffered a recent personal crime. Burglarized houses are often victimized twice at relatively short intervals [34]. Repeat Victimization is not a perspective in the same sense as RCP, RAA, and CPT, but it is an important result from crime analysis. Repeat Victimization probably also applies to cyber-crime, but reports are inconclusive. For example, thieves know that companies are likely to replace stolen laptops so they will come back to take the replacements [166]. Templeton and Kirkman [246] give accounts of how vulnerable the elderly are of Repeat Victimization, where the Internet and email used as a tool by the offenders. We believe that it should be possible to use the Internet also as a tool to detect Repeat Victimization and suggest:

Question 6 *What is the extent and nature of repeat victimization in cyber-crime?*

3.2 Reducing the opportunity for crime

Based on the conceptual framework described above, Crime Scientists have developed a number of principles that – if applied correctly – should make prevention more effective.

Two points need to be mentioned, before explaining these principles. First, Crime Science studies up to now have shown that one needs to be specific in terms of incident context and goals of stakeholders to understand precisely why specific crimes are committed and accordingly, how they can be prevented. For example marking car parts may discourage a thief trying to sell the parts, but it will not be effective against joyriding, because this is an incident with a different context and different actor goals. Second, the principles, and more specifically, the different techniques should be considered as work in progress [70]. As research progresses and our knowledge of crime prevention increases, the principles and the techniques may increase in number, for example to deal with cyber-crime more effectively.

3.2.1 The 5 principles of opportunity reduction

The five principles try to prevent the crime or to deter the offender. The first three principles are economic in nature, the last two are psychological:

i Increase the effort of crime, for example better locks require more effort to pick, or better passwords require more effort to guess;

ii 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;

iii Reduce the rewards of crime, for example marked parts of a stolen vehicle are harder to fence, or encrypted data is harder to sell;

iv Reduce provocations that invite criminal behaviour, for example rapid cleaning of graffiti discourages the application of more graffiti, or rapid restoration of defaced web sites discourages repetition;

v Remove excuses for criminal behaviour. For example Bateson et al [18], claim that a sign asking people to pay for a service is more effective when a pair of eyes is printed on the sign, as opposed to a bunch of flowers. Other researchers have cast some doubt about the methodological validity of this particular experiment [58]. Eyes have also been used as cues of being watched in privacy controls [222].

For each of the five principles, five generic opportunity-reducing techniques have been developed. Together, they are known as the “25 opportunity reducing techniques”. Table 1 taken from Cornish and Clarke [78] has one column for each of the five principles (numbered i . . . v), and shows five generic techniques in each column (numbered 1 . . . 5 in the first column, 6 . . . 10 in the second column etc), with an example from a specific technique that has been proved to be effective against traditional crime [135]. There is no relation between the items in a row in the table; hence the rows have not been numbered. In principle the items within each column could be presented in a different order.

The 25 generic opportunity reducing techniques cannot be applied directly. A specific instance of the 25 generic techniques must be found that is appropriate in the context of a specific crime, given the goals of specific actors. Consider as an example the generic technique of target hardening for principle i. If the target is a car and the crime is joy riding, then a specific technique would be “implement steering column locks” (See cell **1**). Case studies have proven steering column locks to be successful [188]. Other techniques could also be effective, for example the general technique of conceal targets (See cell **11**) for principle iii can be achieved by implementing the specific technique of “off-street parking”. If the right technique is applied, the results can be significant, as demonstrated by case studies [66]. In these case studies cyber-crimes are not represented yet. However, in the next section we will show that based on our literature review, the 25 generic techniques are in principle as applicable to the prevention of cyber-crime as they are to traditional crime.

Economical cost and balance			Psychological cost and balance	
i. Increase effort	ii. Increase Risks	iii. Reduce Rewards	iv. Reduce Provocation	v. Remove Excuses
1.Harden target Steering column locks and immobilisers	**6.Extend guardianship** Take routine precautions: go out in group at night, leave signs of occupancy, carry phone	**11.Conceal Targets** Off-street parking	**16.Reduce frustrations** Efficient queues and polite service	**21.Set rules** Rental agreements
2.Control access Entry phones	**7.Natural surveillance** Improved street lighting	**12.Remove Targets** Removable car radio	**17.Avoid disputes** Separate enclosures for rival soccer fans	**22.Post instructions** “No Parking”
3.Screen exits Ticket needed for exit	**8.Reduce anonymity** Taxi driver IDs	**13.Identify property** Property marking	**18.Reduce arousal** Controls on violent pornography	**23.Alert conscience** Roadside speed display boards
4.Deflect offenders Street closures	**9.Place Managers** CCTV for double-deck buses	**14.Disrupt markets** Monitor pawn shops	**19.Neutralize peer pressure** “Idiots drink and drive”	**24.Assist compliance** Easy library checkout
5.Control facilitators “Smart” guns	**10.Formal surveillance** Red light cameras	**15.Deny benefits** Ink merchandise tags	**20.Discourage imitation** Rapid repair of vandalism	**25.Control disinhibitors** Breathalyzers in pubs

Table 1: The 25 Generic opportunity reducing techniques used to prevent traditional crime, with an example of a crime specific technique for each of the 25. See also `http://www.popcenter.org/25techniques/`

3.2.2 The 25 opportunity reducing techniques

We have found eight recent reviews in the literature that suggest how Information Security tools can be used as a specific instance of the 25 generic techniques [21, 48, 77, 202, 207, 281, 217, 272].

We will discuss each review briefly, followed by a comparison of the salient recommendations offered by all but the last review, which focuses on a specific technology, a Radio Frequency IDentification (RFID) tag, thus making it unsuitable for the comparison.

The first review by Beebe and Rao [21] associates 44 commonly used Information Security techniques with the 25 generic techniques (actually a predecessor to the 25 generic techniques which consisted of only 16 techniques). It is unclear why these particular 44 techniques have been selected, and the association is not motivated. This raises the question whether other associations could also be justified. Beebe and Rao then count how many Information Security techniques are associated with each of the five principles and observe that more than half associate with principle i. Beebe and Rao then conclude that it would be useful to search for more Information Security techniques that can be associated with the other principles, as these seem under-populated. While we agree that searching for more Information Security techniques to prevent crime is worthwhile, we are not sure that principles ii-v are indeed under-populated, as other mappings would be equally plausible. We will give examples of techniques for principles ii-v below.

Reviews two to six [48, 77, 202, 207, 281] associate specific Information Security techniques with the 25 generic techniques, but do so in a more or less crime specific setting, thus making association well motivated. Brookson et al [48] present their association in the context of fixed and mobile phone fraud, Broadcast and Pay TV fraud, Hacking on the Internet, and misuse of WLAN and Bluetooth networks. Coles-Kemp and Theoharidou [77] analyse how a number of common criminological theories apply to the insider threat on Information Security. Newman and Clarke [207] choose the setting of electronic commerce, and Willison and Siponen [281] present an association in the setting of embezzlement. Morris [202] reports how a panel of about 50 experts proposes to deal with money laundering, fraud, extortion, espionage, malicious software, malicious misinformation, and unlawful markets and communities.

The seventh review by Reyns [217] is most crime specific, as it focuses on cyber-stalking. The review analyses 10 surveys of stalking, showing that in about 25% of the cases, the Internet in one form or another plays a role. Using the structure of the 25 techniques, Reyns suggests a number of ways to make cyber-stalking more difficult, but he has not actually implemented any of his suggestions.

The last review [272] describes the potential for crime prevention with an RFID tag, ranging from inexpensive chip-less tags [17] to high-end tags. The review shows that a specific technique (in this case the RFID) fits in all of the 25 generic techniques. To illustrate the point, the review contains a short case study of Tesco's supermarket in Cambridge where RFID tags are used to protect packets of razor blades. If a packet is taken from the shelf, a security camera starts recording the customer. The customer is again recorded when paying at the checkout. When there is no recording of a paying customer, the recording of the customer taking the blades is handed over to the police.

The complete list of the specific techniques from the eight review papers can be found in Appendix E. Here we provide a summary (see Table 2) comparing the way in which the first seven reviews suggest how prominent Information Security techniques can be used to prevent crime. We define prominent Information Security techniques as those which have been mentioned at least three times in the reviews; there are 12 such prominent Information Security techniques:

1. A password or pin code used to authenticate a user;
2. Encryption of data to ensure that once encrypted, data 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;
4. A De-Militarized 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. An RFID tag used to provide information about the product to which it is attached;
9. The Caller-ID feature of the Phone 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 ISP used to assist its clients in using the information super highway responsibly;
12. User education, which is included in the list to show that we interpret Information Security in a broad sense.

Economical cost and balance			Psychological cost and balance	
i. Increase effort	ii. Increase Risks	iii. Reduce Rewards	iv. Reduce Provocation	v. Remove Excuses
Firewalls	RFID	DMZ	–	Educate end-users
1.Harden target Authentication using passwords, pins	**6.Extend guardianship** Report suspect email and information request to ISP	**11.Conceal Targets** –	**16.Reduce frustrations** –	**21.Set rules** –
2.Control access IDS	**7.Natural surveillance** RFID	**12.Remove Targets** RFID	**17.Avoid disputes** –	**22.Post instructions** Public awareness on the consequences of crime
3.Screen exits	**8.Reduce anonymity**	**13.Identify property**	**18.Reduce arousal**	**23.Alert conscience**
4.Deflect offenders –	**9.Place Managers** IDS	**14.Disrupt markets** ISP should be keen to assist investigations	**19.Neutralize peer pressure** –	**24.Assist compliance** Security education of staff
5.Control facilitators Caller ID	**10.Formal surveillance** Auditing and trail reviews	**15.Deny benefits** Encrypt valuable data	**20.Discourage imitation** Prompt software patching	**25.Control disinhibitors** Cyber-ethics education

Table 2: Prominent examples of the 25 Generic techiques used to structure popular Information Security techniques.

We will now discuss the 12 techniques in more detail.

Passwords and pin codes are mentioned in all reviews, as these are standard tools of Information Security. 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 sometimes weak [9].

Encryption is seen by two reviews [48, 202] as a means to harden targets and by the others [21, 77, 281, 207] 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 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 [96]. Spatial fragmentation is more easily applied to a networked system, for example peer to peer systems usually apply spatial fragmentation for load balancing purposes, 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 [21, 48, 202, 207] as a specific technique for target hardening. One review [77] 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 [48, 21, 77] as a method for target concealment, typically the internal network of an organisation.

An IDS is mentioned in five reviews [202, 48, 281], but in different ways: formal surveillance [77, 281], and utilize place managers [48]. 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 are typically colleagues watching each other. An IDS can also be used for access control [77], Target hardening [202], and Screening exits [21].

A Virus scanner is mentioned as a measure for target hardening [48], and formal surveillance [202]. Screening exits is also mentioned [21], but it is unclear why.

Prompt software patching is mentioned in four reviews. Software patching is a standard method for target hardening [21, 202], but it can be used to discourage imitation [281, 77], since hackers, who often use each others exploits, cannot do so if a vulnerability is patched.

RFID tags are mentioned only by Brookson et al [48], but in four different capacities: extend guardianship to reflect the idea that the tag can be used to raise the alarm in the case of shoplifting, reduce anonymity since tagged goods can be used to trace the person carrying the goods, and formal surveillance, since tagged goods make it easier to recognise shoplifters. RFID tags can be thought of as a technique to identify property. A separate study [272] shows that RFID tags can be used for all of the 25 generic techniques.

Caller-ID is mentioned in two reviews [48, 202] 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 [65]. 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 [274], requires hardware support and changes to the way that an ISP operates. The second approach, called Clue [5], 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 hijacks 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 [21, 48, 77, 202, 207] 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 [207].

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 Kennedy [164] claims that only 5% of all downloads are paid for, which causes a problem for the music industry. Kennedy describes two approaches where the ISP can play a key role. The first approach consists of introducing new business models such as Nokia's "Comes with Music", which gives the customer who buys a handset a years worth of free music. The catch is that included in the price of the handset is a fee for the music. The customer can keep the music, also after the contract has expired. This can be seen as an attempt by the ISP to reduce the rewards for illegal downloading. The second approach is to observe that usign 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 [262]. ISP blocking can even help the offender rather than preventing crime: Clayton [74] describes how a major ISP implemented a system for blocking content (child pornography), which readily 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 base crime prevention is doomed to failure; instead the potential targets are engaged in a perpetual arms race with the offenders.

The Morris reports [201, 202] contain suggestions for empowering the ISP. The panels would like to see the ISP as a first line of defence (i.e. target hardening) so as to assist the consumer in her task of keeping her computer clean and healthy. The services provided by the ISP can also be seen as a tool for the offender to reach his 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 facilitators 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. We believe that it would be a interesting to investigate:

Question 7 *What roles can ISPs have in preventing cyber-crime, and what is the effectiveness of these roles?*

Education of offenders, targets, and guardians is considered useful by all reviews to remove excuses. Brookson et al [48] believe that if we alert conscience potential offenders might be discouraged from engaging in software and content piracy. In the context of his work on insiders, Willison [281] suggests that the education of staff might assist compliance with company policies. The panel of Morris [202] 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 early nineties some users adhered to the "hacker's ethic" which promoted that information should be free [109]. 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 [207]. Education would be appropriate to explain the difference between information that is free and information that is not.

Table 2 offers one suggestion to reduce provocation and only three suggestions to reduce rewards. This does not mean to say that there are no Information Security techniques that can be applied for these principles; it just means that the reviews have given such means emphasis, or more likely, that researchers in the Computer Science community do not think of their work as a means to reduce provocation, or to reduce rewards.

There are Computer Science techniques that fit perfectly in the scheme of the 25 generic techniques, but which have not been mentioned by the eight review papers. For example:

Control facilitators is the technique implemented by modern colour copiers that refuse to copy a bank note [162].

Deny benefits by personalisation is not considered by any of the reviews but we have found suggestions in the Crime Science literature that this could work [96]. For example the buyer of a new car can choose from a range of options how to personalise the car, not only by the engine and body identification systems but also by colour schemes, choice of upholstery, accessories etc. It is not unreasonable to expect product personalisation to be applicable to less expensive products as well, such as the mobile phone, the computer, music, film or software. Once personalised and sold, it would be possible to trace the movements of a personalised product when it is lost or stolen, thus denying benefits to the offender.

Control disinhibitors plays a role in traditional crime, which is often fuelled by drugs and alcohol. However, little is known about Internet addiction. The first reference to Internet addiction that we have been able to trace is Young [289], who argues that Internet addiction is a behavioural disorder like pathological gambling. Internet addition can be serious; in the press there are reports of fatalities, and reports of deviant behaviour promulgated by Internet addiction [132] have appeared in the literature too.

Privacy Enhancing Technologies try to help online users to reduce the amount of private information divulged on the Internet, and thus to limit their exposure to malicious activity. For example Atkinson et al [13] propose a browser plug-in that records where the user has disclosed personal information. Goecks et al [123] show how recommendations by others can help users make the right decisions about privacy and security settings.

Summarising, it appears that the techniques from Information Security help to prevent cyber-crime. This leads to the following suggestion for future research:

Question 8 *Which of the 25 opportunity-reducing techniques is effective in preventing which class of cyber-*

crime?

3.3 A body of evaluated practice

There are studies that report on the effectiveness of Crime Science for traditional crime; Guerette and Bowers [135] provide a starting point. However, for Cyber-crime Science only a few relevant studies exist. We substantiate this claim in Appendix A.

3.4 Displacement of crime and diffusion of benefits

A difficult aspect of reducing the opportunity for crime is to make sure that there is a real reduction and not simply displacement. In some case studies, displacement of crime can be ruled out. The classic example is the detoxification of gas used in British households. Coal based gas, which contains a fraction of toxic Carbon Monoxide (CO), was the method of choice to commit suicide. When natural gas replaced coal based gas the total number of suicides (i.e. regardless of the method by which the suicide was committed) dropped [71]. An example that does apply to crime is the alley-gating scheme that was implemented in Liverpool (UK) to prevent burglary [35]. The scheme involved the installation of lockable gates across these alleys preventing access to the alley for those without a key. An evaluation showed that there was a reduction of burglaries within the alley-gated areas. Also, the initiative had not caused geographical displacement of burglary. On the contrary: there was evidence of a “diffusion of benefit”, whereby, burglary not only reduced within the gated areas but also fell by 10% in several 200m buffer zones surrounding the gated areas [36]. Another example is the installation of Closed Circuit Television (CCTV) in certain London Underground stations but not in all, the level of crime, in contrast, dropped in all stations [73]. It is assumed that when offenders notice crime prevention they become more alerted to the risk of crime generally, and not just in situations were crime preventions measures were taken [69].

A review of the literature found 102 studies that contained 574 observations reporting displacement of crime in 26% of the observations, and diffusion of benefits in 27% of the observations [135]. Overall, the effect of diffusion of benefits was larger than the effect of displacement of crime and the total results were larger than the results in the experimental area only [135].

We have not found any studies of displacement of crime or diffusion of benefits in Information Security. This leads to the following suggestion for future research:

Question 9 *Which techniques merely displace the benefits for the criminal, and which ones actually diffuse them?*

An interesting aspect of this is whether displacement of crime and diffusion of benefits functions the same way in cyber-space as in the physical world.

3.5 Practical issues

Manufacturers generally consider crime prevention a task for the police, because manufacturers assume that their customers do not want to pay for security features. Therefore, manufacturers are generally unwilling to invest in crime prevention, unless forced by government to do so. Governments have good reasons to intervene because the cost of crime is not simply the replacement cost of a stolen item. For example the average cost of a simple street robbery is estimated at over 7,000 pounds by the UK home office, due to the cost of the criminal justice system, reduced productivity of the target etc [185].

One of the pitfalls of crime prevention is that it is easy to alienate the manufacturers by blaming them for criminogenic design [12]. A better way to proceed is to find convincing arguments to do something about crime, for example by developing a theft index. In the UK, car theft became endemic in the late eighties, because it proved to be easy to defeat the locks. In 1992 the Home office started to publish an annual car theft index, which shows which cars are at risk. This proved to be an incentive for the car industry to improve the locks [174]. In the following years, car theft was reduced considerably. While it cannot be excluded that the reduction was due to other causes, such alternative causes have never been found, so it is assumed that the car theft index did indeed cause the reduction in the number of car thefts.

Criminologists at Loughborough University have investigated theft of mobile phones from a Crime Science perspective. First, the criminogenic properties of the mobile phone were analysed in detail [273]. The analysis found several approaches to reduce the opportunity for phone theft, of which blacklisting of the phone IMEI number appeared to be a good choice. The problem with this approach is that the cost borne by the operators to maintain and enforce the blacklist is not insignificant, particularly when considering that stolen phones are easily exported to another country. So naturally, the operators are not keen, and again a theft index could prove to be a useful tool to persuade the operators to spend more effort on the problem.

Due to the necessary data cleaning, developing a theft index from existing data bases is a labour intensive process. A typical problem that still has to be overcome is that the relevant data base may not be set up to be used for this purpose. For example once a stolen car is recovered, the relevant entry in the UK police national computer database is removed [174]. To obtain the necessary data, researchers had to go directly to the individual police forces. With a little foresight, this problem could have been prevented, although the legal implications of re-purposing data bases must be carefully assessed.

Even if blacklisting is universally enforced, offenders are often able to change the IMEI number by reprogramming the mobile phone [161]. Prevention of phone theft is predicted to become even more important in the future, as more and more mobile phones are able to make payments as well [271]. This is where new ideas from Computer Scientists are welcome, especially considering the fact that an increasing range of products that are IP enabled [96], such as smart phones. IP enabled TV sets have recently appeared on the market, with IP enabled cars just around the corner. If Mark Weiser's vision [270] of Ubiquitous Computing (a calm technology that recedes into the background of our lives) becomes true, then at some point in time every object will be networked. This provides new tools for the designer against crime such as being able to register the whereabouts of the product so that a theft index can be made. Naturally, there are interesting privacy issues to be taken into account.

The examples above show that we all have a responsibility for crime prevention: for example motorists must lock their cars; the manufacturer must design and implement appropriate locks, and the government must make sure that each party behaves responsibly [174].

4 Conclusions

Our main conclusion is that the methods from Crime Science applied to Information Security lead to a useful refinement of Crime Science which we call Cyber-crime Science. This refinement provides an array of tools both from Crime Science and from Information Security that can be used to prevent cyber-crime.

Cyber-crime can also be prevented by measures focusing on the offender but this is beyond the scope of our paper. There might be breaches of Information Security that are merely a nuisance and not crime, and not all cyber-crime is caused by breaching Information Security. However we argue that treating a breach of Information Security primarily as an occurrence of cyber-crime gives us two complementary opportunities.

The first opportunity is to deploy the knowledge from Crime Science to come to the assistance of Information Security. We give two examples:

- Crime Science promotes a crime specific approach embodied in a number of checklists, such as CRAVED which we discussed on page 6 but also others, such as:
  - High Value, low Inertia, high Visibility and easy Access (VIVA) [67];
  - Identifiable, Neutral, Seen, Attached, Findable, Executable, Hidden, Automatic, Necessary, Detectable, and Secure (INSAFEHANDS) [273];
  - Stealth, Challenge, Anonymity, Reconnaissance, Escape, and Multiplicity (SCAREM) [207];

  Each checklist helps to design crime prevention measures. These checklists have proven to be effective for crime involving tangible objects such as theft of mobile phones, but only CRAVED has been applied to information [207, chapter 4];

- The research methodology of Crime Science has proved its value in traditional crime. We see opportunities to apply the method also to cyber-crime. For example, in the phishing case study discussed in Appendix B.1 we suggest how the researchers could have improved their results if they had applied results from Crime Science.

The second opportunity is to augment the array of crime prevention techniques from Crime Science with appropriate techniques from Information Security to deal with cyber-crime.

In Section 3 we cite related work that shows that there is overlap between existing Information Security techniques and the 25 generic opportunity reducing techniques (for example access control as a technique for target hardening). We have not found techniques from Information Security that cannot be classified as an instance of one of the 25 techniques. However, there are generic techniques for which we have not been able to find convincing specific Information Security techniques. For example for generic technique reduce arousal, we only found the unconvincing specific technique "make shop lifting less attractive if goods are believed chipped with RFID" [272].

If Information Security indeed overlaps with situational prevention of cyber-crime, then why have we found so little evidence of this in the literature? For example the first edition of Ross Anderson's book on Security Engineering [7] does not mention Crime Science. However, the second edition [9] does mention Crime Science, but only in connection with physical security. We believe that the role of Information Security as technology for cyber-crime prevention is as yet largely unexplored because:

- Information Security researchers are not normally taught Criminology, nor Crime Science;
- Information Security focuses on the technology, which is important for Crime Science but the context is at least as important for the prevention of crime;
- Assessing the effectiveness of crime prevention measures requires knowledge of Social Science research

methods [89], and in particular the prosecution of realistic experiments for which Computer Scientists are not always well equipped, and which if embarked on naively run the risk of problems with the law.

