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 a typical Information Security problem, namely phishing, 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.

Contents

1 Introduction 3

2 Definitions 4

2.1 Analysing the definitions 4

2.2 Cyber-crime Science 5

3 Crime Science from an Information Security perspective 7

3.1 Conceptual framework 7

3.1.1 Routine Activity Approach 7

3.1.2 Crime Pattern Theory 9

3.1.3 Rational Choice Perspective 10

3.1.4 Repeat Victimization 10

3.2 Reducing the opportunity for crime 10

3.2.1 The 5 principles of opportunity reduction 11

3.2.2 The 25 opportunity reducing techniques 11

3.3 A body of evaluated practice 16

3.4 Displacement of crime and diffusion of benefits 16

4 On the lack of evaluated practice in the Computer Science literature 17

4.1 Searches 17

4.2 Analysis 19

5 Crime Science applied to cyber-crime: Two Case studies 20

5.1 Phishing 20

5.1.1 Is phishing a real problem? 20

5.1.2 Is phishing a new problem? 20

5.1.3 How could the 25 generic techniques help control phishing? 20

5.1.4 How to avoid phishing scams? 22

5.1.5 Anti-phishing research is hard 22

5.2 On-line Auction Fraud 23

5.2.1 Using the 25 techniques against on-line auction fraud 24

6 Disciplines supporting Cyber-crime Science 26

6.1 Computational Social Science 26

6.2 Economics 27

6.2.1 Economics of Information Security 28

6.2.2 Economics of Information Privacy 29

6.3 Law 29

6.3.1 Differences between Crime and Cyber-crime 29

6.3.2 Reconciling the differences between crime and cyber-crime 31

7 Stakeholders in Cyber-crime Science 32

7.1 Manufacturers 32

7.2 Students 33

8 Conclusions 33
<table>
<thead>
<tr>
<th>page</th>
<th>abbreviation</th>
<th>concept</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>ACM</td>
<td>Association of Computing Machinery</td>
</tr>
<tr>
<td>9</td>
<td>BotNet</td>
<td>collection of computers programmed to attack on a massive scale</td>
</tr>
<tr>
<td>16</td>
<td>CCTV</td>
<td>Closed Circuit Television</td>
</tr>
<tr>
<td>16</td>
<td>CO</td>
<td>Carbon Monoxide</td>
</tr>
<tr>
<td>8</td>
<td>CRAVED</td>
<td>Concealable, Removable, Available, Valuable, Enjoyable, and Disposable</td>
</tr>
<tr>
<td>8</td>
<td>CSP</td>
<td>Cloud Service Provider</td>
</tr>
<tr>
<td>28</td>
<td>DDoS</td>
<td>Distributed Denial of Service</td>
</tr>
<tr>
<td>22</td>
<td>DEA</td>
<td>Disposable Email Address</td>
</tr>
<tr>
<td>9</td>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>19</td>
<td>GIS</td>
<td>Geographic Information System</td>
</tr>
<tr>
<td>13</td>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>17</td>
<td>IEEE</td>
<td>Institute for Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>33</td>
<td>IMEI</td>
<td>International Mobile Equipment Identity</td>
</tr>
<tr>
<td>33</td>
<td>INSAFEHANDS</td>
<td>Identifiable, Neutral, Seen, Attached, Findable, Executable, Hidden, Automatic, Necessary, Detectable, and Secure</td>
</tr>
<tr>
<td>8</td>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>4</td>
<td>IRC</td>
<td>Internet Relay Chat</td>
</tr>
<tr>
<td>4</td>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>3</td>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>17</td>
<td>LNCS</td>
<td>Lecture Notes in Computer Science</td>
</tr>
<tr>
<td>9</td>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>28</td>
<td>Online Polling</td>
<td>using computers and the Internet for an opinion poll</td>
</tr>
<tr>
<td>17</td>
<td>RCT</td>
<td>Randomized Controlled Trial</td>
</tr>
<tr>
<td>23</td>
<td>reshipper</td>
<td>someone who is prepared to receive and reship goods in exchange for a fee</td>
</tr>
<tr>
<td>11</td>
<td>RFID</td>
<td>Radio Frequency IDentification</td>
</tr>
<tr>
<td>33</td>
<td>SCAREM</td>
<td>Stealth, Challenge, Anonymity, Reconnaissance, Escape, and Multiplicity</td>
</tr>
<tr>
<td>8</td>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>17</td>
<td>SOUPS</td>
<td>Symposium on Usable Privacy and Security</td>
</tr>
<tr>
<td>22</td>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
<tr>
<td>33</td>
<td>VIVA</td>
<td>high Value, low Inertia, high Visibility and easy Access</td>
</tr>
<tr>
<td>28</td>
<td>Online Voting</td>
<td>using computers and the Internet for casting and counting votes in elections</td>
</tr>
<tr>
<td>5</td>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
<tr>
<td>23</td>
<td>zero-day attack</td>
<td>an attack that has just been discovered, but for which no defence is available yet</td>
</tr>
</tbody>
</table>

Table 1: Glossary
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 [64, 130, 224]. Crime Science, in contrast is interested in explaining the short term causes of offending and the “how” of offending [66]. 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 trans-generational background, and on the long-term causes of criminal behaviour.

In its short history, Crime Science has delivered on its promise of fast and effective scientific approach for the prevention of crime [160, 219, 251]. We can describe Crime Science by means of seven characteristics [219]:

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, but also accidents in medication [75, 98], public health [222, 157], and personal safety [127, 189]. 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 the Rational Choice Perspective, the Routine Activity Approach, and Crime Pattern Theory (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, mishaps, accidents, disorder, etc;

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 large variety of fields: all professionals active in the field of crime prevention and disorder, such as policemen, 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 sources of methods of 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 many well intended policies are often 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 the sticky 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 much well intended advice designed to stop phishing [132]. To make Information security more effective, economic and human factors must be taken into account.

