Leveraging The Multi-Disciplinary Approach to Countering Organised Crime

Anna Cevidalli

Technical Report
RHUL–MA–2010–06
31st March 2010

Department of Mathematics
Royal Holloway, University of London
Egham, Surrey TW20 0EX, England

http://www.rhul.ac.uk/mathematics/techreports

ROYAL HOLLOWAY

MSc PROJECT

Anna Cevidalli
Student Number: 100630541

Supervisor: John Austen

Leveraging The Multi-Disciplinary Approach to Countering Organised Crime

An Evaluation for Information Security and Business Professionals

SEPTEMBER 2009

Submitted as part of the requirements for the award of the MSc in Information Security at Royal Holloway, University of London.

Signature Date

ACKNOWLEDGEMENTS

I would like to thank the staff at Royal Holloway and especially John Austen, my Project Supervisor, for their invaluable support and assistance in completing this project.

TABLE OF CONTENTS

1 INTRODUCTION

"The key to formulating effective responsive strategies to cybercrime is to understand the different perspectives that the different actors in the field of cybercrime bring to the subject rather than see them in binary terms as either right or wrong... See, for example, the different, but real, experiences of the business community and the individual user. It is also crucial to hold realistic expectations of what the police can and cannot do."

David Wall, 'Cybercrime, Media and Insecurity:
The Shaping of Public Perceptions of Cybercrime'[1]

If the warnings are to be believed, organised crime is rapidly taking over criminal activity on the Internet, cynically exploiting legitimate business models in the pursuit of huge profit. At the same time, some critics remain doubtful whether such statements can be taken to be authoritative or are merely 'hype'. They highlight the issue that 'organised crime' is an imprecise concept which is very susceptible to subjective interpretation.

A substantial academic literature has developed over half a century to answer the question, 'What is organised crime?' and still the concept remains elusive, complicated by the recent emergence of the online criminal groups. These groups share many characteristics with their terrestrial counterparts yet they are also, due to their sophisticated exploitation of the benefits and vulnerabilities of the Internet, said to be evolving new characteristics whereby they are more educated, innovative and collaborative than the crime groups that came before them. [2]

For governments, law enforcement, Information Security (IS) professionals and others who are tasked with protecting the valuable assets accessible stored on the Internet, 'tried and trusted' resources such as technical countermeasures and the international Information Security Standards, the 27000 series, have existed for some time to combat all types of online threat, including those from organised crime. In the last few years, professionals from all disciplines have recognised that they can no longer work in 'silos' and must collaborate to manage the problem. Considerable progress is being made in this area, for instance with the publication of national cybersecurity and organised crime strategies in the US and UK.

However, if it is true that there is a close correlation between online organised crime and business, perhaps there is another resource available which remains largely

unrecognised and unexploited and which can perhaps be applied equally to legal and illegal ventures, namely the insights which a business perspective can bring to a situation. Is there potential for IS and business professionals (IS/business professionals) to contribute to the multi-disciplinary approach to combating organised crime by applying strategic management methods and their professional knowledge and expertise? Is there mileage in considering online organised crime 'primarily as a business activity' [3] or 'as various forms of business activity which may or may not have attracted the label of criminality'?[4]

This paper explores these issues and related questions, with a view to maximising the resources of IS/ business professionals when risk-assessing technology-oriented organised crime, in particular online organised crime threats.

1.1 Overall Purpose

The overall intent of this paper is to raise awareness about the multi-disciplinary resources for combating online organised crime which already exist and to suggest approaches to assist IS/ business professionals in the strategic management of anti-online organised crime strategies.

It is intended that this purpose is achieved by building on the findings of Gilligan, [5] Gottschalk [6] and others by extending their approach to the arena of online criminal activity.

1.2 Specific Objectives

The specific objectives of this project are to:

- Present a basic overview of some of the different attitudes and perspectives which are associated with the concept of 'organised crime'
- Raise awareness of the diverse range of existing resources for combating organised crime, including online organised crime, that can be utilised by any sector which adopts a multi-disciplinary approach
- Separate the 'facts from the fiction' of organised crime, with specific focus on aspects which most concern IS/business professionals

- Compare and contrast key terrestrial and technology-oriented organised crime characteristics
- Categorise some of the threats and vulnerabilities within modern information technology which online organised crime groups (OOCGs) can exploit
- Briefly highlight the significance of legal/illegal online business models
- Highlight existing theoretical and practical multi-disciplinary methods which IS/ business professionals can utilise when analysing online organised crime data within their specific roles.