While Computer Scientists appear to have had limited exposure from the ideas of Criminologists, the reverse is certainly not true. Appendix D reviews only the tip of the iceberg of the papers where Computer Science technologies such as data mining, simulation, and geographical information systems are used effectively by Social Scientists in general and Criminologists in particular.

To bridge the gap between Crime Science and Information Security we have identified a number of research questions for multidisciplinary research teams throughout the paper and the online appendices labelled Question 1 . . . 24. Here we bring all questions together. We discuss first the questions emanating from the conceptual framework of Crime Science, and then follow with the questions arising from the review of the disciplines closely related to Crime Science.

RAA. The opportunity for crime is likely to present itself during routine activities, when (1) a potential offender meets (2) a suitable target in the absence of (3) a capable guardian. Transferring preventive measures from traditional crime to cyber-crime prevention requires some conceptual changes: In the case of cyber-crime, routine activities include the daily workflow of on-line actions of potential offenders, who may be insiders or outsiders of an organization, or perhaps we should say who may or may not have specialised access. Digital targets may be manipulated remotely after they have been are stolen. Guardians need some access and overview of potential targets and therefore need to be "close" to their target. All of this raises three questions:

- What distinguishes insiders from outsiders (or specialised access from regular access) in a cyber-physical world? (Question 1) How can we observe their routine activities effectively, while preserving anonymity? What deterrence techniques [151] are available for these categories and how effective are these techniques? What about the category of people who are both insiders and outsiders (e.g. consultants, free lancers, outsourcing providers)?

- What manipulations of e.g. value of stolen digital goods would be effective in deterring potential attackers of these assets? (Question 2) Would it be possible to assist digital forensics too?

- What is proximity in a cyber-physical world? (Question 3)

CPT. Offenders find opportunities for crime during the daily journey between home, work, and leisure. As a result, crime usually occurs in specific patterns and it is usually concentrated at particular places, and at particular times, i.e. hotspots. Prevention must therefore target these hotspots. In the cyber-physical world too, potential offenders move around, both physically (taking mobile devices to places) and digitally (surfing the web). Identification of hot-spots in the cyber-physical world is however conceptually difficult and identifying hotspots may violate privacy rules. This raises the question:

- How can we monitor activity on the Internet to identify hotspots and still respect privacy? What concept(s) of "location" are relevant for the identification of hot sports in the Internet? (Question 4)

Offenders who commit a cyber-crime are usually able to conceal their identities better than for traditional crime. We believe that mechanisms are needed that enable law enforcement to revoke anonymity in cyber-space without placing undue restrictions on the freedom of law abiding citizens.

RCP. Human behaviour is governed by its expected consequences. Criminal actors thus make cost/benefit tradeoffs of expected consequences. This view is applicable without change to cyber-crime. The leading research question here is:

- Which cost/benefit tradeoffs do cybercriminals actually make? (Question 5) Are there different classes of criminals that make different kinds of tradeoffs? What role does bounded rationality play?

Some research on this question has already been done but more work needs to be done.

Repeat Victimization. Some victims are repeatedly victims of the same crime. This is useful knowledge for taking preventive measures but so far not much is known about repeat victimization in cyber-crime. This raises the question:

- What is the extent and nature of repeat victimization in cyber-crime? (Question 6)

The 25 generic opportunity-reducing techniques of Crime Science can be applied to reduce the opportunity of cyber-crime. There are three aspects to this:

1. Applying current results of Crime Science to cyber-crime;

2. Extending this with elements specific to the cyber-physical world, and not yet studied in Crime Science;

3. Applying the methods of Crime Science to generate new knowledge about cyber-crime that can be used for preventing cyber-crime.

We discuss each of these three aspects in turn.

Firstly, the questions related to applying current results to cyber-crime are:

- Which of the 25 generic opportunity-reducing techniques is effective in preventing which class of cyber-crime? (Question 8)

- Which techniques merely displace the criminal activities, and which ones actually diffuse the benefits of prevention? (Question 9)

- All questions suggested in the Phishing case study (Question 12 ... 17) and the Online auction fraud case study (Questions 18 ... 19) of Appendix B.

Secondly, the questions related to extending current results specific to the cyber-physical world should take a new role into account, which is that of the ISP. For traditional crime there is not a single agent that promotes crime, whereas without the Internet, cyber-crime would not exist. The ISP should therefore play a key role in the fight against cyber-crime, and further research is needed into methods that empower the ISP in the fight against cyber-crime. This raises the following question:

- What roles can ISPs have in preventing cyber-crime, and what is the effectiveness of these roles? (Question 7)

More generally, perhaps Cyber-crime requires an extension of the Crime Science methods:

- Does Cyber-crime Science require an extension of the set of 25 generic opportunity reducing techniques? (Question 11)

Thirdly, the questions related to generating new knowledge about cyber-crime would have to look specifically at forms of cyber-crime that do not have an obvious pendant in the real world. Examples of such crimes are fraud in Second Life [242, 216], click fraud [170], and one-click fraud [62]. Fraud in second life targets virtual property that can be monetized in the real world. One-click fraud is a form of blackmail that is apparently successful in Japan; it works as follows. Suppose that the target visits a web site that he would not like his wife or his employer to know about. The controller of the web site then asks for money to keep silent, and enforces his request by promising to send a postcard to the address of the target. Click fraud works as follows. An advertiser places an advert on a hosting web site, which receives a certain amount of money for each time a visitor to the hosting web site clicks on the advert. A fraudulent hosting web site then employs inexpensive labour or automated tools to generate as many clicks on the advert as possible. Finding measures to prevent these new forms of cyber-crime will require new research. Click fraud resembles the real world fraud whereby people fill postage paid reply envelopes with something heavy, but the motive is not the same.

- How can we apply the empirical evaluation methods of Crime Science to cyber-crime? (Question 10)

For example, we believe that the percentage of cyber-crime that is reported to the police is lower than the percentage of traditional crime reported to the police. Companies have a natural inclination to keep cyber-crime event secret. The lack of adequate statistics is an impediment to the development of the field and the development of policy. Further research is needed into methods of collecting relevant cyber-crime statistics.

Finally, it would be useful to have a collection of case studies for each of the 25 generic techniques applied to specific forms of cyber-crime. For example, the generic technique of control disinhibitors which focuses on drugs and alcohol could perhaps be instantiated by studying Internet addiction. Such a cyber-crime specific collection could then serve as the starting point for a more systematic approach towards solving new forms of cyber-crime.

Disciplines supporting Cyber-crime Science. There are three disciplines that contribute significantly to Crime Science in general, and to Cyber-crime Science in particular. These are Computational Social Science, Economics, and Law.

Methods and techniques from Computation Social Science can be used to simulate crime, and hence cyber-crime. This does not lead to a particular research question but to a research approach:

- Use computational simulation as a research method in the study of cyber-crime. (Approach 27)

Economic approaches can be used to understand crime, for example by taking the bounded rationality point of view. From an economic point of view some specific questions have been raised (Questions 20 ... 22), all of which lead to the following research approach:

- Use economic methods in the study of cyber-crime. (Approach 23)

Similarly, legal approaches can be used to understand crime, and hence cyber-crime. Cyber-crime can be automated to a degree that cannot be achieved for traditional crime. This provides a challenge for law enforcement and the judicial system that must be met by further research. For example intelligence gathering on the Internet can be automated just like cyber-crime itself. Based on Questions 24 ... 26 we suggest the following research approach:

- Use legal methods to control the cost of cyber-crime to society.

Finally we believe that there are important opportunities to make Information Security teaching both more relevant and more exciting:

- Computer scientists would benefit from a basic grounding in Criminology as well as standard research methods from Social Science;

- Design products and systems to reduce the opportunity for crime is fun, and young designers are particularly apt at “lateral thinking” needed to be successful. Gamman and Hughes [111] present a range of imaginative designs by their students to prevent pick pocketing. A multidisciplinary course on Cybercrime Science is probably attractive to students who now go straight into the police or the security industry [70]. A useful starting point for a curriculum would be Brooks [47], who creates a mind map of all the relevant disciplines that deal with all aspects of security, including physical security, Information Security. Teaching Information Security as a technology to prevent crime creates opportunities for exciting student projects. For example we have run a series of projects where student are asked to steal laptops from our colleagues at the university [87]. The ingenuity and enthusiasm of the student for such projects is truly amazing, and can be channelled in an effective learning experience.

Acknowledgments

We are grateful to Ron Clarke, Hans Hendrickx, and Ken Pease for their suppport.

The references below are annotated with the main discipline (i.e. *Biology*, *Computing*, *Crime Science*, *Cybercrime Science*, *Criminology*, *Economics*, *Economics of Privacy*, *Economics of Security*, *Ethics*, *Forensics*, *Information Security*, *Law*, *Medicine*, *Physics*, *Psychology*, *Sociology*) and in some cases also the main topic of the paper, which is either *Analysis* or *Simulation* of Crime, or Cyber-crime in general or more specifically *Phishing*, *Insider* attacks, or *Mobile / Laptop* theft. Papers annotated with *IEEE* are IEEE Security & Privacy papers that mention crime. A paper that cites the work of the Crime Science pioneers is annotated with an asterisk.

References

[1] A. Acquisti. Privacy and security of personal information : Economic incentives and technological solutions. In J. Camp and R. Lewis, editors, *The Economics of Information Security*, pages 179–186. Kluwer, 2004. (Computing-Economics Privacy). Available from: `http://www.heinz.cmu.edu/~acquisti/papers/acquisti_eis_refs.pdf`.

[2] A. Acquisti. Nudging privacy: The behavioral economics of personal information. *IEEE Security and Privacy*, 7(6):82–85, Nov 2009. (Computing-Economics Privacy). Available from: `http://dx.doi.org/10.1109/MSP.2009.163`.

[3] A. Acquisti, R. Dingledine, and P. Syverson. On the economics of anonymity. In *7th Int. Conf. on Financial Cryptography*, volume 2742 of *LNCS*, pages 84–102, Guadeloupe, French West Indies, Jan 2003. Springer. (Computing-Economics Privacy). Available from: `http://dx.doi.org/10.1007/978-3-540-45126-6_7`.

[4] * R. Adderley. The use of data mining techniques in operational crime fighting. In *2nd Symp. on Intelligence and Security Informatics (ISI)*, volume 3073 of *LNCS*, pages 418–425, Tucson, Arizona, Jun 2004. Springer. (Computing-Analysis). Available from: `http://dx.doi.org/10.1007/978-3-540-25952-7_32`.

[5] M. Afanasyev, T. Kohno, J. Ma, N. Murphy, S. Savage, A. C. Snoeren, and G. M. Voelker. Privacy-preserving network forensics. *Commun. ACM*, 54(5):78–87, Mar 2011. (Computing). Available from: `http://dx.doi.org/10.1145/1941487.1941508`.

[6] R. Albert and A.-L. Barabási. Statistical mechanics of complex networks. *Reviews of Modern Physics*, 74(1):47–97, Jan 2002. (Physics). Available from: `http://dx.doi.org/10.1103/RevModPhys.74.47`.

[7] R. J. Anderson. *Security Engineering: A guide to building dependable distributed systems.* John Wiley & Sons Inc, New York, 2001. (Computing). Available from: `http://www.cl.cam.ac.uk/~rja14/book.html`.

[8] R. J. Anderson. Why information security is Hard-An economic perspective. In *17th Annual Computer Security Applications Conf. (ACSAC)*, pages 358–365, New Orleans, Louisiana, Dec 2001. IEEE. (Computing-Economics Security). Available from: `http://dx.doi.org/10.1109/ACSAC.2001.991552`.

[9] R. J. Anderson. *Security Engineering: A guide to building dependable distributed systems.* John Wiley & Sons Inc, New York, second edition, 2008. (Computing). Available from: `http://www.cl.cam.ac.uk/~rja14/book.html`.

[10] R. J. Anderson, R. Boehme, R. Clayton, and T. Moore. Security economics and the internal market. Technical report, ENISA - the European Network and Information Security Agency,

Jan 2008. (Computing-Economics Security). Available from: http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec.

[11] R. J. Anderson and T. Moore. The economics of information security. *Science*, 314(5799):610–613, Oct 2006. (Computing-Economics Security). Available from: http://dx.doi.org/10.1126/science.1130992.

[12] * R. Armitage and K. Pease. Design and crime: Proofing electronic products and services against theft. *European J. on Criminal Policy and Research*, 14(19):1–9, Mar 2008. (Criminology-Crime Science). Available from: http://dx.doi.org/10.1007/s10610-007-9043-6.

[13] * S. Atkinson, C. Johnson, and A. Phippen. Improving protection mechanisms by understanding online risk. *Information Management and Computer Security*, 15(5):382–393, 2007. (Computing). Available from: http://dx.doi.org/10.1108/09685220710831125.

[14] R. August. International cyber-jurisdiction: a comparative analysis. *American Business Law J.*, 39(4):531–574, Jun 2002. (Law). Available from: http://dx.doi.org/10.1111/j.1744-1714.2002.tb00305.x.

[15] T. Aura, P. Nikander, and G. Camarillo. Effects of mobility and multihoming on transport-protocol security. In *25th IEEE Symp. on Security and Privacy (S&P)*, pages 12–26, Oakland, California, May 2004. IEEE. (Computing-IEEE). Available from: http://dx.doi.org/10.1109/SECPRI.2004.1301312.

[16] K. Aytes and T. Connolly. Computer security and risky computing practices: A rational choice perspective. *J. of Organizational and End User Computing*, 16(3):22–40, 2004. (Computing). Available from: http://dx.doi.org/10.4018/joeuc.2004070102.

[17] I. Balbin and N. C. Karmakar. Phase-encoded chipless RFID transponder for large-scale low-cost applications. *IEEE Microwave and Wireless Components Letters*, 19(8):509–511, Aug 2009. (Computing). Available from: http://dx.doi.org/10.1109/LMWC.2009.2024840.

[18] M. Bateson, D. Nettle, and G. Roberts. Cues of being watched enhance cooperation in a real-world setting. *Biology Letters*, 2(3):412–414, Sep 2006. (Biology). Available from: http://dx.doi.org/10.1098/rsbl.2006.0509.

[19] J. Becker. Who are the computer criminals? *SIGCAS Comput. Soc.*, 12(1):18–20, 1982. (Computing-Cybercrime). Available from: http://dx.doi.org/10.1145/957893.957898.

[20] R. A. Becker, C. Volinsky, and A. R. Wilks. Fraud detection in telecommunications: History and lessons learned. *Technometrics*, 52(1):20–33, Feb 2010. (Computing-Analysis). Available from: http://dx.doi.org/10.1198/TECH.2009.08136.

[21] * N. L. Beebe and V. S. Rao. Using situational crime prevention theory to explain the effectiveness of information systems security. In *Conf. on Protecting the Intangible Organizational Assets (SoftWars)*, Las Vegas, Nevada, Dec 2005. The Information Institute. (Computing-Cybercrime Science).

[22] S. M. Bellovin. Spamming, phishing, authentication, and privacy. *Commun. ACM*, 47(12):144, Dec 2004. (Computing-Phishing). Available from: http://dx.doi.org/10.1145/1035134.1035159.

[23] B. Berendt, O. Gunther, and S. Spiekermann. Privacy in e-commerce : Stated preferences vs. actual behavior. *Communications of the ACM*, 48(4):101–106, Apr 2005. (Computing-Economics Privacy). Available from: http://dx.doi.org/10.1145/1053291.1053295.

[24] R. Berk. How you can tell if the simulations in computational criminology are any good. *J. of Experimental Criminology*, 4(3):289–308, Sep 2008. (Criminology-Simulation). Available from: http://dx.doi.org/10.1007/s11292-008-9053-5.

[25] S. Bhattacharjee, R. D. Gopal, K. Lertwachara, and J. R. Marsden. Consumer search and retailer strategies in the presence of online music sharing. *J. of Management Information Systems*, 23(1):129–159, Summer 2006. (Computing-Economics Security). Available from: http://dx.doi.org/10.2753/MIS0742-1222230104.

[26] N. Bird, C. Conrado, J. Guajardo, S. Maubach, G. Jan Schrijen, B. Škorić, A. M. H. Tombeur, P. Thueringer, and P. Tuyls. ALGSICS - combining physics and cryptography to enhance security and privacy in RFID systems. In F. Stajano, C. Meadows, S. Capkun, and T. Moore, editors, *4th European Workshop on Security and Privacy in Adhoc and Sensor Networks (ESAS)*, volume 4572 of *LNCS*, pages 187–202, Cambridge, UK, Jul 2007. Springer. (Computing). Available from: http://dx.doi.org/10.1007/978-3-540-73275-4_14.

[27] M. S. Blumenthal and D. D. Clark. Rethinking the design of the Internet: the end-to-end arguments

vs. the brave new world. *ACM Trans. Inter. Tech.*, 1(1):70–109, 2001. (Computing). Available from: http://dx.doi.org/10.1145/383034.383037.

[28] * T. Bosse and C. Gerritsen. Agent-based simulation of the spatial dynamics of crime: on the interplay between criminal hot spots and reputation. In *7th Int. joint Conf. on Autonomous agents and multiagent systems (AAMAS)*, pages 1129–1136, Estoril, Portugal, May 2008. Int. Foundation for Autonomous Agents and Multiagent Systems. (Computing-Simulation). Available from: http://dx.doi.org/10.1145/1402298.1402378.

[29] * T. Bosse and C. Gerritsen. Comparing crime prevention strategies by Agent-Based simulation. In *IEEE/WIC/ACM Int. Joint Conf. on Web Intelligence and Intelligent Agent Technologiesi (WI-IAT)*, volume 2, pages 491–496, Milan, Italy, Sep 2009. IEEE. (Computing-Simulation). Available from: http://dx.doi.org/10.1109/WI-IAT.2009.200.

[30] * T. Bosse, C. Gerritsen, M. C. A. Klein, and F. M. Weerman. Development and validation of an Agent-Based simulation model of juvenile delinquency. In *Int. Conf. on Computational Science and Engineering (CSE)*, pages 200–207, Vancouver, Canada, Aug 2009. IEEE. (Computing-Simulation). Available from: http://dx.doi.org/10.1109/CSE.2009.136.

[31] * T. Bosse, C. Gerritsen, and J. Treur. Case analysis of criminal behaviour. In *20th Int. Conf. on Industrial, Engineering and Other Applications of Applied Intelligent Systems (IEA/AIE) - New Trends in Applied Artificial Intelligence*, volume 4570 of *LNCS*, pages 621–632, Kyoto, Japan, Jun 2007. Springer. (Computing-Simulation). Available from: http://dx.doi.org/10.1007/978-3-540-73325-6_62.

[32] * T. Bosse, C. Gerritsen, and J. Treur. Cognitive and social simulation of criminal behaviour: the intermittent explosive disorder case. In *6th Int. joint Conf. on Autonomous agents and multiagent systems (AAMAS)*, pages 1–8, Honolulu, Hawaii, 2007. ACM. (Computing-Simulation). Available from: http://dx.doi.org/10.1145/1329125.1329195.

[33] * T. Bosse, C. Gerritsen, and J. Treur. Towards integration of biological, psychological and social aspects in agent-based simulation of violent offenders. *Simulation*, 85(10):635–660, Oct 2009. (Computing-Simulation). Available from: http://dx.doi.org/10.1177/0037549709103407.

[34] * K. J. Bowers and S. D. Johnson. Domestic burglary repeats and Space-Time clusters. *European J. of Criminology*, 2(1):67–92, 2005. (Criminology-Analysis). Available from: http://dx.doi.org/10.1177/1477370805048631.

[35] * K. J. Bowers, S. D. Johnson, and A. F. G. Hirschfield. Closing off opportunities for crime: An evaluation of Alley-Gating. *European J. on Criminal Policy and Research*, 10(4):285–308, Sep 2004. (Criminology-Analysis). Available from: http://dx.doi.org/10.1007/s10610-005-5502-0.

[36] * K. J. Bowers, S. D. Johnson, and K. Pease. Prospective Hot-Spotting - the future of crime mapping? *The British J. of Criminology*, 44(5):641–658, 2004. (Criminology-Analysis). Available from: http://dx.doi.org/10.1093/bjc/azh036.

[37] * P. L. Brantingham and P. J. Brantingham. Environment, routine and situation: Towards a pattern theory of crime. In R. V. Clarke and M. Felson, editors, *Routine Activity and Rational Choice*, volume Advances in Criminological Theory 5, pages 259–294. Transaction Publishers, 1993. (Criminology-Crime Science).

[38] * P. L. Brantingham and P. J. Brantingham. Criminality of place : Crime generators and crime attractors. *European J. on Criminal Policy and Research*, 3(3):5–26, Sep 1995. (Criminology-Analysis). Available from: http://dx.doi.org/10.1007/BF02242925.

[39] * P. L. Brantingham, P. J. Brantingham, and U. Glässer. Computer simulation in criminal justice research. *Criminal Justice Matters*, 58(1):18–19, 2004. (Computing-Simulation). Available from: http://dx.doi.org/10.1080/09627250408553238.

[40] * P. L. Brantingham, U. Glässer, B. Kinney, K. Singh, and M. Vajihollahi. A computational model for simulating spatial aspects of crime in urban environments. In *Int. Conf. on Systems, Man and Cybernetics*, volume 4, pages 3667–3674. IEEE, Oct 2005. (Computing-Simulation). Available from: http://dx.doi.org/10.1109/ICSMC.2005.1571717.

[41] S. W. Brenner. Organized cybercrime? how cyberspace may affect the structure of criminal relationships. *Int. J. of Law and Information Technology*, 4(1):1–50, Fall 2002. (Law). Available from: http://jolt.unc.edu/abstracts/volume-4/ncjltech/p1.

[42] S. W. Brenner. Cybercrime metrics: New wine, old bottles? *Virginia J. of Law and Technology*, 9(4):Article 13, Fall 2004. (Law). Available from: http://www.vjolt.net/vol9/issue4/v9i4_a13-Brenner.pdf.

[43] S. W. Brenner. U.S. cybercrime law: Defining offenses. *Information Systems Frontiers*, 6(2):1387–3326, Jun 2004. (Law). Available from: http://dx.doi.org/10.1023/B:ISFI.0000025780.94350.79.

[44] S. W. Brenner. Fantasy crime: the role of criminal law in virtual worlds. *Vanderbilt J. of Entertainment and Technology Law*, 11(1):Article 1, Fall 2008. (Law). Available from: http://law.vanderbilt.edu/publications/journal-entertainment-technology-law/archive/download.aspx?id=3644.