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 show that there are only a few cyber-crime prevention studies in the Computer Science literature. In Section 4 we apply the ideas from Crime Science to cyber-crime. Section 5 discusses the relationship between Information Security, and the disciplines that are most closely related from a crime prevention point of view, which are Computational Social Science, Economics, and Law. Section 6 presents an analysis of the most important practical issue: getting the cooperation for cyber-crime prevention of the most important stakeholders, such as government and industry. The last section concludes and sets the research agenda for the area of Cyber-crime Science.

2 Definitions

We start with 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 [118]. 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 and is morally or legally wrong.

For the purpose of this paper we will however use an objectivist definition from criminal law [211]: 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 [194]. 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 [193] 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 [160] [188]: Crime Science is the application of the methods of Science to the prevention or detection of disorder, 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 [183]. 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 [43]. This eventually led to the introduction of the modern police force. It is possible that the information revolution will have a significant effect on law enforcement too. However, before cyber-crime is subsumed by the definition of crime, there are some significant 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 [131] 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 a significant overlap between cyber-crime and breaches of 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 clearly crimes. All common forms of cyber-crime, i.e. cyber-trespass, cyber-deceptions and thefts, cyber-pornography, and cyber-violence typ-
ically involve a breach of Information Security.

Despite this large 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, which works 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 of Cyber-crime Science (i.e. Information Security) failed to act, another discipline of 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 will eventually be 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” [17]. 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 [17] 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 [169] 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 [182]. McCarty [171] 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 [172] 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 [203] describe how in the early days of Wireless Local Area Network (WLAN), most 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 serious trouble because of their negligence. Most of the offenders were caught because they did not think about hiding their actions. Computers and networks thus provide significant 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 in-

---

1. Like Crime Science, Information Security is not in-

---

---
terested in the personality of the offender, but is in-
terested in the incidents, such as violated security
policies, broken security protocols, hacked web sites,
guessed passwords, cloned smart cards etc. In this re-
spect, Cyber-crime Science and Information Security
research have always been similar.

2. Like Crime Science, Information Security is problem-
oriented and focuses on ways to prevent concrete in-
cidents (such as hacking a web site). Information
Security is “crime” specific. For example, all well de-
dsigned 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 con-
sidered). By aiming to prevent or detect specific
outcomes, Information Security research is outcome-
oriented. Here too Cyber-crime Science and Informa-
tion Security research have always been similar.

3. However, unlike Crime Science, Information Security
research does not normally study the outcome of In-
formation 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 enrich-
ment of Information Security research that is dis-
cussed further in Section 5.

4. Information security research does not have a concep-
tual 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 guidelines for Information Security.
The Rational Choice Perspective is fundamental to
the Economics of Information Security and Privacy; we
will discuss this in detail in Section 6.2. There is
a role for the Routine Activity Approach [254, 138]
and Crime Pattern Theory too, but there is a signif-
ificant difference between cyber-crime and traditional
crime that has a large 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 develop-
ment, which is discussed in Section 6.1.

5. Unlike Crime Science, Information Security research
does not investigate incidents to identify rules and
patterns of human behaviour that explain the oc-
currence of these incidents. Rather, Information Se-
curity develops new techniques to prevent and de-
tect security breaches, and investigates the proper-
ties 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 mul-
tidisciplinary field. Information Security is inti-
mately related to Mathematics, but also Physics [24],
Law [209], Economics [9], and Psychology [195]. 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 Geog-
raphy, which as we have already mentioned in item 5
above 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 busi-
nesses.

Summarising, Cyber-crime Science and Information Se-
curity 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 &
Tilley [186]:

Context & Treatment causes Outcome.

- The context is the environment in which opportuni-
ties for crime exist.
- The treatment consists of the application of tech-
niques aiming to prevent crime.
- The outcome is the result of applying the treatment
  in a specific, concrete context.

In the approach by Pawson & Tilley, empirical investiga-
tion of outcomes in Crime Science is done by case stud-
ies. 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 Infor-
mation 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;

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

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 [97], we will present top down:

- The Routine Activity Approach operates at the level of society or a large 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 the Routine Activity Approach [71], which states that the opportunity for crime is most 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. Many individuals in modern society are potential offenders [68, 113, 229]. For example when there is little supervision or likelihood of detection, people are vulnerable to temptations [96]. 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. Therefore, Information Security emphasizes the distinction between insiders and outsiders. The Information Security literature is replete with papers on insider threats, dating back to at least Dorothy Denning’s seminal paper in 1987 [79]. The idea of separating offenders into a 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 [250] theorises about certain characteristics of insiders, but without any empirical evidence, and Theoharidou et al [217] examine various social and criminological theories, including those discussed here, as a basis for containing the insider threat. Neumann [181] provides an older but still valid overview of the challenges of preventing insider attacks. Finally Caputo et al [55] 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 [243] 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 most to the collapse of the bank. A series of three papers [215, 216, 214] propose the idea 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 [217, 212] (and a paper by other authors [164]) frame software piracy in terms of a number of criminological theories (such as Differential Association Theory, and Neutralization Theory) that focus mostly on the offender, thus falling beyond the scope of the present paper. The seventh paper [245] 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 (and Siponen) [248] is a synthesis of earlier work published in the flagship jour-
nal of the Association of Computing Machinery (ACM). This we hope will lead to a better uptake of the ideas from Crime Science in the Computer Science community.

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 are now accessible to a large 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” [96] 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 outsourcees, 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 [95]. 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 [65]. The mobile phone is a perfect example of a CRAVED product [74], and so is the laptop [151]. Information (e.g. credit card data) can also be described in terms of CRAVED [184] 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 [230]. Similarly, a laptop or mobile phone can be fitted with remote wipe technology [207], 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 e.g. value 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 [71]. 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 many classical scams showing how even the most vigilant people can become personal targets [205].

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 meteoric 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 [71].