1.3 Scope

This paper takes a high-level business management approach to IS and technology-oriented organised crime, with a specific focus on online organised crime. In-depth social, economic and technical assessments of technology-oriented organised crime threats are outside scope as they have been addressed elsewhere and would constitute whole papers in themselves. Wherever possible, the reader is directed to sources of further reading for these and other subjects.

Aside from contextual international references, the paper has an overall Western capitalist perspective towards organised crime.

Due to word limit restrictions and the vast potential scope, the paper is unable to address every aspect of the subject. Consequently, it assumes that the reader is conversant with IS concepts such as 'risk', 'threat', 'vulnerability', 'encryption', 'virus' and 'botnet'.

1.4 Methodology

The methods used in this paper consist of:

- A literature review (books, journals, industry reports, Internet searches) across the disciplines of criminology, sociology, economics, law, commerce and IS. The literature review focuses primarily on post-2000 material and includes both UK and international sources such as government and private sector reports, academic books and papers and media coverage (eg from newspapers and the Internet).

- Tabulation of the key characteristics of terrestrial and technology-oriented organised crime
- Comparison between theoretical online crime characteristics and real-life case studies
- Application of Morphological Analysis within a hypothetical practical context.

Note about Web Sources: This paper recognises that the use of web sources in academic projects continues to be problematic for a variety of reasons, some of which are discussed in relation to the portrayal of high-profile IS incidents. However, to ignore them completely within the context of current organised crime discussion would be to distort the cultural context of the situation. Also, although there are many unverifiable, transitory sources available on the Internet, it is also used as the primary medium for serious news media, academic and technical reference points, interviews and discussions which may not be published elsewhere.

Accordingly, web sources are used within this paper and its references with some caution and predominantly within the following contexts:

- Where the information is from a well-established recognised source (eg the *BBC.co.uk* or *TimesOnline.co.uk* websites)
- To provide links to copies of electronic academic journals
- To provide examples of how the online media industry portrays organised crime
- Where a web source indicates an innovative approach or piece of information which may not have been identified elsewhere.

2 EXECUTIVE SUMMARY

"Amateurs study cryptography. Professionals study economics."

Shostack and Stewart, Ch 5, '*The New School of Information Security*' (2008) [1]

"Looking to the future the equation is simple. Money is going electronic and where money goes so will organised crime."

Bob Packham, Deputy Director General, UK National Crime Squad (2001) [2]

This paper provides a high-level evaluation of organised crime and the threats arising from online organised crime, within a multi-disciplinary perspective. It draws on a range of academic, industry and other materials to distinguish the key characteristics of online organised crime and to identify some of the multi-disciplinary resources which are available to counter it. Real-life case studies and other examples, together with the Tables in the Appendices, are used to demonstrate how contemporary online organised crime is profit-driven and has a strong commercial focus.

The paper is accompanied by a series of Appendices and Glossaries and a comprehensive Reference list (provided within a separate document to facilitate cross-referencing with this paper) that includes suggestions for further reading and research.

Section Three begins by demonstrating how there are many possible approaches which can be taken towards organised crime, which may at first appear confusing, contradictory or overwhelming. It mentions that law enforcement is adopting a multi-disciplinary approach and working in partnership with other sectors, including the business sector, to counter the problem.

Next, the paper attempts to separate the 'fact from the fiction' of organised crime, highlighting the pitfalls of relying on any single source (for instance, media reports or statistics) when analysing the subject. It identifies reliable sources for information about organised crime (for instance, the *United Nations Convention on Transnational Organised Crime* and several established, academic sources) and aggregates some of the key organised crime characteristics from the sources within ***Tables 1*** to ***6*** in **Appendix A**.

Having established that, despite initial impressions, it is possible to obtain a consensus view about theoretical organised crime characteristics within carefully-defined parameters, the project aligns the theoretical criteria against real-life online organised crime case studies. This establishes that, although there are many similarities between terrestrial and online organised crime groups (OOCGs), the online groups also display characteristics which are unique to them, for instance a high dependence on the use of the Internet and transnational strategies.

With regard to online involvement by 'traditional' organised crime groups such as the Mafia, the paper highlights that, although there is some indication in both the theoretical literature and the case studies that traditional organised crime groups are targeting the Internet, the evidence in the case studies suggests that involvement of traditional organised crime groups is not a dominant feature at the moment.