[45] S. W. Brenner and L. L. Clarke. Distributed security: Preventing cybercrime. *John Marshall J. of Computer & Information Law*, XXIII(4):659–710, Summer 2005. (Law). Available from: http://www.jcil.org/journal/articles/434.html.

[46] S. W. Brenner and B.-J. Koops. Approaches to cybercrime jurisdiction. *J. of High Technology Law*, 4(1):1–46, 2004. (Law). Available from: http://www.jhtl.org/publications/index.cfm?vol=4\&num=1.

[47] D. J. Brooks. A study to develop a consensual map of security expert knowledge structure. In *40th Int. Carnahan Conf. on Security Technology*, pages 173–179, Lexington, Kentucky, Oct 2006. IEEE. (Computing-Information Security). Available from: http://dx.doi.org/10.1109/CCST.2006.313446.

[48] * C. Brookson, G. Farrell, J. Mailley, S. Whitehead, and D. Zumerle. ICT product proofing against crime. ETSI White Paper 5, European Telecommunications Standards Institute, Sophia Antipolis, France, Feb 2007. (Computing-Cybercrime Science). Available from: http://www.etsi.org/WebSite/document/Technologies/ETSI-WP5_Product_Proofing.pdf.

[49] * D. E. Brown. The regional crime analysis program (ReCAP): a framework for mining data to catch criminals. In *3rd IEEE Int. Conf. on Systems, Man, and Cybernetics (ICSMC)*, pages 2848–2853, San Diego, California, Oct 1998. IEEE. (Computing-Simulation). Available from: http://dx.doi.org/10.1109/ICSMC.1998.725094.

[50] * D. E. Brown and L. F. Gunderson. Using clustering to discover the preferences of computer criminals. *IEEE Trans. on Systems, Man and Cybernetics, Part A: Systems and Humans*, 31(4):311–318, Jul 2001. (Computing-Analysis). Available from: http://dx.doi.org/10.1109/3468.935048.

[51] D. E. Brown, L. F. Gunderson, and M. H. Evans. Interactive analysis of computer crimes. *Computer*, 33(8):69–77, Aug 2000. (Computing-Analysis). Available from: http://dx.doi.org/10.1109/2.863970.

[52] * D. E. Brown and R. B. Oxford. Data mining time series with applications to crime analysis. In *Int. Conf. on Systems, Man and Cybernetics*, volume 3, pages 1453–1458, Tucson, Arizona, Oct 2001. IEEE. (Computing-Analysis). Available from: http://dx.doi.org/10.1109/ICSMC.2001.973487.

[53] D. Brumley, P. Poosankam, D. Song, and Jiang Zheng. Automatic Patch-Based exploit generation is possible: Techniques and implications. In *29th IEEE Symp. on Security and Privacy (S&P)*, pages 143–157, Oakland, California, May 2008. IEEE. (Computing-IEEE). Available from: http://dx.doi.org/10.1109/SP.2008.17.

[54] J. M. Buchanan. An economic theory of clubs. *Economica, New Series*, 32(125):1–14, Feb 1965. (Economics). Available from: http://www.jstor.org/stable/2552442.

[55] M. A. Caloyannides. Forensics is so "yesterday". *IEEE Security and Privacy*, 7(2):18–25, Mar 2009. (Computing-Forensics). Available from: http://dx.doi.org/10.1109/MSP.2009.37.

[56] J. Camenisch and E. Van Herreweghen. Design and implementation of the idemix anonymous credential system. In *9th ACM Conf. on Computer and communications security (CCS)*, pages 21–30, Washington, DC, 2002. ACM. (Computing). Available from: http://dx.doi.org/10.1145/586110.586114.

[57] D. Caputo, M. Maloof, and G. Stephens. Detecting insider theft of trade secrets. *IEEE Security and Privacy*, 7(6):14–21, Nov 2009. (RCT). Available from: http://dx.doi.org/10.1109/MSP.2009.110.

[58] C. C. Carbon and V. M. Hesslinger. Bateson et al.'s (2006) cues-of-being-watched paradigm revisited. *Swiss Journal of Psychology*, page to appear, 2012. (Psychology). Available from: http://www.experimental-psychology.de/ccc/docs/pubs/ms_SJP_CarbonHesslinger_EyesAsSocialCues_IN%20PRESS.pdf.

[59] A. Cardenas, S. Radosavac, J. Grossklags, J. Chuang, and C. Hoofnagle. An economic map of cybercrime. In *37th Research Conf. on Communication, Information and Internet Policy (TPRC)*, page online, George Mason University Law School, Arlington, Virginia, Sep 2009. TPRC, Franham, Virginia. (Computing-Economics Security). Available from: `http://www.tprcweb.com/images/stories/papers/cardenas_2009.pdf`.

[60] E. Casey and G. J. Stellatos. The impact of full disk encryption on digital forensics. *ACM SIGOPS Operating Systems Review*, 42(3):93–98, Apr 2008. (Computing-Forensics). Available from: `http://dx.doi.org/10.1145/1368506.1368519`.

[61] M. Chau and J. Xu. Mining communities and their relationships in blogs: A study of online hate groups. *Int. J. Human-Computer Studies*, 65(1):57–70, Jan 2007. (Computing-Analysis). Available from: `http://dx.doi.org/10.1016/j.ijhcs.2006.08.009`.

[62] N. Christin, S. S. Yanagihara, and K. Kamataki. Dissecting one click frauds. In *17th ACM Conf. on Computer and communications security (CCS)*, pages 15–26, Chicago, Illinois, Oct 2010. ACM. (Computing). Available from: `http://dx.doi.org/10.1145/1866307.1866310`.

[63] M. Christodorescu, S. Jha, A. A. Seshia, D. Song, and R. E. Bryant. Semantics-aware malware detection. In *26th IEEE Symp. on Security and Privacy (S&P)*, pages 32–46, Oakland, California, May 2005. IEEE. (Computing-IEEE). Available from: `http://dx.doi.org/10.1109/SP.2005.20`.

[64] * H. Chua, J. Wareham, and D. Robey. The role of online trading communities in managing internet auction fraud. *MIS Quarterly: Management Information Systems*, 31(4):759–781, Dec 2007. (Computing-Cybercrime Science). Available from: `http://www.misq.org/archivist/vol/no31/Issue4/ChuaWarehamRobey.html`.

[65] * R. V. Clarke. Deterring obscene phone callers: Preliminary results of the New Jersey experience. *Security J.*, 1(3):143–148, 1990. (Criminology-Crime Science).

[66] R. V. Clarke. Introduction. In R. V. Clarke, editor, *Situational Crime Prevention: Successful Case Studies*, pages 1–43. Harrow and Heston, 1997. (Criminology-Crime Science). Available from: `http://www.popcenter.org/library/reading/PDFs/scp2_intro.pdf`.

[67] * R. V. Clarke. Hot products: understanding, anticipating and reducing demand for stolen goods. Police Research Series Paper 112, Home Office, Policing and Reducing Crime Unit, London, 1999. (Criminology-Crime Science). Available from: `http://www.crimereduction.homeoffice.gov.uk/stolengoods/stolengoods1.htm`.

[68] * R. V. Clarke. Technology, criminology and crime science. *European J. on Criminal Policy and Research*, 10(1):55–63, Mar 2004. (Criminology-Crime Science). Available from: `http://dx.doi.org/10.1023/B:CRIM.0000037557.42894.f7`.

[69] * R. V. Clarke. Situational crime prevention. In R. Wortley and L. Mazerolle, editors, *Environmental Criminology and Crime Analysis*, pages 178–194. Willan Publishing, London, Jun 2008. (Criminology-Crime Science). Available from: `http://www.willanpublishing.co.uk/cgi-bin/indexer?product=9781843922803`.

[70] * R. V. Clarke. Crime science. In E. McLaughlin and T. Newburn, editors, *Handbook of Criminal Theory*, pages 271–283. Sage, London, 2009. (Criminology-Crime Science). Available from: `http://www.sagepub.com/books/Book228876`.

[71] * R. V. Clarke and P. Mayhew. The British gas suicide story and its criminological implications. *Crime and Justice*, 10:79–116, 1988. (Criminology-Crime Science). Available from: `http://www.jstor.org/stable/1147403`.

[72] R. V. Clarke and D. Weisburd. On the distribution of deviance. In D. M. Gottfredson and R. V. Clarke, editors, *Policy and Theory in Criminal Justice: Contributions in Honour of Leslie T. Wilkins*, volume Cambridge studies in criminology 62, pages 10–27. Avebury, Aldershot, UK, 1990. (Criminology).

[73] * R. V. Clarke and D. Weisburd. Diffusion of crime control benefits: Observations. In R. V. Clarke, editor, *Crime Prevention Studies on the Reverse of Displacement*, volume 2, pages 165–183. Criminal Justice Press, Monsey, New York, 1994. (Criminology-Crime Science). Available from: `http://www.popcenter.org/library/CrimePrevention/Volume_02/08clarke.pdf`.

[74] R. Clayton. Failures in a hybrid content blocking system. In *5th Int. Workshop on Privacy Enhancing Technologies (PET)*, volume 3856 of *LNCS*, pages 78–92, Cavtat, Croatia, May 2005. Springer. (Computing). Available from: `http://dx.doi.org/10.1007/11767831_6`.

[75] * L. E. Cohen and M. Felson. Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4):588–608, Aug 1979. (Criminology-Crime Science). Available from: `http://www.jstor.org/pss/2094589`.

[76] J. S. Coleman and T. J. Fararo. Introduction. In J. S. Coleman and T. J. Fararo, editors, *Rational Choice Theory: Advocacy and Critique*, pages ix–xix. Sage Publications Inc., Newbury Park, California, 1992. (Criminology).

[77] * L. Coles-Kemp and M. Theoharidou. Insider threat and information security management. In C. W. Probst, J. Hunker, D. Gollmann, and M. Bishop, editors, *Insider Threats in Cyber Security*, volume Advances in Information Security 49, pages 45–71. Springer, Jan 2010. (Computing). Available from: `http://dx.doi.org/10.1007/978-1-4419-7133-3_3`.

[78] * D. B. Cornish and R. V. Clarke. Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. In M. J. Smith and D. B. Cornish, editors, *Theory for Practice in Situational Crime Prevention*, volume Crime Prevention Studies 16, pages 41–96. Criminal Justice Press, Monsey, New York, 2003. (Criminology-Crime Science). Available from: `http://www.popcenter.org/Library/CrimePrevention/Volume_16/OpportunitiesPrecipitators.pdf`.

[79] * D. B. Cornish and R. V. Clarke. The rational choice perspective. In R. Wortley and L. Mazerolle, editors, *Environmental Criminology and Crime Analysis*, pages 21–47. Willan Publishing, Uffculme, UK, 2008. (Criminology-Crime Science). Available from: `http://www.willanpublishing.co.uk/cgi-bin/indexer?product=9781843922803`.

[80] * K. Cox. The application of crime science to the prevention of medication errors. *British J. of Nursing*, 17(14):924–927, Jul 2008. (Medicine). Available from: `http://www.internurse.com/cgi-bin/go.pl/library/abstract.html?uid=30662`.

[81] T. Craddock, C. R. Harwood, J. Hallinan, and A. Wipat. Opinion: e-Science: relieving bottlenecks in large-scale genome analyses. *Nature Reviews Microbiology*, 6:948–954, Dec 2008. (Biology). Available from: `http://dx.doi.org/10.1038/nrmicro2031`.

[82] P. Cromwell and J. N. Olson. *Breaking and Entering: Burglars on Burglary.* Wadsworth Publishing Company, Belmont, California, 2004. (Criminology).

[83] G. Cybenko, A. Giani, and P. Thompson. Cognitive hacking: a battle for the mind. *IEEE Computer*, 35(8):50–56, Aug 2002. (Computing-Cybercrime). Available from: `http://dx.doi.org/10.1109/MC.2002.1023788`.

[84] D. E. Denning. An Intrusion-Detection model. *IEEE Trans. Software. Eng.*, 13(2):222–232, 1987. (Computing). Available from: `http://dx.doi.org/10.1109/TSE.1987.232894`.

[85] D. E. Denning. *Information Warfare and Security.* Addison Wesley, Reading, Massachusetts, 1999. (Computing).

[86] R. Dhamija, J. D. Tygar, and M. Hearst. Why phishing works. In *Conf. on Human Factors in Computing Systems (CHI)*, pages 581–590, Montréal, Canada, 2006. ACM. (Computing-Phishing). Available from: `http://dx.doi.org/10.1145/1124772.1124861`.

[87] * T. Dimkov, W. Pieters, and P. H. Hartel. Laptop theft: a case study on effectiveness of security mechanisms in open organizations. Technical Report TR-CTIT-10-07, CTIT, University of Twente, Mar 2010. (Computing-MobileLaptop). Available from: `http://eprints.eemcs.utwente.nl/17358/`.

[88] R. C. Dodge Jr., C. Carvera, and A. J. Fergusona. Phishing for user security awareness. *Computers & Security*, 26(1):73–80, Feb 2007. (Computing-Phishing). Available from: `http://dx.doi.org/10.1016/j.cose.2006.10.009`.

[89] D. Dooley. *Social Research Methods.* Prentice Hall, fourth edition, May 2000. (Psychology). Available from: `http://www.pearsonhighered.com/educator/product/Social-Research-Methods/9780139554285.page`.

[90] N. M. Döring. The Internet's impact on sexuality: A critical review of 15 years of research. *Computers in Human Behavior*, 25(5):1089–1101, Sep 2009. (Psychology). Available from: `http://dx.doi.org/10.1016/j.chb.2009.04.003`.

[91] J. S. Downs, M. B. Holbrook, and L. F. Cranor. Decision strategies and susceptibility to phishing. In *2nd Symp. on Usable privacy and security (SOUPS)*, pages 79–90, Pittsburgh, Pennsylvania, Jul 2006. ACM. (Computing-Phishing). Available from: `http://dx.doi.org/10.1145/1143120.1143131`.

[92] * J. E. Eck. What do those dots mean? mapping theories with data. In D. Weisburd and T. McEwen, editors, *Crime Mapping and Crime*

Prevention - Crime Prevention Studies, volume 8, pages 379–406. Criminal Justice Press, Monsey, New York, 1998. (Criminology-Analysis). Available from: http://www.popcenter.org/library/CrimePrevention/Volume_08/13-Eck.pdf.

[93] * J. E. Eck and L. Liu. Contrasting simulated and empirical experiments in crime prevention. *J. of Experimental Criminology*, 4(3):195–213, Sep 2008. (Criminology-Simulation). Available from: http://dx.doi.org/10.1007/s11292-008-9059-z.

[94] * J. E. Eck and L. Liu. Varieties of artificial crime analysis: Purpose, structure, and evidence in crime simulations. In L. Liu and J. E. Eck, editors, *Artificial Crime Analysis Systems: Using Computer Simulations and Geographic Information Systems*, pages 413–432. Information Science Reference, Mar 2008. (Criminology-Simulation). Available from: http://www.igi-global.com/reference/details.asp?ID=7291.

[95] I. Ehrlich. Participation in illegitimate activities: A theoretical and empirical investigation. *The J. of Political Economy*, 81(3):521–565, May 1973. (Economics). Available from: http://dx.doi.org/10.1086/260058.

[96] * P. Ekblom. Designing products against crime. In R. Wortley and L. Mazerolle, editors, *Environmental Criminology and Crime Analysis*, pages 195–220. Willan Publishing, Uffculme, UK, 2008. (Criminology-Crime Science). Available from: http://www.willanpublishing.co.uk/cgi-bin/indexer?product=9781843922803.

[97] M. Eleccion. Beating the blue-box bandits. *IEEE Spectrum*, 9(8):52–58, Aug 1972. (Computing). Available from: http://dx.doi.org/10.1109/MSPEC.1972.5219018.

[98] J. M. Epstein. Agent-based computational models and generative social science. *Complexity*, 4(5):4160, May 1999. (Criminology-Simulation). Available from: http://www3.interscience.wiley.com/journal/63000401/abstract.

[99] * G. Farrell and K. Pease. *Repeat Victimization*, volume Crime Prevention Studies 12. Criminal Justice Press, Monsey, New York, 2001. (Criminology). Available from: http://www.popcenter.org/library/CrimePrevention/Volume_12/0introduction.pdf.

[100] * D. P. Farrington, S. Bowen, A. Buckle, T. Burns-Howell, J. Burrows, and M. Speed. An experiment on the prevention of shoplifting. In R. V. Clarke, editor, *Crime Prevention Studies*, volume 1, pages 93–119. Criminal Justice Press, Monsey, New York, 1993. (Criminology).

[101] * M. Felson. *Crime and nature*. Pine Forge Press, Thousands Oaks, California, 2006. (Criminology). Available from: http://www.sagepub.com/books/Book225968.

[102] * M. Felson and R. L. Boba. *Crime and Everyday Life*. Sage, Thousands Oaks, California, 4th edition, 2010. (Criminology). Available from: http://www.sagepub.com/books/Book228844.

[103] * M. Felson and R. V. Clarke. Opportunity makes the thief: Practical theory for crime prevention. Police Research Series Paper 98, Home Office, Policing and Reducing Crime Unit, London, 1998. (Criminology-Crime Science). Available from: http://www.homeoffice.gov.uk/rds/prgpdfs/fprs98.pdf.

[104] R. E. Ferner and J. K. Aronson. Medication errors, worse than a crime. *The Lancet*, 355(9208):947–948, Mar 2000. (Medicine). Available from: http://dx.doi.org/10.1016/S0140-6736(00)99025-1.

[105] P. Finn and M. Jakobsson. Designing ethical phishing experiments. *IEEE Technology and Society Magazine*, 26(1):46–58, Spring 2007. (Ethics-Phishing). Available from: http://dx.doi.org/10.1109/MTAS.2007.335565.

[106] D. Floreêncio and G. Herley. Phishing and money mules. In *IEEE Int. Workshop on Information Forensics and Security (WIFS)*, page Article 31, Seattle, Washington, Dec 2010. IEEEE. (Computing-Phishing). Available from: http://dx.doi.org/10.1109/WIFS.2010.5711465.

[107] D. Florêncio and C. Herley. Evaluating a trial deployment of password re-use for phishing prevention. In *2nd Annual eCrime Researchers Summit (eCrime)*, pages 26–36, Pittsburg, Pennsylvania, Oct 2007. ACM. (Computing-Phishing). Available from: http://dx.doi.org/10.1145/1299015.1299018.

[108] J. Franklin, V. Paxson, A. Perrig, and S. Savage. An inquiry into the nature and causes of the wealth of Internet miscreants. In *14th ACM Conf. on Computer and communications security (CCS)*, pages 375–388, Alexandria, Virginia, USA, Oct 2007. ACM. (Computing-Economics Security). Available from: http://dx.doi.org/10.1145/1315245.1315292.

[109] S. M. Furnell, P. S. Dowland, and P. W. Sanders. Dissecting the hacker manifesto information. *Management & Computer Security*, 7(2):69–75, 1999. (Computing-Cybercrime). Available from: http://dx.doi.org/10.1108/09685229910265493.

[110] S. Gajek and A.-R. Sadeghi. A forensic framework for tracing phishers. In *3rd IFIP WG 9.2, 9.6/ 11.6, 11.7/FIDIS Int. Summer School on The Future of Identity in the Information Society*, volume IFIP Int. Federation for Information Processing 262, pages 23–35, Karlstad, Sweden, Aug 2007. Springer, Boston. (Computing-Phishing). Available from: http://dx.doi.org/10.1007/978-0-387-79026-8_2.

[111] * L. Gamman and B. Hughes. Thinking thief - designing out misuse, abuse and criminal aesthetics. *The Ingenia Magazine*, 15, Feb 2003. (Criminology-Crime Science). Available from: http://www.ingenia.org.uk/ingenia/issues/issue15/Gamman.pdf.

[112] Hongyu Gao, Jun Hu, Christo Wilson, Zhichun Li, Yan Chen, and Ben Y. Zhao. Detecting and characterizing social spam campaigns. In *17th ACM Conf. on Computer and communications security (CCS)*, pages 681–683, Chicago, Illinois, Oct 2010. ACM. (Computing). Available from: http://dx.doi.org/10.1145/1866307.1866396.

[113] S. L. Garfinkel and R. C. Miller. Johnny 2: A user test of key continuity management with S/MIME and outlook express. In *1st Symp. on Usable privacy and security (SOUPS)*, pages 13–24, Pittsburgh, Pennsylvania, Jul 2005. ACM. (Computing-Phishing). Available from: http://dx.doi.org/10.1145/1143120.1143131.

[114] P. P. Garlinger. Privacy, free speech, and the patriot act: First and fourth amendment limits on national security letters. *New York University Law Review*, 84(4):1105–1147, 2009. (Law). Available from: http://www.law.nyu.edu/journals/lawreview/issues/vol842009/number4/.

[115] K. Geers. The challenge of cyber attack deterrence. *Computer Law & Security Review*, 26(3):298–303, May 2010. (Law). Available from: http://dx.doi.org/10.1016/j.clsr.2010.03.003.

[116] Z. J. M. H. Geradts, J. Bijhold, M. Kieft, M. Kurosawa, K. Kuroki, and N. Saitoh. Methods for identification of images acquired with digital cameras. In *Enabling Technologies for Law Enforcement and Security*, volume 4232, pages 505–512, Boston, Massachusetts, Nov 2000. SPIE - The Int. Society for Optical Engineering. (Computing-Forensics). Available from: http://dx.doi.org/10.1117/12.417569.

[117] G. Gigerenzer and D. G. Goldstein. Reasoning the fast and frugal way: Models of bounded rationality. *Psychological Review*, 103(4):650–669, 1996. (Psychology). Available from: http://dx.doi.org/10.1037/0033-295X.103.4.650.

[118] * J. Giles. Crime prevention: The lab arm of the law. *Nature*, 422:13–14, Mar 2003. (Criminology-Crime Science). Available from: http://dx.doi.org/10.1038/422013a.

[119] * U. Glässer, S. Rastkar, and M. Vajihollahi. Computational modeling and experimental validation of aviation security procedures. In *Int. Conf. on Intelligence and Security Informatics (ISI)*, volume 3975 of *LNCS*, pages 420–431, San Diego, California, May 2006. IEEE. (Computing-Simulation). Available from: http://dx.doi.org/10.1007/11760146_37.

[120] * U. Glässer, S. Rastkar, and M. Vajihollahi. Modeling and validation of aviation security. In *Intelligence and Security Informatics*, volume Studies in Computational Intelligence 135, pages 337–355. Springer, Berlin, Jun 2008. (Computing-Simulation). Available from: http://dx.doi.org/10.1007/978-3-540-69209-6_18.