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 Internet usage of their children, but this is more easily said than done [173]. Chua et al [60] 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 condone the activities of the vigilantes, because it is undesirable that people take the law in their own hands [149].

Whether the Routine Activity Approach works as well for cyber-crime as for traditional crime is an open question. On the one hand, Yar [251] suggests that in general the ideas apply, but that the differences between the Internet and the real world are large, 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 will 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 the World Wide Web form cliques, just like social networks. In a social network 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 suggest focusing on a semantic notion of place, a nice example of which is provided by Holt and Bossler. They report on an empirical test designed to explore the applicability of the Routine Activity Approach to a specific form of cyber-crime: On-line harassment. A survey amongst 788 college students found that spending a lot of time on the Internet does not necessarily increases the risk of victimization, unless significant 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 online harassment.

Summarising, according to the Routine Activity Approach, 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 proximity in the cyber-physical world?

### 3.1.2 Crime Pattern Theory

Crime Pattern Theory 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. hot spots. Knowledge of such hot spots can be used to protect those who have been victimized, since if we can predict what the hot spots are, where they are, and who is likely to be victimized, we can target the efforts of crime prevention more precisely and effectively. For example town planners can use maps showing the incidence of crime to change street plans, and police resources can be deployed more effectively.

Traditional crime is generally serial crime because physical constraints make it difficult to commit more than one crime at once. 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, 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.

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 hot spot. The only exception that we have found is formed by the chartrooms 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 easy to commit many crimes at once at many places all over 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 many interconnected computers, where hot spots 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/), 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. It is probably harder to collect traces in the real world than on the Internet, thus for once creating an advantage for cyber-crime prevention over traditional crime prevention.

However, collecting large amounts of information that could eventually be used to prevent or detect cyber-crime would have serious 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.
of conclusion we offer two suggestions for future research:

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

Question 5 What exactly is a “hot spot” on the Internet?

3.1.3 Rational Choice Perspective

The Rational Choice Perspective of human action is used in Economics [201], Psychology [225], and Sociology [72], 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 [74]. The Rational Choice Perspective 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 Rational Choice Perspective 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” [108]. 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 [77]. Burglars are often more preoccupied by minimizing risk rather than increasing the rewards [77].

The Rational Choice Perspective 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 [11] present a survey of 167 college students showing that risky behaviour, such as sharing passwords, or opening suspect emails is a rational choice. Higgins [131] 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.

The Rational Choice Perspective has been applied in simulation in Social Science [92] and more specifically in crime simulations [168] (see Section 6.1) as well as the study of the Economics of Information Security (see Section 6.2). While these are promising results, there is considerable scope for more research into the Rational Choice Perspective on cyber-crime.

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

Question 6 Which cost/benefit tradeoffs do cybercriminals actually make?

3.1.4 Repeat Victimization

Many crimes target the same victim repeatedly, which is referred to as Repeat Victimization [32]. 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. Burglarised houses are often victimized twice at relatively short intervals [32]. Repeat Victimization is not a perspective in the same sense as the Rational Choice Perspective, the Routine Activity Approach, and Crime Pattern Theory, 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 [151]. Templeton and Kirkman [215] give many tragic 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 7 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 joyroiding, 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 [66]. 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 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 [10], or educating Internet users the difference between content that is free and content that is not free.

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 2 taken from Cornish and Clarke [73] 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 [124]. 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 [170]. 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 many case studies [62]. In these case studies cyber-crimes are not represented yet. However, in the next section we will show that based on our literature review, many of the 25 generic techniques are in principle applicable to the prevention of cyber-crime as they are to traditional crime.

3.2.2 The 25 opportunity reducing techniques

We have found seven recent reviews in the literature that suggest how Information Security tools can be used as a specific instance of the 25 generic techniques [19, 46, 180, 184, 248, 191, 239].

We will discuss each of seven reviews briefly, followed by a comparison of the salient recommendations offered by the first six reviews. The last review focuses on a specific technology, a Radio Frequency IDentification (RFID) tag, which makes it less suitable for the comparison.

The first review by Beebe and Rao [19] 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.

The next four reviews [46, 180, 184, 248] 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 [46] 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. Newman and Clarke [184] choose the setting of electronic commerce, and Willison and Siponen [248] present an association in the setting of embezzlement. Morris [170, 180] 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 sixth review by Reyns [191] is 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
<table>
<thead>
<tr>
<th>Economical cost and balance</th>
<th>Psychological cost and balance</th>
</tr>
</thead>
<tbody>
<tr>
<td>i. Increase effort</td>
<td>iv. Reduce Provocation</td>
</tr>
<tr>
<td>ii. Increase Risks</td>
<td>v. Remove Excuses</td>
</tr>
<tr>
<td>iii. Reduce Rewards</td>
<td></td>
</tr>
<tr>
<td>1. Harden target</td>
<td>11. Conceal Targets</td>
</tr>
<tr>
<td>- Steering column locks and immobilisers</td>
<td>- Off-street parking</td>
</tr>
<tr>
<td>2. Control access</td>
<td>12. Remove Targets</td>
</tr>
<tr>
<td>- Entry phones</td>
<td>- Removable car radio</td>
</tr>
<tr>
<td>3. Screen exits</td>
<td>13. Identify property</td>
</tr>
<tr>
<td>- Ticket needed for exit</td>
<td>- Property marking</td>
</tr>
<tr>
<td>4. Deflect offenders</td>
<td>14. Disrupt markets</td>
</tr>
<tr>
<td>- Street closures</td>
<td>- Monitor pawn shops</td>
</tr>
<tr>
<td>5. Control facilitators</td>
<td>15. Deny benefits</td>
</tr>
<tr>
<td>- “Smart” guns</td>
<td>- Ink merchandise tags</td>
</tr>
<tr>
<td>6. Extend guardianship</td>
<td>16. Reduce frustrations</td>
</tr>
<tr>
<td>- Take routine precautions: go out in group at night, leave</td>
<td>- Efficient queues and polite service</td>
</tr>
<tr>
<td>signs of occupancy, carry phone</td>
<td></td>
</tr>
<tr>
<td>7. Natural surveillance</td>
<td>17. Avoid disputes</td>
</tr>
<tr>
<td>- Improved street lighting</td>
<td>- Separate enclosures for rival soccer fans</td>
</tr>
<tr>
<td>8. Reduce anonymity</td>
<td>18. Reduce arousal</td>
</tr>
<tr>
<td>- Taxi driver IDs</td>
<td>- Controls on violent pornography</td>
</tr>
<tr>
<td>- CCTV for double-deck buses</td>
<td>- “Idiots drink and drive”</td>
</tr>
<tr>
<td>10. Formal surveillance</td>
<td>20. Discourage imitation</td>
</tr>
<tr>
<td>- Red light cameras</td>
<td>- Rapid repair of vandalism</td>
</tr>
<tr>
<td>- Off-street parking</td>
<td>- Rental agreements</td>
</tr>
<tr>
<td>22. Post instructions</td>
<td></td>
</tr>
<tr>
<td>- “No Parking”</td>
<td></td>
</tr>
<tr>
<td>- Roadside speed display boards</td>
<td>- Easy library checkout</td>
</tr>
<tr>
<td>25. Control disinhibitors</td>
<td></td>
</tr>
<tr>
<td>- Breathalyzers in pubs</td>
<td></td>
</tr>
</tbody>
</table>