In Section Four, the paper assumes a non-technical IS perspective and describes some of the vulnerable elements within information technology, especially within the structures of the Internet and the Web, which all offenders, including OOCGs, are exploiting. It explains some of the reasons why these vulnerabilities exist and why they are attractive to offenders. In particular, it highlights the serious threat which crimeware, which is often sold and distributed by OOCGs, poses to the Web environment.

In Section Five, the paper shifts to a business perspective, emphasising the importance of understanding online organised crime business models and mentioning the work of particular authors whose work in this field adopts a multi-disciplinary approach.

The paper then uses Morphological Analysis (MA) to demonstrate how a multi-disciplinary approach to strategic analysis can utilise the skills and experience of IS/ business professionals, as well as assisting them to manage the threat which OOCGs may pose to their business.

The paper concludes with the observation from academic and industry sources that directly targeting the profit-making aspects of an online organised crime business may be one of the most effective responses to the problem.

3 OVERVIEW OF ORGANISED CRIME

3.1 Different Perceptions about Organised Crime

'Much of the Mafia image revolves around symbols associated with mysticism …mystification ….and styles of self-presentation….There is drama associated with Mafia identity and Mafia activity, even if much of the actual activity of the people involved in such groups is in fact quite unglamorous and dull.'

Eric Gordy, 'Notes from the Iron Cage' (February 2006) [1]

'An instant gangster classic. This is in a league with the epics of Scorsese and Coppola.'

Quotation from 'Empire' Magazine, cited on the film poster for 'Mesrine: Killer Instinct' (Released in UK, August 2009)

'It's about time law enforcement got as organised as organised crime.'

Rudy Giuliani, Former Mayor of New York (October 1984) [2]

'*Organised crime taking over spam – survey*'

Global Secure Systems (July 2004) [3]

'Organised crime' is an emotive, confusing and controversial subject which can conjure many widely-divergent associations, as illustrated by the examples above. [4] Unlike many other forms of crime, associations with organised crime permeate the consciousness of people all over the world, in subtle ways.

One objective this paper will attempt to demonstrate will be to show that, although it is extremely difficult, if not impossible, to reach a single consensus on the subject of 'organised crime', multi-disciplinary professionals working in this field can use the varying perceptions to their advantage.

3.1.1 The International Perspective

At the international level, the history, popular image and perceptions of organised crime have a long tradition and deep cultural resonance within many countries across the world, as is the case in Italy, the United States and Japan. Crime organisations, in the sense of their most basic meaning of a group of people jointly engaged in activities contrary to their society's designated norms, have existed for millennia [5].

Societal attitudes towards organised crime vary depending on the values of the society in which the organised crime group operates, the robustness of the organised crime

group structure (for instance, whether it is based on an established ethnic or other dynasty), actual or perceived corruption within the State and the extent to which the activities of the organised crime group are perceived to be integrated within the norms of that society.

3.1.2 The Public/ Media Perspectives

To the layperson, 'organised crime' may evoke images of Mafia or other 'gangster chic'. As the first two quotations that head this section illustrate, organised crime retains a mystique due to its inherently clandestine nature and its ambivalent treatment in the media. This mystique, together with the dramatic potential of its 'larger than life' aspects, for instance, escalated levels of violence and the potential for enormous profits, can be exaggerated for dramatic effect, evoking contradictory emotions such as fear and admiration.

At the same time, according to the UK government, the public 'recognises that serious organised crime is a significant problem', with 84% of respondents believing 'it was a very or fairly big problem in the UK, with one in three thinking it was a problem where they live.' [6] A recent UK Home Office report states that the estimated annual cost of organised crime activity to the British economy is in the region of £30 billion and that 'there was a 250 per cent increase' over the previous year 'in the use of malicious programmes' by organised crime groups in 2008 alone. [7]

It is this capacity to superimpose both positive and negative associations without apparent contradiction which differentiates organised crime from other, supposedly more 'mundane' categories of crime [8] in the public perception. Real and mythical criminal gang leaders such as Ronald Biggs, Jonathan Wild, Robin Hood, Fagin, Al Capone, Bonnie and Clyde, the Kray Twins, Don Corleone and Tony Soprano have attained equal status as archetypes within the criminal folklore of the Western tradition.