[121] * U. Glässer and M. Vajihollahi. Computational modeling of criminal activity. In *1st European Conf. on Intelligence and Security Informatics (EuroISI)*, volume 5376 of *LNCS*, pages 39–50, Esbjerg, Denmark, Dec 2008. Springer. (Computing-Simulation). Available from: http://dx.doi.org/10.1007/978-3-540-89900-6_7.

[122] V. D. Gligor. 20 years of operating systems security. In *20th IEEE Symp. on Security and Privacy (S&P)*, pages 108–110, Oakland, California, May 1999. IEEE. (Computing-IEEE). Available from: http://dx.doi.org/10.1109/SECPRI.1999.766904.

[123] J. Goecks, W. K. Edwards, and E. D. Mynatt. Challenges in supporting end-user privacy and security management with social navigation. In *5th Symp. on Usable Privacy and Security (SOUPS)*, page Article 5, Mountain View, California, Jul 2009. ACM. (Computing). Available from: http://dx.doi.org/10.1145/1572532.1572539.

[124] P. Golle, F. McSherry, and I. Mironov. Data collection with Self-Enforcing privacy. *ACM*

Trans. on Information and System Security (TISSEC), 12(2):Article 9, Dec 2008. (Computing). Available from: http://dx.doi.org/10.1145/1455518.1455521.

[125] J. Goodman, G. V. Cormack, and D. Heckerman. Spam and the ongoing battle for the inbox. *Communications of the ACM*, 50(2):25–33, Feb 2007. (Computing-Phishing). Available from: http://dx.doi.org/10.1145/1216016.1216017.

[126] M. D. Goodman and S. W. Brenner. The emerging consensus on criminal conduct in cyberspace. *Int. J. of Law and Information Technology*, 10(2):139–223, Summer 2002. (Law). Available from: http://dx.doi.org/10.1093/ijlit/10.2.139.

[127] R. D. Gopal and G. L. Sanders. Preventive and deterrent controls for software piracy. *J. of Management Information Systems*, 13(4):29–47, Mar 1997. (Computing-Economics Security). Available from: http://www.jmis-web.org/articles/v13_n4_p29/.

[128] * M. R. Gottfredson and T. Hirschi. The nature of crime. In *A General Theory of Crime*, pages 15–44. Stanford University Press, 1990. (Criminology). Available from: http://www.sup.org/book.cgi?id=2686.

[129] W. R. Gove, M. Hughes, and M. Geerken. Are uniform crime reports a valid indicator of the index crimes - an affirmative answer with minor qualifications. *Criminology*, 23(3):451–502, 1985. (Criminology). Available from: http://dx.doi.org/10.1111/j.1745-9125.1985.tb00350.x.

[130] T. R. Graeff and S. Harmon. Collecting and using personal data: consumers awareness and concerns. *J. of Consumer Marketing*, 19(4):302–318, Mar 2002. (Computing-Economics Privacy). Available from: http://dx.doi.org/10.1108/07363760210433627.

[131] C. Grier, K. Thomas, V. Paxson, and M. Zhang. @spam: the underground on 140 characters or less. In *17th ACM Conf. on Computer and communications security (CCS)*, pages 27–37, Chicago, Illinois, Oct 2010. ACM. (Computing). Available from: http://dx.doi.org/10.1145/1866307.1866311.

[132] M. B. Griffiths. Excessive Internet use: Implications for sexual behavior. *CyberPsychology and Behavior*, 3(4):537–552, Aug 2000. (Psychology). Available from: http://dx.doi.org/10.1089/109493100420151.

[133] * E. Groff and L. Mazerolle. Simulated experiments and their potential role in criminology and criminal justice. *J. of Experimental Criminology*, 4(3):187–193, Sep 2008. (Criminology-Simulation). Available from: http://dx.doi.org/10.1007/s11292-008-9058-0.

[134] R. Gross and A. Acquisti. Information revelation and privacy in online social networks. In *ACM Workshop on Privacy in the Electronic Society (WPES)*, pages 71–80, Alexandria, Virginia, Nov 2005. ACM. (Computing-Economics Privacy). Available from: http://dx.doi.org/10.1145/1102199.1102214.

[135] * R. T. Guerette and K. J. Bowers. Assessing the extent of crime displacement and diffusion of benefits: a review of situational crime prevention evaluations. *Criminology*, 47(4):1331–1368, Nov 2009. (Criminology-Crime Science). Available from: http://dx.doi.org/10.1111/j.1745-9125.2009.00177.x.

[136] * L. F. Gunderson. Using data mining and judgment analysis to construct a predictive model of crime. In *7th Int. Conf. on Systems, Man and Cybernetics*, pages 246–250, Yasmine Hammamet, Tunisia, Oct 2002. IEEE. (Computing-Analysis). Available from: http://ieeexplore.ieee.org/arnumber=1175702.

[137] * L. F. Gunderson and D. E. Brown. Using a multi-agent model to predict both physical and cyber criminal activity. In *Int. Conf. on Systems, Man, and Cybernetics*, volume 4, pages 2338–2343, Nashville, Tenessee, Oct 2000. IEEE. (Computing-Simulation). Available from: http://dx.doi.org/10.1109/ICSMC.2000.884340.

[138] W. Haddon Jr. The changing approach to the epidemiology, prevention, and amelioration of trauma: the transition to approaches etiologically rather than descriptively based. *Injury Prevention*, 5(3):231–235, Sep 1999. (Medicine). Available from: http://dx.doi.org/10.1136/ip.5.3.231.

[139] J. A. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman, J. Appelbaum, and E. W. Felten. Lest we remember: cold-boot attacks on encryption keys. *Commun. ACM*, 52(5):91–98, May 2009. (Computing-Forensics). Available from: http://dx.doi.org/10.1145/1506409.1506429.

[140] R. Hasan and W. Yurcik. A statistical analysis of disclosed storage security breaches. In *2nd*

ACM Workshop on Storage Security and Survivability (StorageSS), pages 1–8, Alexandria, Virginia, Oct 2006. ACM. (Computing). Available from: http://dx.doi.org/10.1145/1179559.1179561.

[141] J. J. Heckman. Skill formation and the economics of investing in disadvantaged children. *Science*, 312(5782):1900–1902, 2006. (Economics). Available from: http://dx.doi.org/10.1038/428598a.

[142] J. B. Helfgott. *Criminal Behavior Theories, Typologies and Criminal Justice*. SAGE Publications, 2008. (Criminology). Available from: http://www.sagepub.com/books/Book226655.

[143] C. Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Workshop on New security paradigms (NSPW)*, pages 133–144, Oxford, UK, Sep 2009. ACM. (Computing-Economics Security). Available from: http://dx.doi.org/10.1145/1719030.1719050.

[144] C. Herley and D. Florêncio. A profitless endeavor: phishing as tragedy of the commons. In *Workshop on New security paradigms (NSPW)*, pages 59–70, Lake Tahoe, California, USA, Sep 2008. ACM. (Computing-Phishing). Available from: http://dx.doi.org/10.1145/1595676.1595686.

[145] G. E. Higgins. Can low self-control help with the understanding of the software piracy problem? *Deviant Behavior*, 26(1):1–24, Dec 2004. (Criminology). Available from: http://dx.doi.org/10.1080/01639620490497947.

[146] T. M. Hinnen. The cyber-front in the war on terrorism: curbing terrorist use of the Internet. *The Columbia Science and Technology Law Review*, 5:Article III, 2003. (Law). Available from: http://www.stlr.org/html/volume5/hinnenintro.php.

[147] J. H. Hoepman. Revocable privacy. *ENISA Quarterly Review*, 5(2):16–17, Jun 2009. (Computing).

[148] J. Hofste. Hyves for criminals - A case study showing the privacy risks of social networks. In *12th Twente Student Conference on IT (TSConIT)*, pages A–3, Enschede, Netherlands, Jan 2010. Univ. Of Twente. (Computing). Available from: http://referaat.cs.utwente.nl/new/paper.php?paperID=604.

[149] * C. W. Holsapple, D. Iyengar, H. Jin, and S. Rao. Parameters for software piracy research. *The Information Society*, 24(4):199–218, Jul 2008. (Economics). Available from: http://dx.doi.org/10.1080/01972240802189468.

[150] * T. J. Holt and A. M. Bossler. Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, 30(1):1–25, Jan 2009. (Criminology-Crime Science). Available from: http://dx.doi.org/10.1080/01639620701876577.

[151] * Qing Hu, Zhengchuan Xu, T. Dinev, and Hong Ling. Does deterrence work in reducing information security policy abuse by employees? *Commun. ACM*, 54(6):54–60, Jun 2011. (Computing). Available from: http://dx.doi.org/10.1145/1953122.1953142.

[152] Xin Hu and Z. Morley Mao. Accurate real-time identification of IP prefix hijacking. In *18th IEEE Symp. on Security and Privacy (S&P)*, pages 3–17, Oakland, California, 2007. IEEE. (Computing-IEEE). Available from: http://dx.doi.org/10.1109/SP.2007.7.

[153] * W. Huang and S.-Y. K. Wang. Emerging cybercrime variants in the Socio-Technical space. In S. Dasgupta, editor, *Social Computing: Concepts, Methodologies, Tools, and Applications*, pages 1726–1739. Information Science Reference, IGI Global, Hershey, Pennsylvania, 2010. (Computing-Phishing). Available from: http://www.igi-global.com/Bookstore/Chapter.aspx?TitleId=39819.

[154] P. Hunter. BT's bold pioneering child porn block wins plaudits amid Internet censorship concerns. *Computer Fraud & Security*, 9:4–5, Sep 2004. (Computing). Available from: http://dx.doi.org/10.1016/S1361-3723(04)00109-5.

[155] T. N. Jagatic, M. Johnson, M. Jakobsson, and F. Menczer. Social phishing. *Commun. ACM*, 50(10):94–100, Oct 2007. (Computing-Phishing). Available from: http://dx.doi.org/10.1145/1290958.1290968.

[156] Y. Jewkes and M. Yar. Introduction: the Internet, cybercrime, and the challenges of the 21st century. In Y. Jewkes and M. Yar, editors, *Handbook of Internet Crime*, pages 1–7. Willan Publishing, Cullompton, UK, 2010. (Law). Available from: http://www.willanpublishing.co.uk/cgi-bin/indexer?product=9781843925231.

[157] D. R. Johnson and D. G. Post. Law and borders - the rise of law in cyberspace. *Stanford Law Review*, 48(5):1367–1402, May 1996. (Law). Available from: http://www.jstor.org/stable/1229390.

[158] A. Juels and J. G. Brainard. Client puzzles: A cryptographic countermeasure against connection depletion attacks. In *Network and Distributed System Security Symp. (NDSS)*, page Paper 11, San Diego, California, Feb 1999. The Internet Society. (Computing). Available from: http://www.isoc.org/isoc/conferences/ndss/99/proceedings/papers/juels.pdf.

[159] J. Jung, V. Paxson, A. W. Berger, and H. Balakrishnan. Fast portscan detection using sequential hypothesis testing. In *25th IEEE Symp. on Security and Privacy (S&P)*, pages 211–225, Oakland, California, May 2004. IEEE. (Computing-IEEE). Available from: http://dx.doi.org/10.1109/SECPRI.2004.1301325.

[160] R. Kailar. Reasoning about accountability in protocols for electronic commerce. In *16th IEEE Symp. on Security and Privacy (S&P)*, pages 236–250, Oakland, California, May 1995. IEEE. (Computing-IEEE). Available from: http://dx.doi.org/10.1109/SECPRI.1995.398936.

[161] * T. Kaplankira, J. Mailley, S. Whitehead, and G. Farrell. Mobile phone reprogramming: Its extent and prevention. *Crime Prevention and Community Safety*, 10(4):271–279, Oct 2008. (Criminology-Crime Science). Available from: http://dx.doi.org/10.1057/palgrave.cpcs.8150060.

[162] M. Katoh, K. Ohmae, S. Sonoda, M. Yanagida, and M. Senga. Image processing device and method for identifying an input image, and copier scanner and printer including same. United States Patent and Trademark Office 5,845,008, Dec 1998. (Computing).

[163] E. E. Kenneally and K. Claffy. Dialing privacy and utility: A proposed Data-Sharing framework to advance Internet research. *IEEE Security & Privacy*, 8(4):31–39, July-Aug 2010. (Computing). Available from: http://dx.doi.org/10.1109/MSP.2010.57.

[164] J. Kennedy. *Digital music report 2009: New Business Models for a Changing En vironment.* IFPI, 2009. (Computing-Economics Security). Available from: http://www.ifpi.org/content/library/DMR2009.pdf.

[165] M. Keyser. The council of Europe convention on cybercrime. *J. of transnational law & policy*, 12(2):287–326, Spring 2003. (Law). Available from: http://www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf.

[166] * G. Kitteringham. Lost laptops = lost data: Measuring costs, managing threats. Crisp report, ASIS Int. Foundation, 2008. (Criminology-Crime Science). Available from: http://www.asisonline.org/foundation/lostlaptop.pdf.

[167] P. Knickerbocker, Dongting Yu, and Jun Li. Humboldt: A distributed phishing disruption system. In *4th Annual eCrime Researchers Summit (eCrime)*, page Article 1, Dallas, Texas, Oct 2009. IEEE. (Computing-Phishing). Available from: http://dx.doi.org/10.1109/ECRIME.2009.5342620.

[168] L. Kool and V. Frissen. Rethinking privacy in online environments. In *19th ITS-Europe Regional Conf.*, Rome, Italy, Sep 2008. (Computing).

[169] R. E. Kraut, J. Morris, R. Telang, D. Filer, M. Cronin, and S. Sunder. Markets for attention: will postage for email help? In *Conf. on Computer supported cooperative work (CSW)*, pages 206–215, New Orleans, Louisiana, Nov 2002. ACM. (Computing-Phishing). Available from: http://dx.doi.org/10.1145/587078.587108.

[170] N. Kshetri. The economics of click fraud. *IEEE Security and Privacy*, 8(3):45–54, May 2010. (Computing). Available from: http://dx.doi.org/10.1109/MSP.2010.88.

[171] P. Kumaraguru, J. Cranshaw, A. Acquisti, L. Cranor, J. Hong, M. Blair, and T. Pham. School of phish: a real-word evaluation of anti-phishing training. In *5th Symp. on Usable Privacy and Security (SOUPS)*, page Article 3, Mountain View, California, Jul 2009. ACM. (Computing-Phishing). Available from: http://dx.doi.org/10.1145/1572532.1572536.

[172] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong. Lessons from a real world evaluation of anti-phishing training. In *3rd annual eCrime Researchers Summit (eCrime)*, page Article 6, Atlanta, Georgia, Oct 2008. IEEE. (Computing-Phishing). Available from: http://dx.doi.org/10.1109/ECRIME.2008.4696970.

[173] R. H. Langworthy. *Measuring what matters. Proceedings from the Policing Research Institute meetings.* National Institute of Justice, Office of Community Oriented Policing Services (COPS), Washington, DC, 1999. (Criminology). Available from: http://www.ncjrs.gov/pdffiles1/170610-1.pdf.

[174] * G. Laycock. The UK car theft index: An example of government leverage. In M. G. Maxfield

and R. V. Clarke, editors, *Understanding and Preventing Car Theft*, volume Crime Prevention Studies 17, pages 25–44. Criminal Justice Press, Monsey, New York, 2004. (Criminology-Crime Science). Available from: http://www.popcenter.org/library/CrimePrevention/Volume_17/03_laycock_webb_uk_car_theft.pdf.

[175] * G. Laycock. Defining crime science. In M. J. Smith and N. Tilley, editors, *Crime science: new approaches to preventing and detecting crime*, pages 3–24. Willan Publishing, Uffculme, UK, 2005. (Criminology-Crime Science).

[176] D. Lazer, A. Pentland, L. Adamic, S. Aral, A.-L. Barabási, D. Brewer, N. Christakis, N. Contractor, J. Fowler, M. Gutmann, T. Jebara, G. King, M. Macy, D. Roy, and M. Van Alstyne. Computational social science. *Science*, 323(5915):721–723, Feb 2009. (Criminology-Analysis). Available from: http://dx.doi.org/10.1126/science.1167742.

[177] E. R. Leukfeldt, M. M. L. Domenie, and W. Ph. Stol. Kinderporno. In *Verkenning Cybercrime in Nederland 2009*, pages 139–178. Boom Juridische Uitgevers, Den Haag, 2010. (Law-Cybercrime).

[178] K. Levchenko, A. Pitsillidis, N. Chachra, B. Enright, M. Féelegyháazi, C. Grier, T. Halvorson, C. Kanich, C. Kreibich, He Liu, D. McCoy, N. Weaver, V. Paxson, G. M. Voelker, and S. Savage. Click trajectories: End-to-End analysis of the spam value chain. In *32th IEEE Symp. on Security and Privacy (S&P)*, pages 431–446, Berkely, California, May 2011. IEEE. (Computing-IEEE). Available from: http://dx.doi.org/10.1109/SP.2011.24.

[179] * S. Lin and D. E. Brown. Criminal incident data association using the OLAP technology. In *First NSF/NIJ Symp. Intelligence and Security Informatics (ISI)*, volume 2665 of *LNCS*, pages 13–26, Tucson, Arizona, Jun 2003. Springer. (Computing-Analysis). Available from: http://dx.doi.org/10.1007/3-540-44853-5_2.

[180] * S. Lin and D. E. Brown. An outlier-based data association method for linking criminal incidents. *Decision Support Systems*, 41(3):604–615, Mar 2006. (Computing-Analysis). Available from: http://dx.doi.org/10.1016/j.dss.2004.06.005.

[181] * Tung-Ching Lin, Meng Hsiang Hsu, Feng-Yang Kuo, and Pei-Cheng Sun. An intention model-based study of software piracy. In *32nd Annual Hawaii Int. Conf. on System Sciences (HICSS)*, Maui, Hawaii, Jan 1999. IEEE. (Computing-Cybercrime Science). Available from: http://dx.doi.org/10.1109/HICSS.1999.772932.

[182] A. Litan. *The War on Phishing Is Far From Over*. Gartner Group, Stamford, Connecticut, Apr 2009. (Computing-Phishing). Available from: http://www.gartner.com/DisplayDocument?id=927921.

[183] Gang Liu, Guang Xiang, B. A. Pendleton, Jason I. Hong, and Wenyin Liu. Smartening the crowds: Computational techniques for improving human verification to fight Phishing scams. In *7th Symposium on Usable Privacy and Security (SOUPS)*, page Article 8, Pittsburg, Pennsylvania, Jul 2011. ACM, New York. (Computing). Available from: http://cups.cs.cmu.edu/soups/2011/proceedings/a8_Liu.pdf.

[184] * L. Liu, X. Wang, J. E. Eck, and J. Liang. Simulating crime events and crime patterns in RA/CA model. In F. Wang, editor, *Geographic Information Systems and Crime Analysis*, pages 197–231. Idea Group, London, 2005. (Criminology-Simulation). Available from: http://www.igi-global.com/books/details.asp?ID=4643.

[185] * J. Mailley, R. Garcia, S. Whitehead, and G. Farrell. Phone theft index. *Security J.*, 21(3):212–227, 2008. (Criminology-Crime Science). Available from: http://dx.doi.org/10.1057/palgrave.sj.8350055.

[186] * N. Malleson, A. Heppenstall, and L. See. Crime reduction through simulation: An agent-based model of burglary. *Computers, Environment and Urban Systems*, 34(3):236–250, May 2010. (Computing-Simulation). Available from: http://dx.doi.org/10.1016/j.compenvurbsys.2009.10.005.

[187] A. M. Marshall and B. C. Tompsett. Identity theft in an online world. *Computer Law & Security Report*, 21(2):128–137, 2005. (Computing-Cybercrime). Available from: http://dx.doi.org/10.1016/j.clsr.2005.02.004.

[188] * P. Mayhew, R. V. Clarke, and M. Hough. Steering column locks and car theft. In R. V. Clarke and First, editors, *Situational Crime Prevention: Successful Case Studies*, pages 52–65. Harrow and Heston, Albany, New York, 1992. (Criminology-Crime Science).

[189] B. McCarty. Automated identity theft. *IEEE Security and Privacy*, 1(5):89–92, Sep 2003. (Computing-Economics Security). Available from: http://dx.doi.org/10.1109/MSECP.2003.1236244.

[190] S. McCombie and J. Pieprzyk. Winning the Phishing war: A strategy for Australia. In *2nd Cybercrime and Trustworthy Computing Workshop*, pages 79–86, Ballarat, Victoria Australia, Jul 2010. IEEE. (Computing-Phishing). Available from: http://dx.doi.org/10.1109/CTC.2010.13.

[191] * R. N. McEwen. Tools of the trade: Drugs, law and mobile phones. *Proceedings of the American Society for Information Science and Technology*, 44(1):1–16, 2007. (Computing-MobileLaptop). Available from: http://dx.doi.org/10.1002/meet.1450440231.

[192] P. N. McGrain and J. L. Moore. Pursuing the panderer: An analysis of united states v. williams. *J. of Child Sexual Abuse*, 19(2):190–203, Mar 2010. (Law-Cybercrime). Available from: http://dx.doi.org/10.1080/10538711003622760.

[193] * G. Me and P. Spagnoletti. Situational crime prevention and cyber-crime investigation: The online pedo-pornography case study. In *EUROCON 2005 - The Int. Conf. on Computer as a Tool*, volume II, pages 1064–1067, Belgrade, Serbia, Nov 2005. IEEE. (Computing-Information Security). Available from: http://dx.doi.org/10.1109/EURCON.2005.1630133.

[194] R. T. Mercuri. Scoping identity theft. *Commun. ACM*, 49(5):17–21, May 2006. (Computing-Phishing). Available from: http://dx.doi.org/10.1145/1125944.1125961.

[195] * G. S. Mesch. Parental mediation, online activities, and cyberbullying. *Cyberpsychology and Behavior*, 12(4):387–393, Jul 2009. (Psychology). Available from: http://dx.doi.org/10.1089/cpb.2009.0068.

[196] K. Mitnick, W. L. Simon, and S. Wozniak. *The Art of Deception: Controlling the Human Element of Security.* Wiley, Oct 2002. (Computing). Available from: http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0471237124.html.

[197] T. Moore and R. Anderson. Economics and Internet security: a survey of recent analytical, empirical and behavioral research. In M. Peitz and J. Waldfogel, editors, *Oxford Handbook of the Digital Economy*, page to appear. Oxford University Press, 2011. (Computing-Economics Security).