Table 2: The 25 Generic opportunity reducing techniques used to prevent traditional crime, with an example of a crime specific technique for each of the 25. (From Cornish and Clarke [73])
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 two oldest reviews [180, 184] use the older 16 generic techniques. We have mapped these onto the current 25 generic techniques as indicated in Table 3.

The last review [239] describes the potential for crime prevention with an RFID tag, ranging from inexpensive chip-less tags [15] 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 gross list of the specific techniques from the five review papers can be found at http://eprints.eemcs.utwente.nl/18500/

Here we provide a summary (see Table 4) comparing the way in which the first six 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. These are:

1. A password or pin code when kept secret can be used to authenticate a user;
2. Encryption of data ensures that once encrypted, the data can be read only when the correct decryption key is known;
3. A Firewall is a tool that stops potentially malicious connections to a computer or network;
4. An Intrusion Detection System (IDS) stops potentially malicious information being sent to a computer or network;
5. A Virus scanner detects malicious code in the information being sent to a computer or network;
6. An RFID tag is a tiny embedded computer that can provide information about the product to which it is attached;
7. Caller-ID is a technique that tells the recipient of a telephone call who is calling;
8. An Audit log collects relevant operational data that can be analysed when there is an incident;
9. An ISP is an organisation that provides Internet connectivity to its clients.
10. User education can be a powerful tool. Including this in the list shows that we interpret Information Security in a broad sense.

We will now discuss the 10 techniques in more detail.

Passwords and pin codes are mentioned in all reviews, as these are the basic tools of Information Security. Unfortunately, a good password or pin code is hard to remember so that as a result many passwords and pin codes that are currently in use are weak [8].

Firewalls are mentioned in three of the four reviews [19, 46, 180] as a specific technique for target hardening (principle i). This is also the only technique that all authors associate with the same generic technique. We take this as an indication that there is no ambiguity surrounding the application of firewalls as a means of situational crime prevention.

Encryption is seen by two reviews [46, 180] as a means to harden targets (principle i) and by the others [19, 248] as a means to deny benefits (principle iii). 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 many components built into various places into a car is harder to steal than a single component [90]. 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.)
<table>
<thead>
<tr>
<th>Economical cost and balance</th>
<th>Psychological cost and balance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increase effort</td>
<td>Increase Risks</td>
</tr>
<tr>
<td>- Firewalls  [19]  [46]  [180]  [184]</td>
<td>- RFID  [46]</td>
</tr>
<tr>
<td>- Vulnerability patches  [19]  [180]</td>
<td></td>
</tr>
<tr>
<td>- Encryption  [46]</td>
<td></td>
</tr>
<tr>
<td>- ISP as a first line of defence  [180]</td>
<td></td>
</tr>
<tr>
<td>- IDS  [180]</td>
<td></td>
</tr>
<tr>
<td><strong>2. Control access</strong></td>
<td><strong>7. Natural surveillance</strong></td>
</tr>
<tr>
<td>- Authentication using passwords, pins  [19]  [46]  [184]</td>
<td>- Report suspect email and information request to ISP  [184]</td>
</tr>
<tr>
<td>- Caller ID like technology for Internet  [180]</td>
<td></td>
</tr>
<tr>
<td>- Audit trail  [46]</td>
<td>- Caller ID  [46]</td>
</tr>
<tr>
<td>- Audit trail  [180]  [184]</td>
<td></td>
</tr>
<tr>
<td>- Make the ISP accountable for the traffic  [180]</td>
<td></td>
</tr>
<tr>
<td>- Make the ISP accountable for the traffic  [180]</td>
<td>- RFID  [46]</td>
</tr>
<tr>
<td>- Early warning systems of viruses and hacking attacks  [180]</td>
<td>- IDS  [248]</td>
</tr>
</tbody>
</table>

Table 4: The 25 Generic techniques used to structure popular Information Security techniques.
An **IDS** is mentioned in three of the four reviews [180, 46, 248], but in different ways. The most common is “Formal surveillance” [248], principle ii. However “Utilize place managers” [46], also principle ii is also used, with the addition that the IDS should have “inference capabilities”. 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.

**RFID** tags are mentioned only by Brookson et al [46] 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, all principle ii. RFID tags are most naturally thought of as a technique to “Identify property”, principle iii. A separate study [239] shows that RFID tags can be used for all of the 25 generic techniques.

**Caller-ID** is mentioned in two reviews [46, 180] 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 [61]. This is an indication of the fact that further work is needed to try and find a similar, effective technique for the Internet. There is some promising work on this topic in the Internet but it requires hardware support and changes to the way that an ISP operates [241].