In many cases, for instance in the case of Jacques Mesrine (the subject of the film in the poster quotation), a factual character is able to achieve iconic status in their country of origin or across the world through their portrayal in the mass media of their age.[9] Literature, films and music available on the Internet and elsewhere may all present mixed messages where such characters are portrayed as anti-heroes, thus encouraging public empathy towards their situations. For instance, dilemmas arising from the 'honour among thieves' secret codes derived from certain crime groups, such

as the *omerta* (code of silence) of the original Sicilian Mafia, can be exaggerated to place the anti-hero within a sympathetic moral and ethical context.

These quasi-romantic associations with organised crime clearly influenced the attitudes of some early hackers. In 2004, *PCWorld* [10] reported the example of one former Russian 'hacker-turned-teacher' who had written a message on *GlobalSecurity.org* which described how, during his childhood, he and a couple of friends hacked programmes and distributed them for free:

'It was like our donation to society …It was a form of honour. (We were) like Robin Hood bringing programmes to people.'

Similarly, Michael Calce, the 15-year-old student from Canada who launched a series of attacks in 2000 against some of the leading commercial websites, including *Amazon.com*, *Yahoo!* and *eBay*, remains more commonly known by the alias he chose to represent his online identity, *MafiaBoy*.

Furthermore, contemporary media treatment of real and fictitious criminal activity as entertainment, for instance the media portrayal of real and fictitious hacking activity, has often been exaggerated and ambiguous. This blurring of fact and fiction distorts the public perception of crime in favour of offenders and can create a false sense of familiarity with the subject. [11]

Recently, software and online games have created a new entertainment category which further blurs the distinctions between real and fictional organised crime, with *Neoseeker.com* listing over 50 software games whose titles have a 'Mob/Organised Crime' theme and that are inspired by both real and fictitious sources. [12]

3.1.3 The Government/ Law Enforcement Perspectives

For governments and law enforcers in capitalist societies, modern organised crime is considered to be 'one of the major threats we face' [13], with an international reach that extends from terrestrial prostitution and narcotics networks through to electronic money-laundering and other forms of new and adapted Information Technology-oriented 'cybercrimes'. In its 2003 *European Security Strategy*, [14] the EU identifies 'organised crime' as one of the 5 key security threats to its members and the 2009 '*State of the Future*' report from the *Millennium Project* highlights the 'enormity' of the

threat of transnational organised crime, stating that: 'Its global income is estimated to be about $3 trillion, which is twice all the military budgets of the world combined.' [15]

In response, Western countries have been updating and creating new national and international laws and agreements. [16] Governments and law enforcement are also forging stronger ties with the private sector and are endeavouring to add to traditional law enforcement and detection techniques targeted at specific crimes by adopting a wider, strategic perspective that addresses the totality of the criminal environment and which seeks 'to cement a collaborative approach and to embrace wide-ranging tactics.' [17]

However, as is also the case with the academic and industry studies mentioned below, it is only recently that technology-oriented organised crime, including online organised crime, has begun to receive specific attention in government reports. [18] As combating organised crime is extremely resource-intensive, it remains to be seen if government resourcing and commitment will be sufficient to sustain their objectives. [19]

3.1.4 The Academic Perspective

For academics, organised crime is 'a slippery concept, notably resistant to precise definition due to its blurring of activities and structures'. [20] As Reuter observes: 'For some, it is a set of relationships; for others, a particular set of activities.[21] Klaus von Lampe [22], on his 'Organised Crime' reference website, cites over 100 different government and other references for sources which provide 'organised crime' definitions, including several from different government organisations.

Although academic literature about the definition of 'organised crime' and its characteristics is extensive (encompassing, for instance, criminology, economic, sociology and legal contributions), relatively little serious academic research has been undertaken to date into researching the multi-disciplinary aspects of online organised crime. Consequently, the potential insights such an approach might bring remain largely untapped and fragmented across different disciplines. [23]

3.1.5 The Victim's Perspective

In the case of victims, their perceptions may vary widely. In some cases, they may be unaware that they are being affected by organised crime at all. [24] In other circumstances, for instance where victims live in societies with long-established

organised crime groups such as Sicily, or where the boundaries between legal and illegal activity are unclear and exploited, such as in Russia or Columbia, they may associate organised crime with fear, violence and repression. Conversely, victims' attitudes may be that organised crime is a semi-mundane aspect of their daily existence or even a necessary evil which compensates for deficiencies of the state.[25]