[198] T. Moore and R. Clayton. Examining the impact of website take-down on Phishing. In *2nd annual eCrime researchers summit (eCrime)*, pages 1–13, Pittsburgh, Pennsylvania, Oct 2007. ACM. (Computing-Phishing). Available from: http://dx.doi.org/10.1145/1299015.1299016.

[199] T. Moore and R. Clayton. The consequence of non-cooperation in the fight against phishing. In *3nd Annual eCrime Researchers Summit (eCrime)*, page Article 4, Atlanta, Georgia, Oct 2008. IEEE. (Computing-Phishing). Available from: http://dx.doi.org/10.1109/ECRIME.2008.4696968.

[200] T. Moore and R. Clayton. The impact of incentives on notice and take-down. In M. E. Johnson, editor, *Managing Information Risk and the Economics of Security*, pages 199–221. Springer, 2009. (Computing-Economics Security). Available from: http://dx.doi.org/10.1007/978-0-387-09762-6_10.

[201] * S. Morris. The future of netcrime now: Part 1 threats and challenges. Online Report 62/04, Home Office, Dec 2004. (Criminology-Cybercrime). Available from: http://www.homeoffice.gov.uk/rds/pdfs04/rdsolr6204.pdf.

[202] * S. Morris. The future of netcrime now: Part 2 responses. Online Report 63/04, Home Office, Dec 2004. (Criminology-Cybercrime). Available from: http://www.homeoffice.gov.uk/rds/pdfs04/rdsolr6304.pdf.

[203] S. J. Murdoch and R. Anderson. Verified by visa and MasterCard SecureCode: Or, how not to design authentication (short paper). In *14th. Int. Conf. on Financial Cryptography and Data Security (FC)*, volume 6052 of *LNCS*, pages 336–342, Tenerife, Canary Islands, Jan 2010. Springer. (Computing). Available from: http://dx.doi.org/10.1007/978-3-642-14577-3_27.

[204] P. G. Neumann. The challenges of insider misuse. Technical Report Prepared for the Workshop on Preventing, Detecting, and Responding to Malicious Insider Misuse 16-18 August 1999, at RAND, Santa Monica, CA, SRI Computer Science Lab, Aug 1999. (Computing-Insider). Available from: http://www.csl.sri.com/neumann/pgn-misuse.html.

[205] * G. R. Newman. Identity theft. Problem-Oriented Guides for Police 25, Office of Community Oriented Policing Services, Jun 2004. (Criminology-Cybercrime). Available from: http://www.cops.usdoj.gov/ric/ResourceDetail.aspx?RID=111.

[206] G. R. Newman. Cybercrime. In M. D. Krohn, A. J. Lizotte, and G. Penly Hall, editors, *Handbook on Crime and Deviance*, pages 551–584. Springer, Nov 2009. (Criminology-Cybercrime).

Available from: http://dx.doi.org/10.1007/978-1-4419-0245-0_25.

[207] * G. R. Newman and R. V. Clarke. *Superhighway Robbery: Preventing E-Commerce Crime (Crime Science)*. Willan Publishing, Uffculme, UK, Aug 2003. (Criminology). Available from: http://www.willanpublishing.co.uk/cgi-bin/indexer?product=1843920182.

[208] Joint Task Force on Computing Curricula IEEE/ACM. *Computing Curricula 2001 – Computer Science*. ACM, Dec 2001. (Computing). Available from: http://www.acm.org/sigcse/cc2001/cc2001.pdf.

[209] M. Osadchy, B. Pinkas, and A. Jarrous. SCiFI - A system for secure face identification. In *B. Moskovich*, pages 239–254, Oakland, California, May 2010. IEEE. (Computing-IEEE). Available from: http://dx.doi.org/10.1109/SP.2010.39.

[210] R. R. Panko and H. G. Beh. Monitoring for pornography and sexual harassment. *Commun. ACM*, 45(1):84–87, Jan 2002. (Law-Cybercrime). Available from: http://dx.doi.org/10.1145/502269.502304.

[211] * R. Pawson and N. Tilley. *Realistic Evaluation*. Sage Publications, 1997. (Sociology). Available from: http://www.sagepub.com/books/Book205276.

[212] H. Pearson. Public health: The demon drink. *Nature*, 428:598–600, Apr 2004. (Medicine). Available from: http://dx.doi.org/10.1038/428598a.

[213] * K. Pease. Crime science. In S. G. Shoham, P. Knepper, and M. Kett, editors, *International Handbook of Criminology*, pages 3–23. CRC Press, Feb 2010. (Criminology-Crime Science). Available from: http://www.crcpress.com/product/isbn/9781420085518.

[214] C. Peek-Asa and C. Zwerling. Role of environmental interventions in injury control and prevention. *Epidemiol Rev*, 25(1):77–89, 2003. (Medicine). Available from: http://dx.doi.org/10.1093/epirev/mxg006.

[215] * M. D. Porter and D. E. Brown. Detecting local regions of change in high-dimensional criminal or terrorist point processes. *Computational Statistics and Data Analysis*, 51(5):2753–2768, Feb 2007. (Computing-Analysis). Available from: http://dx.doi.org/10.1016/j.csda.2006.07.002.

[216] A. S. Rakitianskaia, M. S. Olivier, and A. K. Cooper. Nature and forensic investigation of crime in second life. In *10th Annual Information Security South Africa Conf. (ISSA)*, page to appear, Rosebank, Johannesburg, South Africa, Aug 2011. IEEE. (Computing).

[217] B. W. Reyns. 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, Apr 2010. (Criminology). Available from: http://dx.doi.org/10.1057/cpcs.2009.22.

[218] R. Richardson. *14th Annual CSI/FBI Computer crime and security survey*. Computer Security Institute, San Francisco, California, 2009. (Computing). Available from: http://www.gocsi.com/.

[219] T. Rosati, S. A. Vanstone, and D. R. Brown. Method and system of managing and filtering electronic messages using cryptographic techniques. United States Patent and Trademark Office US20070053510, Mar 2007. (Computing-Phishing).

[220] R. J. Sampson and S. W. Raudenbush. Systematic social observation of public spaces: A new look at disorder in urban neighborhoods. *The American J. of Sociology*, 105(3):603–651, 1999. (Criminology). Available from: http://www.jstor.org/stable/3003843.

[221] B. H. Schell, M. V. Martin, P. C. K. Hung, and L. Rueda. Cyber child pornography: A review paper of the social and legal issues and remedies-and a proposed technological solution. *Aggression and Violent Behavior*, 12(1):45–63, Jan 2007. (Law-Cybercrime). Available from: http://dx.doi.org/10.1016/j.avb.2006.03.003.

[222] R. Schlegel, A. Kapadia, and A. J. Lee. Eyeing your exposure: Quantifying and controlling information sharing for improved privacy. In *7th Symposium on Usable Privacy and Security (SOUPS)*, page Article 14, Pittsburg, Pennsylvania, Jul 2011. ACM, New York. (Computing). Available from: http://cups.cs.cmu.edu/soups/2011/proceedings/a14_Schlegel.pdf.

[223] B. Schneier. The psychology of security. In *1st Int. Conf. on Cryptology in Africa (AfricaCrypt)*, volume 5023 of *LNCS*, pages 50–79, Casablanca, Morocco, Jun 2008. Springer. (Psychology). Available from: http://dx.doi.org/10.1007/978-3-540-68164-9_5.

[224] C. L. Schuba, I. V. Krsul, M. G. Kuhn, E. H. Spafford, A. Sundaram, and D. Zamboni. Analysis of a denial of service attack on TCP. In *18th IEEE Symp. on Security and Privacy (S&P)*, pages 208–223, Oakland, California, May 1997. IEEE. (Computing-IEEE). Available from: http://dx.doi.org/10.1109/SECPRI.1997.601338.

[225] J.-M. Seigneur and C. D. Jensen. Privacy recovery with disposable email addresses. *IEEE Security and Privacy*, 1(6):35–39, Nov 2003. (Computing-Phishing). Available from: http://dx.doi.org/10.1109/MSECP.2003.1253566.

[226] S. Sheng, P. Kumaraguru, A. Acquisti, L. F. Cranor, and J. Hong. Improving phishing countermeasures: An analysis of expert interviews. In *4th annual eCrime Researchers Summit (eCrime)*, page Article 6, Tacoma, Washington, Oct 2009. IEEE. (Computing-Phishing). Available from: http://dx.doi.org/10.1109/ECRIME.2009.5342608.

[227] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. Faith Cranor, J. Hong, and E. Nunge. Anti-Phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In *3rd Symp. on Usable privacy and security (SOUPS)*, pages 88–99, Pittsburgh, Pennsylvania, Jul 2007. ACM. (Computing-Phishing). Available from: http://dx.doi.org/10.1145/1280680.1280692.

[228] J. Shepherd and V. Sivarajasingam. Injury research explains conflicting violence trends. *Injury Prevention*, 11(6):324–325, Dec 2005. (Medicine). Available from: http://dx.doi.org/10.1136/ip.2005.009761.

[229] * M. B. Short, P. J. Brantingham, A. L. Bertozzi, and G. E. Tita. Dissipation and displacement of hotspots in reaction-diffusion models of crime. *Proceedings of the National Academy of Sciences USA (PNAS)*, 107(9):3961–3965, Mar 2010. (Computing-Simulation). Available from: http://dx.doi.org/10.1073/pnas.0910921107.

[230] H. A. Simon. Behavioral model of rational choice. *The Quarterly J. of Economics*, 69(1):99–118, 1955. (Economics). Available from: http://www.jstor.org/stable/info/1884852.

[231] * M. Siponen, A. Vance, and R. Willison. New insights for an old problem: Explaining software piracy through neutralization theory. In *Hawaii Int. Conf. on System Sciences (HICSS)*, Honolulu, Hawaii, Jan 2010. IEEE. (Computing). Available from: http://dx.doi.org/10.1109/HICSS.2010.287.

[232] J. Slay and B. Turnbull. The 802.11 technology gap - case studies in crime. In *IEEE Int. Region 10 Conf. (TENCON)*, page Paper 25, Melbourne, Australia, Nov 2005. IEEE. (Computing-Cybercrime). Available from: http://dx.doi.org/10.1109/TENCON.2005.300890.

[233] C. Soghoian. Legal risks for phishing researchers. In *3rd annual eCrime Researchers Summit (eCrime)*, page Article 7, Atlanta, Georgia, Oct 2008. IEEE. (Law-Phishing). Available from: http://dx.doi.org/10.1109/ECRIME.2008.4696971.

[234] * A. Soro, I. Marcialis, D. Carboni, and G. Paddeu. WebRogue: Rendezvous in a web place. *Int. J. Web Based Communities*, 3(4):448–459, Nov 2007. (Computing). Available from: http://dx.doi.org/10.1504/IJWBC.2007.015869.

[235] F. Stajano and P. Wilson. Understanding scam victims: seven principles for systems security. Technical report UCAM-CL-TR-754, Univ. of Cambridge Computer Laboratory, Sep 2009. (Computing). Available from: http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-754.pdf.

[236] D. Staniford-Chen and L. T. Heberlein. Holding intruders accountable on the Internet. In *16th IEEE Symp. on Security and Privacy (S&P)*, pages 39–49, Oakland, California, May 1995. IEEE. (Computing-IEEE). Available from: http://dx.doi.org/10.1109/SECPRI.1995.398921.

[237] D. Stiliadis, A. Francini, S. Kamat, M. Alicherry, A. Hari, P. V. Koppol, A. K. Gupta, and D. Skuler. Evros: A service-delivery platform for extending security coverage and IT reach. *Bell Labs Technical J.*, 12(3):101–119, Fall 2007. (Computing-MobileLaptop). Available from: http://dx.doi.org/10.1002/bltj.20253.

[238] W. Ph. Stol, H. K. W. Kaspersen, J. Kerstens, E. R. Leukfeldt, and A. R. Lodder. Governmental filtering of websites: The Dutch case. *Computer Law & Security Review*, 25(3):251–262, 2009. (Law-Cybercrime). Available from: http://dx.doi.org/10.1016/j.clsr.2009.03.002.

[239] Weiqing Sun, R. Sekar, G. Poothia, and T. Karandikar. Practical proactive integrity preservation: A basis for malware defense. In *29th IEEE Symp. on Security and Privacy (S&P)*, pages 248–262, Oakland, California, May 2008. IEEE. (Computing-IEEE). Available from: http://dx.doi.org/10.1109/SP.2008.35.

[240] C. Sundt. Information security and the law. *Information Security Technical Report*, 11(1):2–9,

2006. (Computing-Information Security). Available from: http://dx.doi.org/10.1016/j.istr.2005.11.003.

[241] D. Talbot. The Internet is broken. *MIT Technology review*, Dec 2005. (Computing). Available from: http://www.technologyreview.com/InfoTech-Networks/wtr_16051,258,p1.html.

[242] D. Talbot. The fleecing of the avatars. *Technology Review*, 3(1):58–62, Jan 2008. (Computing). Available from: http://www.technologyreview.com/article/16356/.

[243] P. W. Tappan. Who is the criminal? *American Sociological Review*, 12(1):96–102, 1947. (Criminology). Available from: http://www.jstor.org/pss/2086496.

[244] M. Taylor. The EU data retention directive. *Computer Law & Security Report*, 22(4):309–312, 2006. (Law). Available from: http://dx.doi.org/10.1016/j.clsr.2006.05.005.

[245] L. G. Telser. A theory of Self-Enforcing agreements. *The J. of Business*, 53(1):27–44, Jan 1980. (Economics). Available from: http://www.jstor.org/stable/2352355.

[246] V. H. Templeton and D. N. Kirkman. Fraud, vulnerability, and aging: Case studies. *Alzheimer's Care Today*, 8(3):265–277, Jul 2007. (Medicine). Available from: http://dx.doi.org/10.1097/01.ALCAT.0000281875.55721.0f.

[247] R. H. Thaler and C. R. Sunstein. *Nudge: Improving Decisions about Health, Wealth, and Happiness.* Penguin, London, 2009. (Economics). Available from: http://www.nudges.org/.

[248] * M. Theoharidou, S. Kokolakis, M. Karyda, and E. Kiountouzis. The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security*, 24(6):472–484, Sep 2005. (Computing-Insider). Available from: http://dx.doi.org/10.1016/j.cose.2005.05.002.

[249] T. P. Thornberry and M. D. Krohn. The Self-Report method for measuring delinquency and crime. In D. Duffee, editor, *Measurement and Analysis of Crime and Justice*, volume 4, pages 33–84. National Institute of Justice, Washington, DC, 2000. (Criminology). Available from: http://www.ncjrs.gov/criminal_justice2000/vol_4/04b.pdf.

[250] * N. Tilley and G. Laycock. From crime prevention to crime science. In G. Farrell, K. J. Bowers, S. D. Johnson, and M. Townsley, editors, *Imagination for Crime Prevention: Essays in Honour of Ken Pease*, volume 21, pages 19–39. Criminal Justice Press, Monsey, New York, 2007. (Criminology).

[251] Y. A. Timofeeva. Worldwide prescriptive jurisdiction in Internet content controversies: A comparative analysis. *Connecticut J. of Int. Law*, 20:199–222, 2005. (Law). Available from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=637961.

[252] * B. C. Tompsett, A. M. Marshall, and N. C. Semmens. Cyberprofiling: offender profiling and geographic profiling of crime on the Internet. In *Workshop of the 1st Int. Conf. on Security and Privacy for Emerging Areas in Communication Networks*, pages 21–24, Athens, Greece, Sep 2005. IEEE. (Computing-Cybercrime Science). Available from: http://dx.doi.org/10.1109/SECCMW.2005.1588290.

[253] J. Townsend. Price and consumption of tobacco. *British Medical Bulletin*, 52(1):132–142, 1996. (Medicine). Available from: http://bmb.oxfordjournals.org/cgi/content/abstract/52/1/132.

[254] R. E. Tremblay. Developmental origins of disruptive behaviour problems: the 'original sin' hypothesis, epigenetics and their consequences for prevention. *J. of Child Psychology and Psychiatry*, 51(4):341–367, Apr 2010. (Psychology). Available from: http://dx.doi.org/10.1111/j.1469-7610.2010.02211.x.

[255] R. E. Tremblay and C. Japel. Prevention during pregnancy, infancy and the preschool years. In D. P. Farrington and J. W. Coid, editors, *Early prevention of adult antisocial behavior*, pages 205–242. Cambridge University Press., 2004. (Criminology). Available from: http://www.cambridge.org/0521651948.

[256] A. Tversky and D. Kahneman. The framing of decisions and the psychology of choice. *Science*, 211(4481):453–458, 1981. (Psychology). Available from: http://dx.doi.org/10.1126/science.7455683.

[257] A. Ungberg. Protecting privacy through a responsible decryption policy. *Harvard J. of Law and Technology*, 22(2):537–558, Spring 2009. (Law). Available from: http://jolt.law.harvard.edu/articles/pdf/v22/22HarvJLTech537.pdf.

[258] S. Vaidhyanathan. *Copyrights and copywrongs: the rise of intellectual property and how it threatens*

creativity. NYU Press, 2003. (Law). Available from: http://www.nyupress.org/books/Copyrights_and_Copywrongs-products_id-3244.html.

[259] W. M. P. van der Aalst and A. K. A. de Medeiros. Process mining and security: Detecting anomalous process executions and checking process conformance. In N. Busi, R. Gorrieri, and F. Martinelli, editors, *2nd Int. Workshop on Security Issues with Petri Nets and other Computational Models (WISP)*, volume 121, pages 3–21. Electronic Notes in Theoretical Computer Science, 121, Feb 2005. (Computing). Available from: http://dx.doi.org/10.1016/j.entcs.2004.10.013.

[260] M. van Eeten and J. M. Bauer. Emerging threats to Internet security: Incentives, externalities and policy implications. *J. of Contingencies and Crisis Management*, 17(4):221–232, Dec 2009. (Economics). Available from: http://dx.doi.org/10.1111/j.1468-5973.2009.00592.x.

[261] J. van Luttikhuizen and J. Roodnat. *Eindrapport Audit CIOT 2009*. Ministerie van Justitie, Den Haag, Apr 2009. (Law). Available from: http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2010/07/01/eindrapport-audit-ciot-en-omgevingen-2009/eindrapport-audit-ciot-en-omgevingen-2009.pdf.

[262] B. van Schewick and D. Farber. Point/counterpoint network neutrality nuances. *Commun. ACM*, 52(2):31–37, Feb 2009. (Computing). Available from: http://dx.doi.org/10.1145/1461928.1461942.

[263] A. Waksman and S. Sethumadhavan. Tamper evident microprocessors. In *31th IEEE Symp. on Security and Privacy (S&P)*, pages 173–188, Oakland, California, May 2010. IEEE. (Computing-IEEE). Available from: http://dx.doi.org/10.1109/SP.2010.19.

[264] * D. S. Wall. *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press, Jul 2007. (Criminology).

[265] D. S. Wall. Criminalising cyberspace: the rise of the Internet as a 'crime problem'. In Y. Jewkes and M. Yar, editors, *Handbook of Internet Crime*, pages 88–103. Willan Publishing, Cullompton, UK, 2010. (Law). Available from: http://www.willanpublishing.co.uk/cgi-bin/indexer?product=9781843925231.

[266] * X. Wang, L. Liu, and J. E. Eck. Crime simulation using GIS and artificial intelligent agents. In L. Liu and J. E. Eck, editors, *Artificial Crime Analysis Systems: Using Computer Simulations and Geographic Information Systems*, pages 209–225. Information Science Reference, Mar 2008. (Criminology-Simulation). Available from: http://www.igi-pub.com/reference/details.asp?id=7291.

[267] S. D. Warren and L. D. Brandeis. The right to privacy. *Harvard Law Review*, 4(5):193–220, Dec 1890. (Law). Available from: http://www.jstor.org/stable/1321160.

[268] D. Weinshall. Cognitive authentication schemes safe against spyware. In *27th IEEE Symp. on Security and Privacy (S&P)*, pages 295–300, Berkeley, California, May 2006. IEEE. (Computing-IEEE). Available from: http://dx.doi.org/10.1109/SP.2006.10.

[269] M. Weir, S. Aggarwal, B. de Medeiros, and B. Glodek. Password cracking using probabilistic Context-Free grammars. In *30th IEEE Symp. on Security and Privacy (S&P)*, pages 391–405, Berkeley, California, May 2009. IEEE. (Computing-IEEE). Available from: http://dx.doi.org/10.1109/SP.2009.8.

[270] M. Weiser. The computer for the 21st century. *Scientific American*, 265(3):94–104, Sep 1991. (Computing).

[271] S. Whitehead and G. Farrell. Anticipating mobile phone smart wallet crime: Policing and corporate social responsibility. *Policing*, 2(2):210–217, 2008. (Criminology-MobileLaptop). Available from: http://dx.doi.org/10.1093/police/pan024.

[272] * S. Whitehead, J. Feketu, K. Pease, and G. Farrell. Radio frequency identification and crime prevention. *Security J.*, page to appear, 2009. (Criminology-MobileLaptop).

[273] * S. Whitehead, J. Mailley, I. Storer, J. McCardle, G. Torrens, and G. Farrell. IN SAFE HANDS: A review of mobile phone anti-theft designs. *European J. on Crime Policy Research*, 14(1):39–60, 2008. (Criminology-MobileLaptop). Available from: http://dx.doi.org/10.1007/s10610-007-9040-9.

[274] H. Widiger, S. Kubisch, P. Danielis, J. Schulz, D. Timmermann, T. Bahls, and D. Duchow. IPclip: An architecture to restore trust-by-Wire in packet-switched networks. In *33rd IEEE Conf.*

on Local Computer Networks (LCN), pages 312–319, Montréal, Canada, Oct 2008. IEEE. (Computing). Available from: http://dx.doi.org/10.1109/LCN.2008.4664185.

[275] M. Williams. Cybercrime. In F. Brookman, M. Maguire, H. Pierpoint, and T. Bennett, editors, *Handbook on Crime*, pages 191–213. Willan Publishing, Cullompton, UK, 2010. (Law). Available from: http://www.willanpublishing.co.uk/cgi-bin/indexer?product=9781843923718.

[276] * R. Willison. Understanding the offender/environment dynamic for computer crimes: Assessing the feasibility of applying criminological theory to the IS security context. In *37th Hawaii Int. Conf. on System Sciences (HICSS)*, page 70187.1, Big Island, Hawaii, Jan 2004. IEEE. (Computing-Insider). Available from: http://dx.doi.org/10.1109/HICSS.2004.1265446.

[277] * R. Willison. Understanding the offender/environment dynamic for computer crimes. *Information Technology and People*, 19(2):170–186, 2006. (Computing-Insider). Available from: http://dx.doi.org/10.1108/09593840610673810.