An **Audit trail** is mentioned by several reviews as a powerful 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 [184].

The **ISP** should be more active in the prevention of crime, this conclusion is shared by all the seven reviews. We have also found many suggestions in the related work to empower the ISP. For example Kennedy [149] claims that only 5% of all downloads are paid for, which causes a serious 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 (principle iii) for illegal downloading. The second approach is to stress the fact that a large fraction of the bandwidth of an ISP is used for illegal downloads, thus reducing the bandwidth for legal use of the network. A typical ISP would block or throttle bit torrent traffic, which is responsible for most of the illegal downloads. This would be an instance of the specific technique “Control facilitators” (Principle i). 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 [230]. ISP blocking can even help the offender rather than preventing crime: Clayton [70] 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 will be engaged in a perpetual arms race with the offenders.

Returning to the five reviews, the Morris reports [179, 180] contain the creative suggestions for empowering the ISP. The panels would like to see the ISP as a first line of defence (i.e. target hardening, principle i) so as to assist the consumer in her arduous 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 (again principle i). Finally, the ISP could advertise that it is proactive in preventing crime, and that the ISP will cooperate closely with the police wherever she can. This falls into the generic technique of “Alert conscience”, principle iv. We believe that it would be interesting to investigate:

**Question 8** What roles can ISPs have in preventing cyber-criminal, and what is the effectiveness of these roles?

**Education** of offenders, targets, and guardians is considered useful by all reviews to remove excuses (principle iv). Brookson et al [46] 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 [248] suggests that the education of staff might “Assist compliance” with company policies. The panel of Morris [180] 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 many users adhered to the “hacker’s ethic” which promoted that information should be free [102]. When the Internet opened for busi-
ness, 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 [184]. Appropriate education would be appropriate to explain the difference between information that is free and information that is not.

Table 4 offers no suggestions to “Reduce provocation” (principle iv) and only two suggestions to “Reduce rewards” (principle iii). This does not mean to say that there are no Information Security techniques that can be applied in these categories; it might mean that the five cited reviews have not thought of such means, or that researchers in the Computer Science community do not think of their work as a means to prevent crime.

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

**Control facilitators** is not considered by any of the reviews but we believe this to be applicable. For example modern colour copiers refuse to copy a bank note [148].

**Deny benefits** is not considered by any of the reviews but we have found suggestions in the Crime Science literature that this could work [90]. 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 produces 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 significant 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 [256], who argues that Internet addiction is a behavioural disorder like pathological gambling. Internet addiction can be serious; in the press there are reports of fatalities, and reports of deviant behaviour promulgated by Internet addiction [121] have appeared in the literature.

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

**Question 9** Which of the 25 opportunity-reducing techniques is most effective in preventing which class of cybercrime?

**3.3 A body of evaluated practice**

A large number of studies report on the effectiveness of Crime Science for traditional crime; Guerette and Bowers [124] provide an excellent starting point. However, for Cyber-crime Science only few relevant studies exist. We substantiate this claim in Section 3.

**3.4 Displacement of crime and diffusion of benefits**

One of the most difficult aspects 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 significant fraction of highly toxic Carbon Monoxide (CO), was the method of choice to commit suicide (Suicide is not a crime in the legal sense). 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 dramatically [67]. An example that does apply to crime is the alley-gating scheme that was implemented in Liverpool (UK) to prevent burglary [33]. 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 significant reduction of burglaries within the alley-gated areas. Also, the initiative had not caused geographical displacement of burglaries. 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 [34]. 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 [69]. It is assumed that when offenders notice crime prevention they become more alerted to the risk of crime generally, and not just in situations where crime prevention measures were taken [65].

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 [124]. 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 [124]. 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 10** Which techniques merely displace the benefits for the criminal, and which ones actually diffuse them?
An interesting issue is whether displacement of crime and diffusion of benefits functions the same way in cyber-space as in the physical world.

4 On the lack of evaluated practice in the Computer Science literature

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 [94]. 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 significant 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 almost 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 evaluations of techniques from information security.

4.1 Searches

Firstly, we searched all 16 online proceedings in the period 1995 – 2010 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 650 online papers, only 14 ([13, 51, 59, 113, 133, 145, 146, 196, 206, 208, 235, 236, 255, 257]) mention the word “crime”, mostly in the abstract, motivation section or in the references. We found not a single paper 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/ the Sym-posium:

“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 77 papers of the ACM Symposium on Usable Privacy and Security (SOUPS) from the years 2005 – 2009. 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 5. Only four (last two rows) out of the 77 papers are relatives of Cyber-crime Science. None of the 77 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, Section 5.1 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 – 2009. Seven papers [100, 152, 157, 177, 178, 198, 204] were found to be relevant from a Cyber-crime Science perspective, all of which are discussed in Section 5.1.

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 mostly applications of general Computer Science techniques (i.e. not

Table 5 lists all the papers cited in this review categorised according to the discipline. An asterisk indicates papers that cite the work of the Crime Science pioneers. The numbers in the second column do not add up due to the presence of the category Recommended.
Table 5: All papers cited in this review categorised according to the discipline. The star indicates papers that cite the work of the Crime Science pioneers. The category Recommended represents highly recommended reading.