[278] * R. Willison. Understanding the perpetration of employee computer crime in the organisational context. *Information and Organization*, 16(4):304–324, 2006. (Computing-Insider). Available from: http://dx.doi.org/10.1016/j.infoandorg.2006.08.001.

[279] * R. Willison and J. Backhouse. Opportunities for computer crime: Considering systems risk from a criminological perspective. *European J. of Information Systems*, 15:403–414, 2006. (Computing-Insider). Available from: http://dx.doi.org/10.1057/palgrave.ejis.3000592.

[280] * R. Willison and M. Siponen. Software piracy: Original insights from a criminological perspective. In *41th Hawaii Int. Conf. on System Sciences (HICSS)*, page paper 266, Waikoloa, Hawaii, Jan 2008. IEEE. (Computing-Insider). Available from: http://dx.doi.org/10.1109/HICSS.2008.407.

[281] * R. Willison and M. Siponen. Overcoming the insider: reducing employee computer crime through situational crime prevention. *Commun. ACM*, 52(9):133–137, Sep 2009. (Computing-Insider). Available from: http://dx.doi.org/10.1145/1562164.1562198.

[282] K. Wittebrood and M. Junger. Trends in violent crime: a comparison between police statistics and victimization surveys. *J. Social Indicators Research*, 59(2):153–173, Aug 2002. (Criminology). Available from: http://dx.doi.org/10.1023/A:1016207225351.

[283] B. Wood. An insider threat model for adversary simulation. In *Research on Mitigating the Insider Threat to Information Systems - #2*, pages 41–48, Arlington, Virginia, Aug 2000. Rand, Santa Monica. (Computing-Insider). Available from: http://www.rand.org/pubs/conf_proceedings/CF163/.

[284] * R. Wortley and L. Mazerolle (Editors). *Environmental Criminology and Crime Analysis.* Willan Publishing, London, Jun 2008. (Criminology). Available from: http://www.willanpublishing.co.uk/cgi-bin/indexer?product=9781843922803.

[285] * Y. Xue and D. E. Brown. Decision based spatial analysis of crime. In *First NSF/NIJ Symp. Intelligence and Security Informatics (ISI)*, volume 2665 of *LNCS*, pages 153–167, Tucson, Arizona, Jun 2003. Springer. (Computing-Analysis). Available from: http://dx.doi.org/10.1007/3-540-44853-5_12.

[286] * Y. Xue and D. E. Brown. Spatial analysis with preference specification of latent decision makers for criminal event prediction. *Decision Support Systems*, 41(3):560–573, Mar 2006. (Computing-Analysis). Available from: http://dx.doi.org/10.1016/j.dss.2004.06.007.

[287] * M. Yar. The novelty of cybercrime : An assessment in light of routine activity theory. *European J. of Criminology*, 2(4):407–427, Oct 2005. (Criminology). Available from: http://dx.doi.org/10.1177/147737080556056.

[288] A. Young and M. Yung. Cryptovirology: extortion-based security threats and countermeasures. In *17th IEEE Symp. on Security and Privacy (S&P)*, pages 129–140, Oakland, California, May 1996. IEEE. (Computing-IEEE). Available from: http://dx.doi.org/10.1109/SECPRI.1996.502676.

[289] K. S. Young. Internet addiction: The emergence of a new clinical disorder. *CyberPsychology & Behavior*, 1(3):237–244, Fall 1998. (Psychology). Available from: http://dx.doi.org/10.1089/cpb.1998.1.237.

[290] Wei Yu, Xinwen Fu, S. Graham, Dong Xuan, and Wei Zhao. DSSS-Based flow marking technique for invisible traceback. In *28th IEEE Symp. on Security and Privacy (S&P)*, pages 18–32, Oakland,

California, May 2007. IEEE. (Computing-IEEE). Available from: http://dx.doi.org/10.1109/SP.2007.14.

[291] Chuan Yue and Haining Wang. Anti-Phishing in offense and defense. In *24th Annual Computer Security Applications Conf. (ACSAC)*, pages 345–354, Anaheim, California, Dec 2008. IEEE. (Computing-Phishing). Available from: http://dx.doi.org/10.1109/ACSAC.2008.32.

[292] A. Zentner. Measuring the effect of file sharing on music purchases. *The J. of Law and Economics*, 49(1):63–90, Apr 2006. (Computing-Economics Security). Available from: http://dx.doi.org/10.1086/501082.

[293] Feng Zhu, S. Carpenter, A. Kulkarni, and S. Kolimi. Reciprocity attacks. In *7th Symposium on Usable Privacy and Security (SOUPS)*, page Article 9, Pittsburg, Pennsylvania, Jul 2011. ACM, New York. (Computing-Psychology). Available from: http://cups.cs.cmu.edu/soups/2011/proceedings/a9_Zhu.pdf.

[294] J. Zhuge, T. Holz, C. Song, J. Guo, X. Han, and W. Zhou. Studying malicious websites and the underground economy on the Chinese web. In M. E. Johnson, editor, *Managing Information Risk and the Economics of Security*, pages 225–244. Springer, 2009. (Computing-Economics Security). Available from: http://dx.doi.org/10.1007/978-0-387-09762-6_11.

Appendices

A On the lack of evaluated practice of Crime Science applied to cyber-crime

Crime Science is an empirical discipline, in which preventive measures are evaluated in practice, with a view to developing useful knowledge about these measures.

After a cursory inspection of the literature in search of evaluated practice of Crime Science applied to cyber-crime we found little. In the following we report on an exhaustive literature search for studies of the effectiveness of cyber-crime prevention.

To illustrate what we have been looking for we give an example of how the effectiveness of crime prevention can be studied.

A Randomized Controlled Trial (RCT) is a study of an intervention (here crime prevention) where the effect of the intervention on an experimental group is compared with a control group that is not subject to the intervention. Farrington et al report on an RCT of measures against shoplifting [100]. Nine shops in the UK were randomly assigned to three experimental conditions that were believed to prevent shoplifting: (1) electronic tagging, (2) store redesign, and (3) a guard, or to (4) a control condition. Shoplifting was measured at pre-test, post-test, and at follow up (6 weeks after post-test). Results showed that electronic tagging led to a decrease in shoplifting that was maintained at follow up (decreases from 30.8% to 4.4% and 17.3% to 5.5% in the two shops). Store redesign leads to a decrease at post-test that was not maintained at follow-up. And having a guard had no effect on shoplifting. In the control shops, shoplifting increased slightly or remained unchanged.

We have conducted an exhaustive search for empirical research of this kind, but to our surprise, little empirical research could be found, and we take this as an indication that Cyber-crime Science is probably terra incognita. To substantiate this claim, we describe the scope of or search in some detail, and we provide possible explanations for the fact that hardly any such research seems to exist. We conclude this section with a call for more empirical evaluation of techniques from information security.

Table 3 lists all the papers cited in this review categorised according to the discipline. The numbers in the second column do not add up due to the presence of the category Recommended.

A.1 Searches

Firstly, we searched all 18 online proceedings in the period 1995 – 2011 of the premier conference in Information Security, i.e. the "Symposium on Security and Privacy" of the Institute for Electrical and Electronics Engineers (IEEE) for evaluated practice. Out of almost 850 online papers, only 17 ([15, 53, 63, 122, 152, 159, 160, 178, 209, 224, 236, 239, 263, 268, 269, 288, 290]) mention the word "crime", in the abstract, motivation section or in the references. We found onle only paper [178] that aims to show that Information Security actually prevents crime. Maybe this is because such papers are out of scope of the conference? We believe that this is not the case. Quoting from http://www.ieee-security.org/ about the Symposium:

> "Papers offer novel research contributions in any aspect of Computer Security or electronic privacy. Papers may represent advances in the theory, design, implementation, analysis, or empirical evaluation of secure systems, either for general use or for specific application domains."

Secondly, we looked in detail at all 111 papers of the Association of Computing Machinery (ACM) Symposium

Category	Papers	Citing Pioneers
Biology	2	0
Computing	138	43
Criminology	64	49
Economics	7	1
Ethics	1	0
Law	23	0
Medicine	8	1
Physics	1	0
Policy	1	0
Psychology	8	1
Sociology	1	1
Recommended	10	3
Total	254	96

Table 3: The papers cited in this review categorised according to the discipline. The category Recommended represents recommended reading.

on Usable Privacy and Security (SOUPS) from the years 2005 – 2011. The idea being that usability research normally focuses on the user aspects of technology, which we imagine would include crime as well. The SOUPS papers can be classified as shown in the Table 4. Only four out of the 111 papers are relatives of Cyber-crime Science. None of the 111 papers refer to the Crime Science literature. Most papers are usability studies of Information Security, which focus on the usefulness of the technology for its user. None of the papers discuss whether the proposed techniques are effective in preventing cyber-crime. However, Appendix B.1 discusses anti-phishing research in detail, showing that the kind of study that we have been looking for is feasible.

Thirdly, we have checked all 27 papers from the AWPG eCrime Researchers summit held in 2006 – 2010. Seven papers [107, 167, 172, 198, 199, 226, 233] were found to be relevant from a Cyber-crime Science perspective, all of which are discussed in Appendix B.1.

Fourthly, we looked for all English language papers in the Computer Science literature that cite the work of one or more of the ten pioneers of Crime Science as mentioned in the introduction. We found 84 such papers in the entire collection of digital libraries maintained by the ACM on `http:www.acm.org/dl/`, the IEEE on `http://ieeexplore.ieee.org/`, and Elsevier on `http://www.scopus.com/` subject area Computing (this includes the Lecture Notes in Computer Science (LNCS) series from Springer). We claim that we have thus captured all of the significant Computer Science literature that can be considered related to Crime Science. Of those 84 papers we discuss the most relevant 24 in this paper. The related work that we do not discuss are applications of general Computer Science techniques (i.e. not Information Security techniques) to problems in Criminology, such as the Geographic Information System (GIS) based analysis of crime data and agent based simulation of crime data. However, we do present a high level review of simulation and analysis of crime data in Appendix D.

Fifthly, we searched the three data bases mentioned above for RCT (including the British spelling Randomised). We found over 1,000 publications, mostly related to Medical Science. Not a single paper reports on crime prevention.

A.2 Analysis

In spite of our efforts we have failed to find documented scientific studies of how Information Security effectively prevents cyber-crime. We offer three reasons why this might be so.

Firstly, let us consider what happens if Information Security is broken. If this happens in the home or a small business, the chances are that the breach will not be noticed. The probability that the breach will be reported to the police is remote. If a breach happens in an organisation with professional Information Security staff, the breach will probably be noticed. The breach may be reported to the management but it will not necessarily be reported to the police. There are three good reasons for this: (1) not all breaches of Information Security constitute a crime, (2) businesses typically prefer to deal with the matter internally, although recent legislation is changing that to some extent, c.f. the US legislation on data breaches [140], and (3) it is often not clear enough what the intention of the offender is to report the offence to the police. For example telephone companies typically shut down the connection used by a fraudulent customer, rather than to report the alleged fraud to the police [20]. The resulting reluctance to report an inci-

Number of papers	Purpose	average number of subjects in case study	Crime Science yes / no
29	no case studies with users	0	no
34	classical usability studies of a new technology	83	no
18	usability studies of various new password technologies (e.g. graphical passwords)	77	no
26	user surveys of various issues (mainly privacy)	164	no
4	teaching people how to avoid Social engineering scams [91, 227, 171, 293]	179	partly

Table 4: An analysis of the related work on phishing from the Crime Science point of view

dent has the consequence that relatively little information on breaches of Information Security is available to researchers, and if there is information, then privacy issues are an impediment to the freedom of the researchers. However, Crime Scientists have encountered similar problems in their study of traditional crime too, with the same privacy issues, and where crime is not always reported either. We propose to use the tools from Crime Science to deal with reluctance to report. The basic idea is that there are a variety of sources (hospitals, housing associations, insurance companies who all record data). The multiplicity of data sources is in some sense even better than just one as sources provide complementary information and have different biases, problems but also different strengths. More importantly one of the important research tools of Crime Science is holding surveys and interviews to collect data that the police (or other relevant sources) do not have.

Secondly, crime prevention falls in the domain of Criminology, whereas Computer Scientists are generally not taught Criminology. For example the joint ACM IEEE curriculum [208] mentions crime but only in an elective on computer crime, which focuses on the technical aspects of computer crime. We have not been able to find an Information Security master program that provides a solid grounding in Criminology. For example course IY5605 computer crime at Royal Holloway `http://www.isg.rhul.ac.uk/node/194/` uses Denning's text book [85] as the main text. Her book offers an encyclopaedic coverage of Information Security, with examples drawn from the authors own experience as an expert witness. The foundation of the book is presented in chapter 2, which describes the "theory of information warfare". This theory is based on ideas from Information Security and is not linked to Criminology.

Thirdly, those Information Security researchers who do try to bridge the gap can fall foul of the legal issues involved. For example Soghian [233] provides a number of examples where Information Security researchers who tried to do empirical research into the relative merits of measures against phishing had problems with the law, see Appendix B.1.5 for details.

In conclusion, we found some work in the literature that suggests how Crime Science methods can be used to prevent cyber-crime, especially on insider threats (See Section 3.1.1) and phishing (See Appendix B.1), but no reports have been found that actually demonstrate a reduction in cyber-crime [264]. We believe that Information Security researchers will be able to make progress in partnership with other disciplines, as has already happened with Law (See Appendix C.2), Economics (See Appendix C.1), and Psychology [223]. We propose that a strong link is developed with Crime Science, and we offer the present paper as a starting point.

Since Crime Science offers a research methodology as well as a number of results that can be applied we make two suggestions for future research. The first suggestion relates to the methodology of Crime Science, and the second suggestion relates to the generic results of Crime Science:

Question 10 *How can we apply the empirical evaluation methods of Crime Science to cyber-crime?*

Studies of displacement of crime and the dissemination of benefits are an essential aspect.

Question 11 *Does Cyber-crime Science require an extension of the set of 25 generic techniques?*

This includes developing a body of evaluated work that tests how effective ideas from Information Security are in preventing cyber-crime.

B Crime Science applied to cyber-crime: three Case studies

The purpose of this section is to show by example how the methods of Crime Science could be used to structure the search for effective cyber-crime prevention methods. In particular the 25 generic techniques can be checked one by one to find appropriate preventive measures. We chose phishing because of its rate of growth [194], its estimated cost [182], and the popularity of the subject amongst Information Security researchers and offenders alike. The first case study focuses on the act of phishing itself, whereas the second case study looks at a particular context for phishing i.e. that of online auction fraud. In the thirs case study we look at the distribution of offensive content, such as (child) pornography.

B.1 Phishing

Before we explain what phishing is, we note that in Information Security the term social engineering means obtaining confidential information by manipulating and/or deceiving people [196]. Phishing is a form of social engineering [155], whereby the offender tries to obtain sensitive information of his targets by masquerading as someone the target trusts. Once the information is obtained, the phisher uses the information for fraudulent purposes. A typical successful phishing attempt may proceed as follows. The phisher buys email addresses in bulk, and then sends a mass mailing to the inbox of potential targets. The phisher pretends that the email is being sent by the helpdesk of the target's bank and asks her to log in to her online banking website. The website is actually a clone created by the phisher of the real banking web site. Once the target has provided her credentials to the cloned web site, the phisher uses the collected credentials to log in to the real online bank and starts emptying the target's bank account. The focus of the case study is on the steps leading to the offender acquiring the credentials. We refer to related work for an analysis of the role of Money Mules [106] and the role of governments and the industry [190] in the process of converting credentials into money.

Phishing is not restricted to online banking; other online services such as online auctions are also heavily attacked.

Raising the level of awareness of potential targets has proved to be somewhat effective against phishing [171]. This has inspired phishers to develop a more effective attack in the form of spear phishing, which uses detailed information about the target or her context to make the scam more convincing. This information is typically collected from blogs, OSN [155] and web search engines.

B.1.1 Is phishing a real problem?

Dhamija et al [86] provide a detailed analysis of why users fall for phishing, claiming that good phishing attacks can fool as many as 90% of the targets. Dodge et al [88] report that spear phishing has a success rate of up to 80%. From a study of 20 non-expert computer users Downs et al [91] claim that people fall victim to phishing attacks because they lack the right mental model of the risks involved in phishing attacks. Obtaining email addresses, cloning web sites, deceiving users, and sending out emails can be automated. Phishers can work anonymously from anywhere in the world, and are therefore hard to catch. This makes phishing a lucrative form of cyber-crime. Gartner group estimates that in 2008 more than 5 million US consumers lost on average 350$ due to phishing scams, and that the number cases is rising, while the average loss is falling [182]. Phishing is thus a real problem.

B.1.2 Is phishing a new problem?

Given that situational crime prevention has thus far been focused on the real world it makes sense to look for information on the prevention of real world scams that are related to phishing. A scam that shares characteristics with phishing is false billing of the bereaved. In this case the offender sends a bill to someone who has recently died. The name and address are obtained from the obituaries in the news papers, and if the invoice appears credible, the bereaved family is likely to pay. False billing and phishing are similar in the sense that the name and address of the target are easily obtained. The actual means by which the offender collects the money is different, but this should not matter if we can prevent the target to fall for the scam. This, after all, is the objective of crime prevention. Thus Phishing is not new, but the degree of automation afforded by computers and the Internet make it a bigger problem than related scams in the real world because the latter cannot be automated. Unfortunately, we have not been able to find effective crime prevention measures to deal with real world phishing.

B.1.3 How could the 25 generic techniques help control phishing?

In this section we will try to use the 25 generic techniques as guidance to look for measures that can prevent against phishing. The idea is to explore the techniques systematically, trying to locate published work on the prevention of phishing where the technique has been applied implicitly. A mismatch can then be taken as an opportunity to develop new anti-phishing measures. We have been able to find published work that addresses 7 of the 25 generic techniques. We discuss each of these 7 below.

Harden target (1) Since phishing is a form of social engineering, target hardening then could be taken as a form of training users to be more vigilant. Several papers have been written on training programs against phishing. The "School of phish" [171] compares to what extent three groups of about 170 participants each fall for phishing scams. The control group received no training, one group was trained once and the last group received training twice. The results suggest that training reduces the likelihood of participants falling for phishing scams. However, even after training the number of participants that fall for phishing scams remains of the order of 20%. The "School of phish" team found that regardless of the demographics all participants are equally likely to fall for phishing. Given that the participants in the experiments are all staff or student at a top university (Carnegie Mellon), it would seem probable that participants selected at random from the population at large would be even more inclined to fall for phishing scams. The "School of phish" study can be taken as an indication that training alone is not going to solve the problem.

The "School of phish" is a well designed experiment in the spirit of Crime Science. The next step would be to investigate whether crime has been reduced or not as a result of the training. This is actually a hard question to answer unless researchers are permitted to commit fraud themselves. The problem here is that for a realistic experiment, one would like the subjects to experience real crime, which, in the case of phishing means to take the subject's money.

Control access to facilities (2) The phisher makes use of four essential facilities to be able to carry out the attack: a bulk email list, mass mailing, the user's inbox, and a fake web site. We discuss some measures to control access to these three facilities.

Bulk email is easily available on the Internet (for as little as a few $ per million addresses); hence it is probably hard to stop phishers from accessing bulk email.

Mass mailings consume resources that can in principle be controlled, for example by using client puzzles [158]. In the context of throttling mass mailings, the sender is required to solve a mathematical puzzle before the recipient is willing to accept the email. This slows the sender down so that mass mailings become impractical. We found one patent application mentioning this possibility [219] but no related work reporting on the effectiveness of such approaches.

An email inbox is easily accessible, but there are various techniques designed to filter out unwanted email. We list some of the more prominent ones below:

- Spam filters are able to stop a percentage of Spam but it is fundamentally impossible to stop all Spam without also filtering out some desirable mail [125]. Spammers also leverage OSN such as Facebook [112] and Twitter [131] to make the spam look more convincing and harder to filter.
- Making the sender pay for each email will discourage offenders to send millions of spam messages, but it is not easy to enforce payment [169].
- Signed email is in principle easier to filter, as the recipient can verify the signature. To rid herself from Spam, a user could insist that all incoming email is digitally signed. Unfortunately, there are problems with signed email too. Firstly, phishers are likely to be the first to adopt signed email [22]. Secondly only well trained users can verify digital signatures [113]. Thirdly, requiring all emails to be signed curtails the freedom of speech [22].
- Reputation based filtering could in principle be use to filter email from sources with a low reputation [83]. This has proved to be an effective method to reduce fraud in online auctions [64], but no related work has been found that applies these ideas to the prevention of phishing.

A fake web site is set up by the offender to look like the web site that the user trusts (i.e. his online banking web site). The phisher then obtains the user's credentials through the web form provided on the fake web site. Google, Microsoft and others maintain black lists of such fake web sites, so that users can be advised not to visit such a site. However, maintaining a black list is time consuming. Liu et al. [183] present an interesting idea where crowd sourcing techniques are used to source sufficient manual labour to keep a black list up to date.

While attempts have been made, it appears to be difficult to protect the user's inbox. This leads to the following suggestion for future research:

Question 12 *Is there a way in which the user's inbox can be protected from unwanted email that does not destroy the advantages of email?*

Natural surveillance (7) Some OSN and related services such as online video and photo sites provide a "report abuse" control [153]. This makes it easier for users to report undesirable content or behaviour than it is to report abuse in the real world. We believe that similar controls could also help to reduce the phishing problem. For example a "report phishing" button could be installed on the email client, which ensures that the alleged phishing email is brought to the attention of the proper authorities (i.e. the ISP) before deleting it from the inbox of the user.

Reduce anonymity (8) Phishers can easily flood the user's inbox, thus essentially mounting a kind of Denial of Service attack on the user. Denial of Service is perhaps not such a problem in the case of phishing but it certainly is a problem in the Internet in general. Interestingly in real life "denial of service" occurs too. For example it is possible to ruin the business of a restaurant by making reservations and then not showing up. Restaurants can protect their business by reducing anonymity [66]. For example a reservation is not accepted unless accompanied by a valid credit card number, which will be charged if the customer does not show up. This leads to the following suggestion for future research:

Question 13 *Would it be possible to prevent denial of service attacks in the Internet by asking for a payment guarantee?*

Formal surveillance (10) As already indicated at the beginning of this section, one of the main differences between cyber-crime and traditional crime is that cyber-space provides better opportunities for surveillance. While extensive monitoring could have implications for the privacy of online users it is already a standard tool in areas of traditional crime fighting, such as analysing credit card and telephone fraud [20]. Monitoring can also be used to fight cyber-crime, for example by gathering offender profiles [252], by analysing the social structure of offender demography [61], or by analysing transactions in Second Life [242]. This leads to the following suggestion for future research:

Question 14 *How could monitoring of Internet activity reduce the threat of phishing?*

Conceal targets (11) An email address is not a secret so whatever a user does to keep an email address private, sooner or later it will end up in the hands of the phishers. Using a Disposable Email Address (DEA) would allow the target to conceal her email address, and thus to conceal the target of attack. Unfortunately, current DEA systems are not able to hide completely that a user has multiple email addresses [225], thus making it inconvenient to use a DEA system.