<table>
<thead>
<tr>
<th>Category</th>
<th>N</th>
<th>Papers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Biology</td>
<td>2</td>
<td>163</td>
</tr>
<tr>
<td>Computing</td>
<td>139</td>
<td>228</td>
</tr>
<tr>
<td>Biology</td>
<td>3</td>
<td>123</td>
</tr>
<tr>
<td>Computing</td>
<td>1</td>
<td>112</td>
</tr>
<tr>
<td>Biology</td>
<td>70</td>
<td>140</td>
</tr>
<tr>
<td>Computing</td>
<td>8</td>
<td>148</td>
</tr>
<tr>
<td>Economics</td>
<td>7</td>
<td>165</td>
</tr>
<tr>
<td>Ethics</td>
<td>1</td>
<td>119</td>
</tr>
<tr>
<td>Law</td>
<td>23</td>
<td>14</td>
</tr>
<tr>
<td>Medicine</td>
<td>8</td>
<td>240</td>
</tr>
<tr>
<td>Physics</td>
<td>1</td>
<td>119</td>
</tr>
<tr>
<td>Policy</td>
<td>1</td>
<td>119</td>
</tr>
<tr>
<td>Psychology</td>
<td>7</td>
<td>124</td>
</tr>
<tr>
<td>Sociology</td>
<td>1</td>
<td>124</td>
</tr>
<tr>
<td>Recommended</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>Total</td>
<td>260</td>
<td></td>
</tr>
</tbody>
</table>

Table 6: An analysis of the related work on phishing from the Crime Science point of view

<table>
<thead>
<tr>
<th>Number of papers</th>
<th>Purpose</th>
<th>average number of subjects in case study</th>
<th>Crime Science yes / no</th>
</tr>
</thead>
<tbody>
<tr>
<td>33</td>
<td>no case studies with users</td>
<td>0</td>
<td>no</td>
</tr>
<tr>
<td>26</td>
<td>classical usability studies of a new technology</td>
<td>29</td>
<td>no</td>
</tr>
<tr>
<td>14</td>
<td>usability studies of various new password technologies (e.g. graphical passwords)</td>
<td>89</td>
<td>no</td>
</tr>
<tr>
<td>8</td>
<td>user surveys of various issues (mainly privacy)</td>
<td>155</td>
<td>no</td>
</tr>
<tr>
<td>3</td>
<td>teaching people how to avoid phishing scams</td>
<td>183</td>
<td>partly</td>
</tr>
<tr>
<td>1</td>
<td>prevent shoulder surfing</td>
<td>20</td>
<td>partly</td>
</tr>
</tbody>
</table>
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 Section 6.3.

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

4.2 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 [129], 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 [18]. The resulting reluctance to report an incident 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 a serious 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 [185] 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 excellent text book [80] as the main text. Her book offers an encyclopaedic coverage of Information Security, with many 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 purely 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 Soghan [204] 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 Section 5.1.5 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 Section 5.1), but no reports have been found that actually demonstrate a reduction in cyber-crime [231]. We believe that Information Security researchers will be able to make progress in partnership with other disciplines, as has already happened with Law (See Section 6.3), Economics (See Section 6.2), and Psychology [195]. 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 11** 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 12** 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.
5 Crime Science applied to cyber-crime: Two 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 alarming rate of growth \[174\], its high estimated cost \[165\], 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.

5.1 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 \[176\]. Phishing is a form of social engineering \[141\], 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 many 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. 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 \[156\]. 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, social networks \[141\] and web search engines.

5.1.1 Is phishing a real problem?

Dhamija et al \[81\] 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 \[83\] report that spear phishing has a success rate of up to 80%. From a study of 20 non-expert computer users Downs et al \[85\] 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 large numbers of 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. \[165\]. Phishing is thus a real problem.

5.1.2 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. One truly vile 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.

5.1.3 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 8 of the 25 generic techniques. We discuss each of these 8 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. Many papers have been written on training programs against phishing. The most prominent is perhaps the “School of
phish” [156]. This is a well designed experiment comparing 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 large, 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 three essential facilities to be able to carry out the attack: bulk email lists, mass mailing, and the user’s inbox. 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 [144]. 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 [193], 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 significant percentage of Spam but it is fundamentally impossible to stop all Spam without also filtering out some desirable mail [115].

- Making the sender pay for each email will discourage offenders to send millions of spam messages, but it is not easy to enforce payment [151].

- 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 serious problems with signed email too. Firstly, phishers are likely to be the first to adopt signed email [20]. Secondly only well trained users can verify digital signatures [105]. Thirdly, requiring all emails to be signed curtails the freedom of speech [20].

- Reputation based filtering could in principle be used to filter email from sources with a low reputation [78]. This has proved to be an effective method to reduce fraud in online auctions [60], but no related work has been found that applies these ideas to the prevention of phishing.

While many 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 13** 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) Many online social networks and related services such as online video and photo sites provide a “report abuse” control [140]. 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 big problem in the case of phishing but it certainly is a big 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 [62]. 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 14** 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 many areas of traditional crime fighting, such as analysing credit card and telephone fraud [18]. Monitoring can also be used to fight cyber-crime, for example by gathering offender profiles [22], by analysing the social structure of offender demography [59], or by analysing transactions in Second Life [210]. This leads to the following suggestion for future research:

**Question 15** 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 [197], 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 [103] and separately by Yue and Wang [258], 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 16** How effective is it to pollute the phishers database?

**Post instructions (22)** If Gajek et al. [103] 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.

**Assist compliance (24)** Adolescents who are active on the Internet have a higher risk of becoming targets of cyber-bullying and cyber-stalking [175]. Privacy Enhancing Technologies try to help online users to reduce the amount of private information divulged on the Internet. Such technologies can help to prevent crimes, such as bullying and stalking. Atkinson et al. [11] propose a browser plug-in that records where the user has disclosed personal information. This raises the awareness of users to the risks of disclosing information, and thus helps the user to manage the risk, including the risk of phishing.

**5.1.4 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. [85]:

- 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 much less sense at an aggregate level [132].

**5.1.5 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 [204] include:

- Extracting significant amounts of information needed for research from an online social network site 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. [141] 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 [99]:

**Question 17** How to design phishing experiments that are ethically acceptable, legally justified, and empirically sound?

Summarising there are many approaches to curtail phishing, but there are probably more opportunities for new preventive measures. We have been able to classify the most 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 18** To what extent do the 25 generic techniques apply to the specific cyber-crime of phishing?

### 5.2 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 many tools of the offender.

The underground economy consists of a large 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 large 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 online 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 almost impossible 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.


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

5.2.1 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 19 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 [101] 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 many 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 [260] 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 a significant amount of time and money, and he has to face fierce competition from many other offenders. Contrary to popular belief, Otto will not get 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 [133].
Figure 1: The ten steps of the on-line auction fraud. The two immediate consequences of step (5) have been indicated by dashed arrows.
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 20 How to decide which of the 25 techniques have the highest potential?**

## 6 Disciplines supporting Cyber-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 in “Thinking Thief” [104]. In this section we present three related disciplines in some detail. Firstly, we show some of the highlights of Computational Social Science, which offers a number of valuable tools for the Crime Scientist, and thus also for the Cyber-crime Scientist. Secondly 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. the Rational Choice Perspective applies to Information Security. Thirdly we will summarise the dramatic effects the rise of cyber-crime as promoted by the Internet has had on the Law, focusing on the deterrent effect of the Law.

### 6.1 Computational Social Science

For many years, Natural Science has made heavy use of 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 [76]. 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 everyday life leaves traces on the Internet [164], thus providing a rich source of information that can be mined and analysed. 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. However, 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 [85].
- Secondly, crime data contains systematic errors. Sometimes, neither the offender, nor the target, nor the police have an interest in providing correct data [110, 158, 218]. For example, a repeat offender has a vested interest in keeping silent about as many of his crimes as possible, and a police officer might be interested in inflating the crime rate to ensure that the police force will receive more funding [87]. It is well known that recording policies of the police have a strong impact on the officially registered volume of crime, particularly violent crime [200, 249].

Computer based simulated experiments can help to circumvent these problems [122]. 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, Crime Pattern Theory. These perspectives can be codified to a certain extent [81], 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 [35]. We will discuss the research of the main groups working on crime simulation, as this is most 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 the most popular method [87], 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 the Rational Choice Perspective) is also the essence of
generative simulation. Quoting Epstein [92]:

“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 [173]. 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 [33].

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 many theories 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 considerable 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 [112].

Any simulation must ultimately be validated with real data [22]. We have not found many reports of such validations, presumably for reasons of cost, ethics, and privacy [161].

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 [29, 30, 26, 31, 29, 27, 31] 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 [110, 112, 111, 37, 38] use an interactive approach towards the detection of the macroscopic regularity, in the sense that successful simulations exhibit for example crime hot spots. Crime Pattern Theory [35, 36] forms the basis of the simulations; hence the focus is on the spatial and temporal behaviour of the offenders and their targets. Researchers at the University of Cincinnati [86, 88, 57, 106, 255] and the University of Virginia in Charlottesville [17, 39, 48, 50, 126, 125, 162, 163, 190, 252, 253] use statistical approaches towards the specification of the macroscopic regularity, such as clustering [48], and data association [49].

We found only one proposal on agent based simulation of cyber-crime. Gunderson and Brown [126], 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 21 Use computational simulation as a research method in the study of cyber-crime.**

### 6.2 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 [201] underpins the Rational Choice Perspective that we discussed earlier, and Ehrlich’s Theory of Participation [89] 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 of the most 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.

6.2.1 Economics of Information Security

Anderson [7,9] argues that many 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 a nice 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 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? More generally the question is:

Question 22 Which economic arguments could be effective in reducing DDoS attacks?

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 large quantities 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 many 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 at least two counteracting effects: one that raises sales and another that reduces sales. Bhattacharjee et al [23] 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 dramatic fall of music sales over the past decade [149], which is generally attributed to piracy [259].

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 [52], Gopal and Sanders [117] 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 23 Which economic arguments could be effective in reducing piracy?

A good starting point for this research would be the work of Holsapple et al [137], 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 cyber-crime, but it provides ideas for solutions too. Self-enforcing protocols [214] is such an idea: make it in the interest of all parties engaging in transactions to remain honest. A nice 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) [114] and using computers and the Internet for casting and counting votes in elections (Online Voting) [53]. 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 [214].

6.2.2 Economics of Information Privacy

Like Information Security, information privacy can be explained (at least 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” [234]. Using this definition, Berendt et al [21] interview a large number of 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 [120]. 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 most obvious, and often lead to instant gratification. For example, in the real world, most consumers subscribe to a loyalty program with their supermarket. Thus the supermarket knows what consumers buy and offers in exchange a small 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 [120]. In the online world, we see similar phenomena. For example participants in social networks willingly enter an astonishing [123] amount of private information, including photographs and personal details in exchange for popularity, or even notoriety. The disadvantages of rich 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 [153].

If users are asked to pay for privacy (rather than to get paid for giving up privacy) the results are even more dramatic. Many 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 [5]. As a result of all this, the market of privacy conscious individuals is small [1].

The conclusion is that behavioural economic theories are called for, such as “soft paternalism”, which gently nudge [216] people in the right direction when faced with a privacy sensitive decision. A suggested research question would be:

Question 24 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 25 Use economic methods in the study of cyber-crime

6.3 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 [40]. 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 large variety of cyber-crime that the information revolution and in particular the meteoric rise of the Internet has given us [242]. 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.

6.3.1 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 many, if not all 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 [11].

Thirdly, several countries, including the US and Canada, have enacted legislation that declares virtual child pornography illegal on the grounds that with modern technology highly 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 [44].

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 [11].

The second example is provided by piracy of intellectual property in the 19-th century in the US [11]. 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 [142]. 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 [227].

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 [50].

Question 26 What is the real cost of cyber-crime to society?

There are many reports of costs attributed to cyber-crime. The most widely known is perhaps the series of Computer Security Institute (CSI) reports, which is now in its 14-th year [192]. 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 [232], which if extrapolated almost certainly 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 losing reputation.