Instead of trying to conceal the target's email address it is also possible to conceal the target's credentials (i.e. usernames, passwords and other identifying information) once the target has disclosed them to the phisher. This idea has been explored by Gajek et al [110] and separately by Yue and Wang [291], who propose to pollute the database of the phishers with false credentials. Since the phisher does not know which credentials are false, he runs the risk of being caught if he uses a false credential. Gajek et al nor Yue and Wang have evaluated their proposals; hence we do not know how effective polluting the phishers data base is in reducing crime. This leads to the following suggestion for future research:

Question 15 *How effective is it to pollute the phishers data base?*

Post instructions (22) If Gajek et al [110] had framed their work in terms of Crime Science; they might have noticed that advertising the fact that active measures against phishing are taken could be an effective prevention.

B.1.4 How to avoid phishing scams?

Finally we would like to summarise the advice on what users can do right now to avoid phishing scams as given by Downs et al [91]:

- Ignore any email asking to update personal info;
- Ignore any email threatening to close your bank account;
- Ignore any email from a bank that is not yours;
- Ignore any email with spelling and/or grammatical errors;
- Ignore a Uniform Resource Locator (URL) with an IP address such as `http://12.34.56.68/Bank/`;
- Check a URL using Google before clicking on it;
- Type the URL yourself, do not click on it.

Taking the advice above seriously will cost users time, which, if it prevents a specific user from being victimized may well be worth the effort at an individual level. However, if we take into account the total effort of the population at large to follow the advice, as compared to the expected reduction in crime, the advice makes less sense at an aggregate level [143].

The recent introduction of the 3-D Secure protocol by the credit card companies unfortunately asks users to click on links that they cannot check, thus confusing the users who are already bewildered [203].

B.1.5 Anti-phishing research is hard

Anti-phishing research is not easy because of the legal and ethical issues that are involved in such research. The legal issues involved [233] include:

- Extracting significant amounts of information needed for research from an OSN violates their terms of service;
- Copyright law prohibits the cloning of web sites;
- Confusing trademarks damages the good name of target;

- Phishing is illegal in California.

The ethical problem at the heart of anti-phishing research is the fact that realistic experiments often do not treat participants in a study in accordance with the rules of university ethical committees. For example, Jagatic et al [155] report on a simple experiment whereby researchers send spear-phishing emails to unsuspecting colleagues and students. On the one hand the validity of the experiment is probably diminished if the subjects are briefed about an impending phishing attack. On the other hand a fully briefed subject does not act as he/she normally would. We see this as a challenge for a multidisciplinary research team [105]:

Question 16 *How to design phishing experiments that are ethically acceptable, legally justified, and empirically sound?*

Summarising there are approaches to curtail phishing, but there are probably more opportunities for new preventive measures. We have been able to classify highly cited related work (32 out of 368 papers from `http://www.scopus.com/`) on phishing using only 8 of the 25 generic techniques. We expect some of the other 17 techniques to be applicable to the phishing problem, and we also expect that framing the technical measures in terms of Crime Science is likely to bring important additional benefits in terms of measuring the effectiveness of preventive measures.

This case study on the relationship between anti-phishing research and Crime Science has hopefully convinced the reader that the Crime Science perspective leads to new ideas for effective crime prevention. Using the 25 generic techniques to structure the discussions has the two important benefits: (1) The structuring provided by the 25 generic techniques classifies the literature. (2) The fact that little or no literature has been found for some of the techniques indicates that there might by further opportunities for effective crime prevention. We suggest by way of future research:

Question 17 *To what extent do the 25 generic techniques apply to the specific cyber-crime of phishing?*

B.2 On-line Auction Fraud

As we have seen in the previous section, Crime Science provides a number of techniques that can be used to combat phishing. However, to be even more effective it pays off to include also the context of phishing into the Crime Science approach. Therefore we will present as a second case study a typical online fraud scenario where phishing is one of the tools of the offender.

The underground economy consists of a market place of buyers and sellers of all manner of purloined information, such as an attack that has just been discovered, but for which no defence is available yet (zero-day attack), a email list, a collection of credit card data, a list of credentials for an online auction or an online bank, the name and address of someone who is prepared to receive and reship goods in exchange for a fee (reshipper) etc.

The following crime scenario is a simplified but we believe realistic version of on-line auction fraud, where the offender (Otto) impersonates one target (Tina) on an on-line auction, while paying with the stolen credit card of another target (Chris). Otto requires the services of his dubious pawn broker Perry.

The idea of the scenario is to involve as many jurisdictions as possible, which makes it so challenging for the legal system to cope, that without sophisticated technology this crime is difficult to prevent. There are ten actors involved in the scenario, all from different countries with the exception of Otto and Perry, who live in the same area.

Three actors are plainly dishonest:

- Otto is the offender.
- Perry is a pawnbroker who has been known to be involved in fencing.
- Sam is the on-line supplier of false credentials, stolen credit card information etc.

One actor, Vera, is honest in the sense that she does not actually do anything illegal, but at the same time her services would not be required by honest Internet users.

- Vera is the underground verification service which Otto can ask whether actors like Sam can be trusted to do business with. Otto needs service providers like Vera because he does not want to be cheated by a partner in crime.

The remaining six actors are honest:

- Alice is an on-line auction service used by Otto to buy goods.
- Dave is a drop box for parcels (e.g. a PO box).
- Max is a merchant who sells expensive, tangible goods at on-line auctions.
- Rachel is a shipping agent, who for a fee receives parcels on behalf of her clients and re-ships them to a drop box as instructed by her client.
- Tina is the first target of Otto's crime; her username and password for on-line auction Alice are stolen by Otto.
- Chris is the second target of Otto's crime; his credit card details are fenced by Sam.

The scenario proceeds in ten steps as illustrated in Figure 1 (some details have been omitted):

1. Otto asks Vera if Sam can be trusted. Vera confirms this.
2. Otto goes shopping at Sam's and buys (a) some new malware, (b) a list of millions of email addresses, and (c) a credit card number that has been stolen from Chris.
3. Otto sends a job advert to all emails on the list he bought from Sam asking for a re-shipper who will be paid handsomely for each package shipped. Rachel accepts the job. Otto instructs Rachel to reship all goods she receives to drop box Dave.
4. Otto sends an email with a malware attachment to all the emails on the list he bought from Sam. Tina opens the attachment, and as a result of her naivety, her user name and password for on-line auction Alice are sent back to Otto.
5. Otto logs in to the online auction Alice using Tina's credentials, and purchases expensive goods from Max.
6. Otto uses Chris' credit card to pay Max for the goods.
7. Max ships the goods to Rachel, as requested by Otto.
8. Rachel receives the goods from Max and sends them on to Dave as instructed by Otto.
9. Otto picks up the goods from Dave, and takes them to Perry.
10. Perry pays Otto.

Figure 1 shows the 10 actors and the 10 steps of the transactions described above.

B.2.1 Using the 25 techniques against on-line auction fraud

There are opportunities to disrupt a complex transaction such as Otto's crime. We revisit the ten steps and, inspired by the 25 techniques, we suggest one possible preventive approach for each of the steps:

1. Subvert the verification service, e.g. by poisoning it with false information. This would make it hard for Otto to find partners in crime that will not cheat him. This is an instance of control tools (5).
2. Police the Internet to detect on-line suppliers of stolen information. This is an instance of strengthening formal surveillance (10).
3. Train Internet users like Rachel to warn her against offers of easy jobs and easy money. This is an instance of remove targets (11).
4. Train Internet users like Tina not to click on dubious attachments. Again an instance of remove targets (11).
5. Improve the analysis of the transactions conducted by on-line auctions like Alice to spot unusual behaviour. Otto would presumably buy more goods than honest buyers, making his behaviour suspect. This is an instance of screen exits (3).
6. Implement checks on stolen credit card numbers faster than at present to make it harder for Otto to pay for his goods. This is an instance of target hardening (1).
7. Mark goods inconspicuously, so that when a crime has been discovered it is easier to track the origin of the goods. This is an instance of identify property (13).
8. Introduce regular spot checks on the contents of drop boxes. This is an instance of extend guardianship (6).
9. Place pawn brokers under surveillance to make it harder for Otto to fence the goods. This is an instance of disrupt markets (14).
10. Could the inland revenue service investigate unexpected accumulation of wealth? This is an instance of alert conscience (23).

Question 18 *Which of the suggestions above has the highest potential?*

We conclude the online auction fraud case study by summarising some related work.

Franklin et al [108] were the first to analyse the public data that is visible in an English speaking part of the Internet services that support the underground economy. Their results indicate that specialist service providers are advertising their wares, including services as provided by Sam and Vera in our crime scenario above. Franklin et al suggest a number of low cost attacks to disrupt the market, either by discrediting the buyers and sellers, or by disabling the system that verifies the trustworthiness of the buyers and sellers. Zhuge et al [294] analyse the Chinese underground economy, which works in a similar fashion, except that instead of using IRC channels, the Chinese underground economy uses bulletin boards for communication.

To conclude a successful deal, Otto has to invest time and money, and he has to face competition from other offenders. Contrary to popular belief, Otto will not get

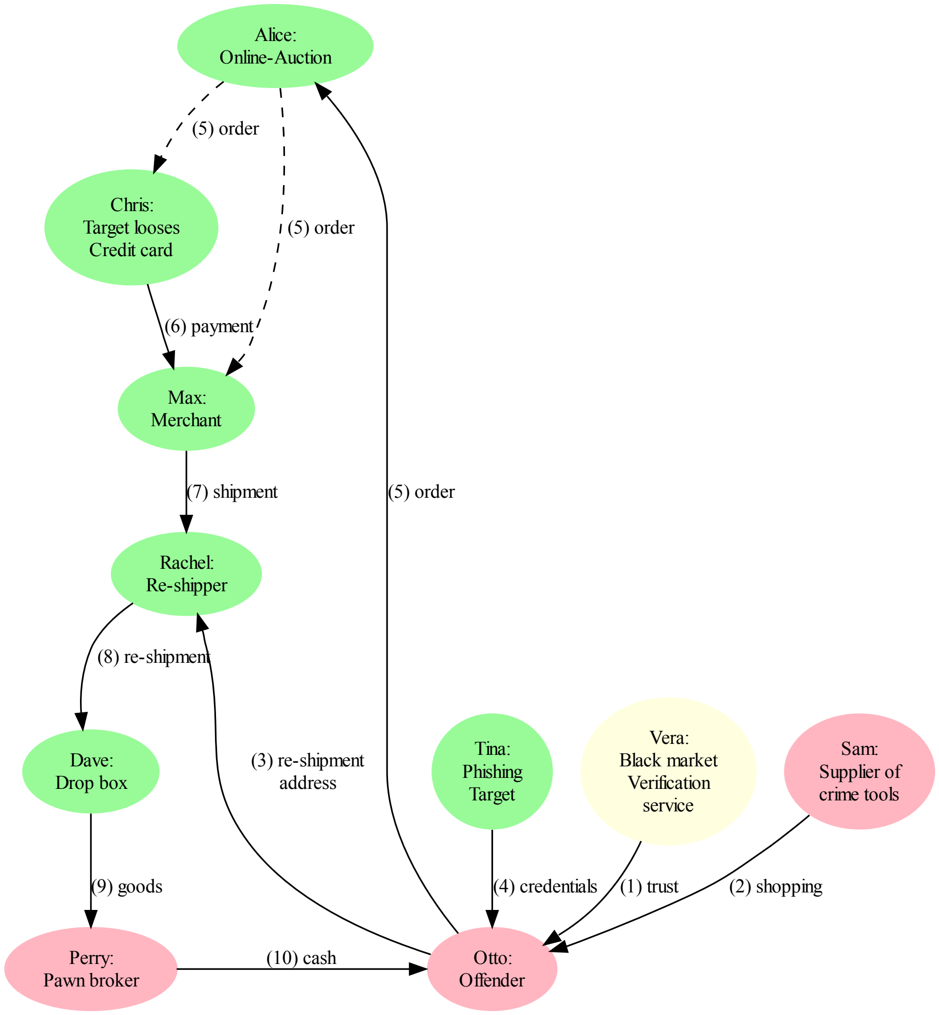

Figure 1: The ten steps of the on-line auction fraud. The two immediate consequences of step (5) have been indicated by dashed arrows.

rich fast. Herley and Florencio argue that Otto and his cronies, who are all trying to deplete the same finite amount of dollars, suffer from the tragedy of the commons [144].

Summarising, there appear to be several opportunities for new preventive measures against online-fraud. Each of the opportunities could be investigated, but there is also a more fundamental issue:

Question 19 *How to decide which of the 25 techniques have the highest potential?*

B.3 Offensive content

People have been trading offensive content, in particularly (child) pornography since time immemorial but current technologies such as the Internet, and digital computers are such powerful tools in the hands of the offenders that the trade and distribution of offensive content is more convenient than ever:

- The Internet is based on the end-to-end argument [241], which stipulates that all the intelligence should be at the end points of the network. The network is neutral in that it simply passes information from end-point to end-point at the highest possible bandwidth and the lowest possible latency. The network thus does not contain intelligence that can be used to filter out offensive material.
- Offensive material itself is stored and transmitted in digital form, which allows perfect copies at low cost. All previous technologies, such as the printing press, and photo copying were more costly and suffered from quality loss.

So what can be done to filter offensive material? We present a brief survey of the state-of-the-art, classifying the various approaches in terms of the 25 techniques, and indicating which avenues of research seem most promising.

B.3.1 Blocking web sites has had limited success

BT in England was the first ISP in the world to introduce a system to block offensive material [154]. The system searches a given URL in a black list, and if the web address is found, the user gets the message "File not found", so it looks like the URL does not exist. The blacklist is hand made by the Internet Watch Foundation (`http://www.iwf.org.uk/`), based on reports from police and the public. It is not difficult to circumvent this technology, for example by storing the content on a peer to peer system such as Kazaa [177]. The fact that a web address is on the black list will soon become known so that the owners of the Web site can move to another web address that is not on the black list. Despite the limitations, BT has been able to block many requests for offensive material. Black lists are an instance of control facilitators, technique 5.

B.3.2 Internet filters can be a threat to the freedom of expression

There are other technical ways to block offensive content, such as blocking IP addresses, or blocking web sites if certain words occur, such as "pre-teen". The major drawback of these (and other) methods is that usually also access to legitimate Web sites is blocked. In the jargon this is called "over blocking", which is tantamount to reducing the freedom of expression [238]. Clayton provides a detailed description of the technical details involved [74] and also shows what measures can be taken to get around blocking on URL or IP addresses.

B.3.3 Scope creep

Another problem with blocking URLs or IP addresses is "scope creep", which instead of just blocking offensive content causes other content to be blocked as well. This basically introduces censorship on the Internet.

B.3.4 The ISP should play a pro-active role

It is inevitable that ISPs should play a major role in the fight against offensive content because the ISP only knows who its customers are. This means that if there is evidence that offensive content is spread by a customer of the ISP, the ISP has to ensure that the distribution stops, usually by means of a "Notice and Takedown" (NTD) order [200]. This is a problem for a number of reasons for the ISP. First NTD requires the ISP to take action against a valued, paying customer, which is against the business interest of the ISP. Secondly, if the NTD is not justified, then the customer can sue the ISP for misconduct. Thirdly, to be sure that the NTD is justified it can take weeks to months before an NTD was performed [200].

There is also a technical argument why the ISP should play the leading role in the fight against PIPs. According to Döring [90] about 1% of all information on the Internet is offensive content (pornography). Part of this is easy to find, but the more serious forms of offensive content (child pornography) is difficult to find. See Leukefeldt et al p 146 and 147 [177] for an action plan to find PIPs. The ISP is the only party who has a chance to see the material, either when it is in transit to or from its customer. If the material is encrypted, then even the ISP will not be able to block it, although there may still be meta-data associated with the content that allow the ISP to take action.

The role of the ISP in the fight against offensive content is a form of Formal surveillance, technique 10.

B.3.5 Internet policing is teamwork

Offensive content in general and (child) pornography in particular is worth billions of dollars annually [221], which is considerably more that the millions that are spent combating offensive content. This means that the offensive content industry is a formidable opponent, and that the fight against offensive content can only succeed through good cooperation [45]. This requires not only a close collaboration between ISPs, police and judiciary, but ISPs will also need to work together [192]. Besides the commercial ISPs, also the IT departments of large organizations, such as companies, government agencies, schools and universities that act as an "internal" ISP for their employees and students must be involved. The incentive for the organisations to empower the "internal" ISP is that no employer or school would like to be exposed as harbouring offensive content [210].

B.3.6 Unreliable ISPs

As expected, there are rogue ISPs, who offer a "bullet proof" service [59]. In practice this means among other things that an NTD is ignored, so that the distribution of offensive content may proceed unhindered. International cooperation has removed some rogue ISPs (i.c. the San Jose based McColo in 2008), but given the large number of commercial ISPs in the world (an estimated 10,000 in 2002 [146]), there will always remain unreliable ISPs.

B.3.7 What does the industry do?

There are several products on the market that can be used to filter offensive content. Microsoft has teamed up with the Canadian police, to build the "Child Exploitation Tracking System" (CETS) [221], but more information on this is hard to find. Digital cameras make it possible to determine which picture was taken with the camera [116]. Some more expensive cameras add a digital watermark to the images, which, for example press photographers use to prove that they have made a picture (because of copyright claims). Cheap digital cameras contain quite a few production flaws that are unique to the camera, and can thus be used to identify it also [116]. Unfortunately, these techniques are only useful for detecting photos if the police have the cameras with which the photos have been made.

Tagging photos with the identity of the camera is a form of Identify property, technique 13.

Summarising, the production and distribution of offensive content is greatly facilitated by modern technology. A small number of the 25 techniques have been deployed in the fight against offensive content, with limited success.

C Economics and Law support Information Security as well as Crime Science

Crime Science requires close cooperation of researchers, designers, and practitioners to analyse the problem, then to design and implement solutions, and finally to evaluate the effectiveness of the solutions in a scientific manner. Crime Science is therefore by definition a multidisciplinary field of study, where the Humanities, the Social Sciences, and the Technical Sciences cooperate [118] in "Thinking Thief" [111]. In this section we present two related disciplines in some detail. Firstly we review the state of the art in the Economics of Information Security and Privacy, to illustrate how one element in particular of the conceptual framework of Crime Science, i.e. RCP applies to Information Security. Secondly we will summarise the effects the rise of cyber-crime as promoted by the Internet has had on the Law, focusing on the deterrent effect of the Law.

C.1 Economics

There is evidence in the literature that theories from Economics can be used to explain aspects of crime. For example Simon's Theory of Bounded Rationality [230] underpins RCP that we discussed earlier, and Ehrlich's Theory of Participation [95] explains how law enforcement can have a deterrent effect. It would be impossible to do justice here to even the tip of the iceberg of the Economics literature that applies to crime. On the other hand since economic thinking is so fundamental to human activity we felt that we could not ignore Economics completely in our discussion on the relation between Information Security and Crime Science. Therefore we will review briefly the work of two prominent researchers in the area, which are Ross Anderson who works on the Economics of Information Security, and Alessandro Acquisti who works on the Economics of Privacy. This section will be concluded by a list of suggestions for further research.

C.1.1 Economics of Information Security

Anderson [8, 11] argues that some of the failures of Information Security are due to perverse incentives that can be explained using economic theories, which are in essence based on the Rational Choice perspective. We discuss two prominent failures by way of example here: Distributed Denial of Service (DDoS) attacks and Music piracy. We conclude by referring to an idea from economic theory to prevent cyber-crime.

To explain the Economics of a DDoS attack, consider the "tragedy of the commons", which is set in medieval England. Since there is plenty of grass on common land, adding a new animal to the flock of sheep creates benefits to the owner of the new animal without noticeably disadvantaging any of the owners of the sheep already grazing on the common. However, as soon as there are too many sheep, the common land turns into a dust bowl, thus causing a problem to all commoners. Only regulation by the village headman can prevent the dust bowl from occurring. Returning to the Internet age, we all find it beneficial to hook up another computer to the Internet, giving all the benefits of Internet access to the user of the new computer. As long as the user can access the Internet, he may be tempted to save the time and money necessary to keep his software, anti virus data base, and firewall up to date. The more out-of-date his PC becomes the more likely it is that it will be hijacked and become part of a BotNet. If the BotNet grows large enough, it can be used to take out any number of prominent web sites by a DDoS attack, thus creating the Internet equivalent of the dust bowl. Unfortunately, there is no village head man who can regulate the global Internet, so the question then becomes: can we still think of incentives for PC owners to make them more difficult to hijack? Could there be a role for the ISP [10]? More generally the question is:

Question 20 *Which economic arguments could be effective in reducing DDoS attacks?*

Botnets are a serious and growing problem, reliable estimates put the number of hijacked PCs at about 10% [260]. Much research remains to be done to tackle this issue, and economic arguments will play an important role.

To explain the Economics of music piracy, Anderson observes that technology, and thus also Information Security, deals with products that have a high fixed but low marginal cost. For example it is expensive to create a new chip, software, movie, or piece of music, but manufacturing such products in quantity is relatively cheap. In the case of software and content, which are basically bits, the manufacturing costs (i.e. basically copying the bits from one medium to another) are close to zero. As a result some technological products are pirated. To assess the scale of the problem, some authors have used economic models to investigate the effects of piracy on the profitability of technology companies. There are two counteracting effects: one that raises sales and another that reduces sales. Bhattacharjee et al [25] argue that music piracy might actually raise sales of digital music. The reasoning is as follows. First, the pirate manages to draw the attention of a music fan to a particular song, thus reducing advertising costs to the legal owner. Second, once the fan discovers that the pirated copy is of low quality (which is often the case with pirated content), she may in the end purchase a legal copy. The statistics published by the music industry on the other hand show a fall of music sales over the past decade [164], which is generally attributed to piracy [292].

Investigating the scale of the piracy problem is one thing, investigating what can be done to prevent the problem is yet another. Also here, economic theories can help. For example, using Buchanan's economic theory of clubs [54], Gopal and Sanders [127] assert that deterrent controls (such as the situational crime prevention principle increase risks) are capable of raising the profitability of a technological product, whereas preventive controls (such as the situational crime prevention principle increase the effort) cannot. The reasoning hinges on the fact that deterrent controls reduce the number of customers of a pirate (the larger the club the more likely it is that it will be discovered and shut down), which in turn increases the fixed cost to the pirate. Since the marginal cost is close to zero, the scale of the piracy problem can be reduced only by playing on the fixed cost. Piracy of technological goods is rife today; hence much research remains to be done to solve the problem:

Question 21 *Which economic arguments could be effective in reducing piracy?*

A good starting point for this research would be the work of Holsapple et al [149], who provide a comprehensive review of the related work on software piracy from a Crime Science perspective.

Economic theory is not only useful to explain cybercrime, but it provides ideas for solutions too. Self enforcing protocols [245] is such an idea: make it in the interest of all parties engaging in transactions to remain honest. An example from Bruce Schneier's August 2009 Cryptogram is as follows. We quote:

"The homeowner decides the value of the property and calculates the resultant tax, and the government can either accept the tax or buy the home for that price."

Self-enforcing protocols already exist when using computers and the Internet for an opinion poll (Online Polling) [124] and using computers and the Internet for casting and counting votes in elections (Online Voting) [56]. Self enforcement is not a solution to all problems as the fundamental motivation to keep the parties in a self enforcement protocol honest is that none of the parties should know when the protocol finishes [245].

C.1.2 Economics of Information Privacy

Like Information Security, information privacy can be explained partially by economic theories. However, the nature of the economic theories is different from those applied to Information Security. To see why this is so, let us first assume that privacy is defined as "the right to be left alone" [267]. Using this definition, Berendt et al [23] interview online users about their privacy preferences and behaviour. The conclusion of the study is that online users do not often act in accordance with their stated preferences. Studies in the real world have come to the same conclusion [130]. The study by Zhu et al [293] investigates to what extent the reciprocity norm explains why people give up privacy.

Acquisti asserts that behavioural economic theories are able to explain our slightly irrational attitudes towards privacy [2]. Let us explore first why classical economic theories, which basically state that “privacy is a tradeoff between the benefits and costs of sharing and hiding information” fail. First of all, the benefits of sharing are real, and often lead to instant gratification. For example, in the real world, consumers may subscribe to a loyalty program with their supermarket. Thus the supermarket knows what consumers buy and offers in exchange a discount on selected purchases. The instant gratification of the discount outweighs the potential disadvantages of a complete shopping profile ending up in the hands of the supermarket or their business partners [130]. In the online world, we see similar phenomena. For example participants in OSN willingly enter a large [134] amount of private information, including photographs and personal details in exchange for popularity, or even notoriety [2]. The information that can be gleaned from an OSN is not limited to cyber crime. For example one of our students has shown how to use the information to burgle residential properties [148]. The disadvantages of profiles ending up in the hands of the service provider, and any one else who pays the service provider (such as a future employer) for the information is largely ignored until it is too late [168].

If users are asked to pay for privacy (rather than to get paid for giving up privacy) the results are even more dramatic. Anonymising services have been deployed over the years, requiring payment and support (for instance to generate cover traffic) by the users. Such services have not done well, simply because the immediate costs are too difficult to balance against the long run benefits [3]. As a result of all this, the market of privacy conscious individuals is relatively small [1].

The conclusion is that behavioural economic theories are called for, such as “soft paternalism”, which gently nudge [247] people in the right direction when faced with an important decision. A good example is a prompted choice for the browser to be installed on a PC, which forces the user to select a browser, rather than to accept a default. A suggested research question would be:

Question 22 *Given that people at some stage regret that they have disclosed private information, would it be possible to remove that information?*

Since we have only scratched the surface of such a vast field as Economics, even in relation to Information Security and Privacy, we cannot offer firm conclusions. Instead we suggest to:

Approach 23 *Use economic methods in the study of cyber-crime*

C.2 Law

New technology has always provided new challenges for the Law. For example the introduction of the motor car gave us joy riding, and the introduction of the telephone gave us obscene calls. The Law continually adapts to face new forms of crime, and as such has been able to deal effectively with technology induced crime [42]. However, the Law cannot be changed abruptly, as law reflects the values of society. Presently, the Law has not adapted sufficiently to cope effectively with the variety of cyber-crime that the information revolution and in particular the rise of the Internet has given us [275]. This reduces the deterrent capability of the Law (as well as the corrective capability, which is beyond the scope of the paper. We will explore the reduced deterrent capability of the Law first) by analysing the differences between traditional crime and cyber-crime from a legal perspective. Then we will summarise a number of, sometimes far reaching proposals from the literature to update the law so that it will be able to deal with cyber-crime.

C.2.1 Differences between Crime and Cyber-crime

At present crime and cyber-crime differ in significant ways, creating a number of challenges for the Law. We list those challenges first, focusing on opportunities for new technology to come to the assistance of the Law.

Some forms of cyber-crime appear to have no pendant in traditional crime. Computers can be used as an instrument of non-traditional crime in such a way that some aspects of the crime are no longer covered by the Law. We give three examples. Firstly, if a computer is used to steal intangible property by making a perfect copy of the original, the original is still with its owner, and the latter may not even notice that a copy has been made. With traditional theft this is not possible; hence any provision in the law that requires the owner to have been permanently deprived of the object no longer applies. This, however, is a standard provision in legal systems.

Secondly, denial of service is a social harm that does not fit any of the categories of traditional offences, in particular denial of service is not stealing as neither the client nor the service provider are actually deprived of anything other than time [43].

Thirdly, several countries, including the US and Canada, have enacted legislation that declares virtual child pornography illegal on the grounds that with modern technology realistic images can be produced that are almost indistinguishable from photographs. Without this new legislation, offenders could simply argue that all their images are virtual images, and therefore there was no actual harm done to children. However, possession of such virtual images represents a crime against morality [46].

All three examples represent forms of cyber-crime that have no pendant in traditional crime, and as such may need new laws to deal with.

Cyber-crime usually is non-local, traditional crime usually is local. Crime is usually a local matter that is best dealt with locally. States have a monopoly on the use of force over their citizens, and the state has a location in geographical space. Geographic location is an important element of the capability of states to deal effectively with crime committed by their nationals. However, some forms of traditional crime are essentially non-local. We give three examples. The first is provided by piracy of the high seas, which was tolerated until the world powers decided that stable commercial relations would be more profitable than stealing from each other [126].

The second example is provided by piracy of intellectual property in the 19-th century in the US [126]. Charles Dickens, whose books were sent by telegraph over the Atlantic, and which were then printed, and sold in the US without his permission was one of the first victims of net piracy [156]. This practice ended when US publishers and authors agreed to bring an end to the ensuing chaos. This moved the American government to outlaw net piracy [258].

The third example is cyber-crime, which, like the previous examples may eventually be dealt with because legislators decide that the cost of cyber-crime is too high for society to bear. This motivates the following suggestion for future research [59]:

Question 24 *What is the real cost of cyber-crime to society?*

There are reports of costs attributed to cyber-crime, such as the series of Computer Security Institute (CSI) reports, which is now in its 14-th year [218]. However, the CSI reports are the result of a questionnaire sent to US businesses, of which about 10% submits a reply. This is hardly representative for the world at large, and extrapolating the CSI finding is likely to overestimate the cost of cyber-crime. Another approach is to look at the number of prosecutions. For example in the UK there have been about 150 relevant prosecutions in the past 20 years [265], which if extrapolated probably underestimates the cost of cyber-crime. More research is needed to assess the cost of cyber-crime, which is made difficult because of the overwhelming desire of victims not to report incidents for fear of loosing reputation.

There are signs that some governments are already worried about the cost of cyber-crime. For example the US Department of Defence has recently created the US Cyber Command to protect US military cyber-space.

It is less clear which court has jurisdiction over cyber-crime than traditional crime. A national court can only deal with a crime or a criminal if there is a connection to the court. Usually the location of a crime, or the nationality of the criminal falls under the jurisdiction of a specific national court, but other connections are possible too. For example the “Universality nexus” gives a court jurisdiction over crimes that are considered by states as of universal concern, such as slavery, or war crimes [14]. The case of the Love Bug computer virus in 2000 is a good illustration of the jurisdictional problem [126] for cyber-crime. When Onel de Guzman released the Love Bug virus from the Philippines, this was not illegal; hence he could not be prosecuted in his country. Even though releasing a computer virus was illegal in the US, where the Love Bug caused damage too, he could not be extradited for the simple reason that extradition requires that the act is punishable in both countries involved [46]. In response to such issues, some countries have introduced legislation that gives their national wide ranging powers. For example, Malaysian law, by the power of the “Effect nexus” [251] effectively claims that Malaysian courts have universal jurisdiction over some forms of cyber-crime [46].

Cyber-crime amplifies the differences in national law. What is legal in one country might be illegal in another, complicating the matter of deciding jurisdiction [42]. Especially differences between common law (for example Continental Europe) and case law (for example UK, USA) countries are significant. We give two examples. Firstly, in the early 2000’s the FBI developed the Magic Lantern, which can be installed surreptitiously on the computer of a suspect. Without the latter’s knowledge Magic Lantern captures the keystrokes of the computer user (such as user names and passwords).The laws of the US permit the FBI to use Magic Lantern globally, but to the law of other states this is misconduct of law enforcement [14]. It is not clear whether Magic Lantern has ever been deployed.

The second example is retailer entrapment, which arises when a retailer sells a product or service to a customer who is not entitled to receive these. Examples include adult content and gambling services. To avoid prosecution the retailer should ask the customer to certify their age and/or their place of domicile. However, it is easy for the customer to cheat [14]. This leads to a new research question about technologies (called geo-location) that are able to determine the geographic location of an offender, or a target:

Question 25 *How to make the information provided by Geo-location more accurate?*

Organized crime relies on strength in numbers, cyber-crime does can be automatied. Organized crime requires strength in numbers [41]. For example the Mafia in the US during the prohibition produced, distributed and sold liquor illegally, requiring an organised work force. Computers are such powerful tools for the automation of all manner of human activity, that a lone hacker is able to inflict damage, simply by enlisting more computer power. The damage is limited only by his imagination and technical skills. For the Law this implies significant changes, as the concept of organised crime might have to be redefined for cyber-space.

Traditional law enforcement is not as effective against cyber-crime as against traditional crime. Sanctioning for traditional crime is efficient in the sense that law enforcement is able to apprehend enough offenders, thus providing a measure of deterrence that is considered acceptable to society [42]. However, the strategies used by law enforcement are not effective to create the same level of deterrence for cyber-crime. We give two examples. Firstly, whereas a neighbourhood watch program might deter local burglars, an international scammer would probably not be deterred by any local measures, as he acts on a global scale. The problem for the law is to measure the harm caused by a cyber-crime, so that calibrated punishment can be imposed.

Secondly, law enforcement is entitled to the proportional use of force, which in the case of real crime might be used to break locks or to break down doors. However, in the case of investigating the encrypted contents of the hard disk of a computer [60], strong encryption would require a disproportionate amount of force to break the encryption [257]. Whereas weaker forms of encryption can be broken using computers and software, strong encryption cannot be broken in a reasonable amount of time, and perfect encryption (using a one-time pad) cannot be broken at all. (We are assuming here that the encryption is also properly implemented, which is not always the case [139]). Law enforcement cannot ask the suspect to hand over a copy of the encrypted original, since that does not provide any guarantees that the copy and the encrypted original are identical. In this case the only option open is to convict the owner for contempt of court if he refuses to disclose the encryption key. In the case of a real, physical vault with a real key, this would not be necessary, as the vault can always be opened by force. This example shows that information technology offers protection of assets that is unparalleled in the real world.

Summarising, we have shown that there are currently significant differences between cyber-crime and traditional crime as far as the law is concerned. In the beginning of the global Internet era, some believed that a new brand of Law should be created for cyber-space [157]. Now 15 years later, we believe that those differences can be taken into account by an appropriate development of the Law. Whether this will always be true is hard to say, however the essay of Brenner on the subject of Fantasy crime [44] suggests that even substantial harm leaking from behaviour in Second Life can be dealt with effectively by the laws governing cyber-crime. It will probably take years to increase the efficiency of the Law sufficiently.

C.2.2 Reconciling the differences between crime and cyber-crime.

Given that the Internet will continue to change our society at a rapid pace, the task of the legislators is not a simple one. Here we summarise three approaches that we have encountered in the literature designed to deal effectively with cyber-crime. The first two are more or less classical approaches, whereas the third is more radical.

International treaties. International cooperation is essential to improve deterrence in cyber-space. Therefore a number of treaties have been enacted. An example is the European Convention on Cyber-crime, which seeks to harmonise national laws on cyber-crime. To date the Convention has been ratified by 29 nation states, with the US as the only non-European country. This clearly shows the importance that the western world attaches to the fight against cyber-crime. The ratification process is slow and there is a long way to go, since there are over 200 nation states world wide [165]. However, there is hope that like the international treaties on nuclear and chemical warfare, this treaty will eventually be able to claim some successes [115].

More power to the police. Some states have decided that the police should be better equipped to gather intelligence and thus to improve the prevention of cyber-crime by deterrence. Better intelligence allows the police to act more quickly and on a larger scale than at present. For example in the US the FBI and other government agencies have the possibility to issue a National Security Letter (NSL) on an ISP, requesting information about its customers without judicial oversight. The NSL is not new but the sweeping powers bestowed on Government services by the 2001 US PATRIOT act allows the FBI to make heavy use of its power [114]. In Europe the data retention directive [244] requires an ISP to collect and store connection information for a period between 6 and 24 months. National police forces, for example in the Netherlands, make heavy use of this and other information, often without involving the courts [261]. Clearly this practice of gathering intelligence without judicial oversight raises severe privacy concerns. This motivates the following suggestion for future research:

Question 26 *To what extent does law enforcement exceeds its authority in the use of connection data?*

Distributed Security. Brenner and (Leo) Clarke [45] propose a radical departure from current law enforcement to deal with these problems in an enforcement model called "distributed security". Centralised (as opposed to distributed) Law enforcement as it exists today is modelled on the London Metropolitan Police, which was created in 1829 by Sir Robert Peel. Before that time, law enforcement was distributed in the sense that it required the citizens to contribute to law enforcement. The idea of distributed security in the cyber-era is to involve individual users, ISPs, and organizational users in the prevention of cyber-crime. For example (1) a producer of software might be held liable for the quality of the software produced, (2) an ISP might require a government licence to operate, and (3) a user who fails to maintain the security of her computer could be fined. To see why in general distributed security makes sense, we compare the information super highway with a regular highway. Driving an unsafe car may endanger the life of others, and is thus illegal. In the same vein, using a badly maintained PC on the Internet could cause damage to others, and could be declared illegal too.

There are practical issues with distributed security. (1) Software producers have always argued that their products are too complex to be able to bear liability, and that liability would chill innovation [45]. (2) Already in 2002 the estimated number of ISPs world wide was 10,000 [146], hence requiring a massive certification effort, for which ISP could also fail. (3) Fining users who do not properly maintain their computers would be a gargantuan task, considering that soon the number of computers connected to the Internet will exceed the size of the world population.

There are also more fundamental issues with distributed security. Firstly, the proposal has privacy implications, as it requires information sharing between law enforcement, individual users, organizational users, and ISPs. Secondly, distributed security requires intelligence in the Internet, which by design has all intelligence in the end points [27].

Finally, distributed security is actually Crime Science because distributed security asserts that everybody has a role to play in crime prevention, thus fundamentally altering the opportunity structure for crime.

Summarising, technological change has presented challenges to the law before. We believe that like the piracy issues of the past, a solution will come about if states agree that the price we pay for cyber-crime is becoming too high. The problem then becomes one of deciding the cost of cyber-crime, which is notoriously hard. Finally, since detection is beyond the scope of the paper we only mention that Law enforcement requires new tools for digital forensics [55].

D Computer Science supports Social Science in general and Criminology in particular

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 [81]. The development of Computational Social Science follows the lead of Natural Science. For example Lazer et al observe that what we all do in our every day life leaves traces on the Internet [176], 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 solved [163].

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 emphasizes 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 analysis of time series. There are practical limitations to what can be achieved in an 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 [37].

Secondly, crime data contains systematic errors. Sometimes, neither the offender, nor the target, nor the police have an interest in providing correct data [129, 173, 249]. For example, a repeat offender has a vested interest in keeping silent about his crimes, and a police officer might be interested in inflating the crime rate to ensure that the police force will receive more funding [93]. It is well known that recording policies of the police have a strong impact on the officially registered volume of crime, particularly violent crime [228, 282].

Computer based simulated experiments can help to circumvent these problems [133]. 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, CPT. These perspectives can be codified to a certain exetent [33], 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; this term seems to have been used first by Patricia and Paul Brantingham from Simon Fraser University [40]. We will discuss the research of the main groups working on crime simulation, as this is relevant to our interest in Cyber-crime Science.

The main idea of crime simulations is to compute the steps leading to a crime event so that predictions about real crime and the prevention thereof can be made. Agent based simulations are commonly used [93], 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 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 [98]:

"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 decision that tries to avoid 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, but we have been able to find only one inconclusive paper in the related work that suggests this approach [193]. The spatial environment could be a geographical environment modelled by a GIS system, 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 [36].

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 based on a proposed theory that does not apply. 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.

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 is required to drive the simulations. As yet there is insufficient progress in the field to make simulated "what-if" experiments routine [121].

Any simulation must ultimately be validated with real data [24]. We have not found reports of such validations, presumably for reasons of cost, ethics, and privacy [176].

We have found several strands of work in the literature on the generative simulation of traditional crime but not cyber-crime. As the focus of our paper is cyber-crime, we will only mention briefly what the main representatives of the related work on traditional crime are. We differentiate related work on the way in which the macroscopic regularity is specified. Researchers at the Vrije Universiteit in Amsterdam [31, 32, 28, 33, 30, 29, 33] 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. (The approach is not proper model checking as there is no exhaustive state space exploration). Researchers at Simon Fraser University in Vancouver [119, 121, 120, 39, 40] use an interactive approach towards the detection of the macroscopic regularity, in the sense that successful simulations exhibit for example crime hotspots. CPT [37, 38] forms the basis of the simulations; hence the focus is on the spatial and temporal behaviour of the offenders and their targets [229]. Researchers at the University of Cincinnati [92, 94, 93, 184, 266] and the University of Virginia in Charlottesville [49, 51, 50, 52, 137, 136, 179, 180, 215, 285, 286] use statistical approaches towards the specification of the macroscopic regularity, such as clustering [50], and data association [51].

We found only one proposal on agent based simulation of cyber-crime. Gunderson and Brown [137], 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 Crime Science in particular. This leads to the following research approach:

Approach 27 *Use computational simulation as a research method in the study of cyber-crime.*

E All 25 Generic techiques mentioned in the eight survey papers

i. Increase effort

1 Harden target

- Firewalls [21, 48, 202, 207]
- Vulnerability patches [21, 202]
- Encryption [48]
- Antivirus [48]
- ISP as a first line of defence [202]
- IDS [202]

6 Extend guardianship

- RFID [48]

11 Conceal Targets

- DMZ [48, 21, 77]

16 Reduce frustrations

- Not mentioned

21 Set rules

- Educate end-users [202]
- Provide a clear code of conduct [217]

ii. Increase Risks

2 Control access

- Authentication using passwords, pins [21, 77, 48, 207]
- Caller ID like technology for Internet [202]
- Logical: IDS [77]
- Logical: Firewalls [77]

7 Natural surveillance

- Report suspect email and information request to ISP [207]

12 Remove Targets

- Not mentioned

17 Avoid disputes

- Not mentioned

22 Post instructions

- Not mentioned

iii. Reduce Rewards

3 Screen exits

- IDS [21]
- Antivirus [21]
- Audit trail [48]
- Audit trail [202, 207]
- Logical: Firewalls [77]

8 Reduce anonymity

- RFID [48]
- Caller ID [48]
- Audit trails [77]

13 Identify property

- RFID [48, 207]

18 Reduce arousal

- Not mentioned

23 Alert conscience

- Public awareness on the consequences of crime [202]
- educate: ‘copying software is stealing’ [207]

iv. Reduce Provocation

4 Deflect offenders

- Not mentioned

9 Place Managers

- IDS [48]

14 Disrupt markets

- ISP should be keen to assist investigations [202]

19 Neutralize peer pressure

- Not mentioned

24 Assist compliance

- Security education of staff [77, 281]

v. Remove Excuses

5 Control facilitators

- Caller ID [48]
- Make the ISP accountable for the traffic [202]

10 Formal surveillance

- Auditing and trail reviews [21]
- RFID [48]
- Early warning systems of viruses and hacking attacks [202]
- IDS [77, 281]

15 Deny benefits

- Encrypt valuable data [21, 77, 281, 207]

20 Discourage imitation

- Prompt software patching [281, 77]

25 Control disinhibitors

- Cyber-ethics education [21]
- Campaign against hacker culture [207]

page	abbreviation	concept
37	ACM	Association of Computing Machinery
8	BotNet	collection of computers programmed to attack on a massive scale
15	CCTV	Closed Circuit Television
15	CO	Carbon Monoxide
2	CPT	Crime Pattern Theory
6	CRAVED	Concealable, Removable, Available, Valuable, Enjoyable, and Disposable
6	CSP	Cloud Service Provider
47	DDoS	Distributed Denial of Service
42	DEA	Disposable Email Address
7	DHCP	Dynamic Host Configuration Protocol
11	DMZ	De-Militarized Zone
38	GIS	Geographic Information System
11	IDS	Intrusion Detection System
37	IEEE	Institute for Electrical and Electronics Engineers
16	INSAFEHANDS	Identifiable, Neutral, Seen, Attached, Findable, Executable, Hidden, Automatic, Necessary, Detectable, and Secure
7	IP	Internet Protocol
4	IRC	Internet Relay Chat
3	ISP	Internet Service Provider
2	IT	Information Technology
38	LNCS	Lecture Notes in Computer Science
7	MAC	Media Access Control
7	OSN	Online Social Network
48	Online Polling	using computers and the Internet for an opinion poll
48	Online Voting	using computers and the Internet for casting and counting votes in elections
2	RAA	Routine Activity Approach
1	RCP	Rational Choice Perspective
37	RCT	Randomized Controlled Trial
43	reshipper	someone who is prepared to receive and reship goods in exchange for a fee
11	RFID	Radio Frequency IDentification
16	SCAREM	Stealth, Challenge, Anonymity, Reconnaissance, Escape, and Multiplicity
6	SLA	Service Level Agreement
37	SOUPS	Symposium on Usable Privacy and Security
42	URL	Uniform Resource Locator
16	VIVA	High Value, low Inertia, high Visibility and easy Access
4	WLAN	Wireless Local Area Network
43	zero-day attack	an attack that has just been discovered, but for which no defence is available yet

Table 5: Glossary