There are signs that some governments are already seriously 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 many states as of universal concern, such as slavery, or war crimes [12]. The case of the Love Bug computer virus in 2000 is a good illustration of the jurisdictional problem [11]. The case of 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 a lot of damage too, he could not be extradited for the simple reason that extradition requires that the act is punishable in both countries involved [11]. 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” [220] effectively claims that Malaysian courts have universal jurisdiction over some forms of cyber-crime [44].

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 [40]. 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 2000s the FBI developed the Magic Lantern, which can be installed surreptitiously on the computer of a suspect. Without the latters 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 [12]. 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. This leads to a new research question about technologies (called geo-location) that are able to determine the geographic location of an offender a target etc.

**Question 27 How to make the information provided by Geo-location more accurate?**

**Organized crime relies on strength in numbers, cyber-crime does can be automated.** Organized crime requires strength in numbers. 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 considerable 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. 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 programme 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, strong encryption would require a disproportionate amount of force to break the encryption. 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.) 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. 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 suggests that even substantial harm leaking from the most bizarre behaviour in Second Life can be dealt with effectively by the laws governing cyber-crime. It will probably take many years to increase the efficiency of the Law sufficiently.

**6.3.2 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. The most prominent is perhaps 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 a slow one and there is a long way to go, since there are over 200 nation states world wide. However, there is hope that like the international treaties on nuclear and chemical warfare, this treaty will eventually be able to claim some successes.

**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 large scale. 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 \[106\]. In Europe the data retention directive \[213\] 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 \[229\]. Clearly this practice of gathering intelligence without judicial oversight raises severe privacy concerns. This motivates the following suggestion for future research:

**Question 28** To what extent does law enforcement exceed its authority in the use of connection data?

### Distributed Security

Brenner and (Leo) Clarke \[43\] 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 \[43\]. (2) Already in 2002 the estimated number of ISPs world wide was 10,000 \[135\], hence requiring a massive certification effort, for which many of the ISP would probably 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 serious 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 \[25\]. Finally, distributed security is actually pure 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 \[53\].

### 7 Stakeholders in Cyber-crime Science

Crime Science requires cooperation of all the relevant stakeholders. We focus on two different types of stakeholders: manufactures of products and our own students.

#### 7.1 Manufacturers

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 \[167\].

One of the pitfalls of crime prevention is that it is easy to alienate the manufacturers by blaming them for criminogenic design \[19\]. 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 most at risk. This proved to be a powerful incentive for the car industry to improve the locks \[159\].

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 per-
spective. First, the criminogenic properties of the mobile phone were analysed in detail [240]. The analysis found several approaches to reduce the opportunity for phone theft, of which blacklisting of the phone International Mobile Equipment Identity (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 [159]. 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 [147]. 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 [238]. This is where new ideas from Computer Scientists are welcome, especially considering the fact that an increasing range of products that are IP enabled [90], 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 [237] 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 [159].

7.2 Students

Design products and systems to reduce the opportunity for crime fun, and young designers are particularly apt at “lateral thinking” needed to be successful. Gamman and Hughes [104] present a range of imaginative designs by their students to prevent pick pocketing. A multidisciplinary course on Cyber-crime Science is probably attractive to students who now go straight into the police or the security industry [60]. A useful starting point for a curriculum would be Brooks [15], who creates a mind map of all the relevant disciplines that deal with all aspects of security, including physical security, Information Security.

8 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 powerful 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 rich 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 8 but also others, such as:
  - high Value, low Inertia, high Visibility and easy Access (VIVA) [63]
  - Identifiable, Neutral, Seen, Attached, Findable, Executable, Hidden, Automatic, Necessary, Detectable, and Secure (INSAFEHANDS) [240]
  - Stealth, Challenge, Anonymity, Reconnaissance, Escape, and Multiplicity (SCAREM) [184]

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 [184] chapter 4;

- The research methodology of Crime Science has proved its value in traditional crime. We see significant opportunities to apply the method also to cybercrime. For example, in the phishing case study discussed in Section 5.1 we suggest how the researchers could have improved their results if they had known about 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 considerable 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” [239].

If Information Security indeed overlaps significantly 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 excellent and encyclopaedic book on Security Engineering [6] does not mention Crime Science. However, the second edition [8] 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 [84], 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. Section 6.1 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.

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 labelled Question 1… [26]. 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.

**Routine Activity Approach** The opportunity for crime is most 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 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 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, freelancers, outsourcing providers)?
- What is proximity in a cyber-physical world? (Question 3)
- 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?

**Crime Pattern Theory** 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. hot spots. Prevention must therefore target at least these hot spots. 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 two questions:

- What exactly is a “hot spot” on the Internet? (Question 5) What concept(s) of “location” are relevant for the identification of hot spots in the Internet?
- How can we monitor activity on the Internet to identify hot spots and still respect privacy? (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.

**Rational Choice Perspective** 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 3) 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 a lot more work needs to be done.

**Repeat Victimization** Many 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 7)

**The 25 generic opportunity-reducing techniques**
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 most effective in preventing which class of cyber-crime? (Question 9)
- Which techniques merely displace the criminal activities, and which ones actually diffuse the benefits of prevention? (Question 10)
- All questions suggested in the Phishing case study (Questions 13 . . . 18) and the Online auction fraud case study (Questions 19 . . . 20).

Secondly, the questions related to extending current results specific to the cyber-physical world should take at least 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 5)

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 12)

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 a pendant in the real world. Two examples of such crimes are fraud in Second Life [210], and click fraud [155]. 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.

- How can we apply the empirical evaluation methods of Crime Science to cyber-crime? (Question 11)

For example, we believe that the percentage of cyber-crime that is reported to the police is significantly 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 cybercrime. 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 cybercrime (Approach 21)

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 very specific questions have been raised (Questions 22 . . . 24), all of which lead to the following research approach:

- Use economic methods in the study of cyber-crime (Approach 25)

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 26 . . . 28 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;
- Teaching Information Security as a technology to prevent crime creates many 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 [32]. 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 help and inspiration.

References


36


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](http://dx.doi.org/10.1109/HICSS.2010.287).