3.1.6 The Economic Perspective

In the field of modern economics, Becker's ground-breaking 'rational crime' theory, [26] whereby individual crime decisions are calculated by weighing up the 'pros and cons' of the costs (eg the likelihood of punishment) and benefits (eg financial reward) of the situation, continues to be influential. One of Becker's key concepts is the notion of 'psychic' costs (ie non-monetary costs) such as thrill-seeking, which has translated well to the field of sociology, where it aligns with the socioeconomic concepts of 'human', 'social' and 'personal' capital. [27]

With specific regard to organised criminal activity, there are two main schools of thought as to whether 'organised crime' is 'market-based or occurs within the framework of an organisation.' [28] Dick, writing in 1995, [29] proposes a 'transaction cost-based theory of organised crime', based in part on the work of Schelling, who sees 'the organised criminal firm as a formal governance structure that specialises in providing illegal goods and services to downstream buyers'.[30] Dick concludes that transaction costs (ie any costs incurred from buying or selling assets),[31] as opposed to monopoly power (Schelling's theory), primarily determine the activities of organised crime firms. [32]

Citing Anderson's transaction cost analysis study of the Sicilian Mafia, [33] Gottschalk extends Dick's analysis, mentioning that, for offenders, 'considerable transaction costs may arise to avoid profit seizure and loss of personal freedom' when factors such as avoiding the consequences of monitoring by the police and informant activity are taken into account. [34]

3.1.7 The Corporate Perspective

The corporate world, while taking on board the economic factors, will also view 'organised crime' from a risk management perspective. For senior managers, 'organised crime' is one among many potential risks on the list which is currently headed by the impacts of the current worldwide economic recession.

The ability to accurately balance the probable risk from all types of organised crime against other business elements is hampered by the fact that, in the past, businesses have been reluctant to formally disclose information about all types of serious online crimes, for reasons including:

- fear of lost profits
- reputational damage leading to reduced consumer confidence
- losing control of the business (for instance due to potential business continuity issues due to system 'down-time' during formal incident investigation) [35]
- concerns that disclosing third party personal data on the borderline of confidentiality could lead to costly legal challenges (irrespective of whether those challenges had any merit)
- concerns that revealing a serious security breach could expose vulnerabilities which could target further criminal attention towards them.

This, in turn, limited the number of business-specific incidents recorded in industry and government statistics and case studies. Many US States, following the example of California's SB 1386, have enacted legislation which mandates disclosure of loss of personal data. [36] The recent high-profile UK data loss incidents have prompted debate as to whether similar legislation should be enacted in the UK. [37]

This situation is reflected in a speech by former UK Home Secretary David Blunkett at the launch of the 3-year *Business Crime Reduction Centre* (BCRC) Project, part of the EU-sponsored *European Crime Prevention Network*, in which he declared that:

'Crime destroys businesses; from traditional industries to modern companies using advanced IT systems. Businesses across the board have generally had a blinkered attitude to organised crime. Now they face the next major challenge – high-tech crime and the sheer enormity of what can be done with the transfer of information.' [38]

Blunkett's statement captures the current mood of public statements issuing from both the corporate and IS industries in that, until recently, in the main, the threat from organised crime was considered to be a peripheral, non-typical issue for some, though not all, industry sectors. [39]

3.1.8 The Information Security Perspective

To some extent, the IS industry, working in concert with government and law enforcement agencies, has also been aware since at least the last century about the potential for organised crime to exploit online data and to threaten national security. In the late 1980s, the incidents described by Stoll in '*The Cuckoo's Egg*' revealed a far-reaching pattern of transnational, organised online criminal activity and espionage driven by financial payments for technical expertise and information.[40] Likewise, in 2002 and 2006, CERT® [41] was highlighting the affinity between legal and illegal online business models.

However, it was the arrest and conviction in 2004 of members of the international *ShadowCrew* organisation, together with the subsequent identified links between the *Russian Business Network* (*RBN*) and the technically-advanced '*Storm*' (2006) and '*Conficker*' (2008) 'botnets', which captured the imagination of the media and which were instrumental in raising the profile of the scale and sophistication of the problem.[42] Until that time, the predominant IS industry focus had been to combat specific known technical threats to information such as viruses and worms, which were being generated by disparate individuals or small groups with many different motivations including altruism, curiosity, arrogance and peer recognition. Although there were exceptions, many of the earliest hackers were not motivated by profit or found few opportunities to exploit the Internet financially.

Gradually, however, the IS industry has identified significant changes in the membership structures and modes of operation of the perpetrators, which were reflected in the nature of the attacks. Whereas formerly, most attack vectors had been through 'malware', the industry has begun to see a greater number of co-ordinated technical and non-technical blended and multi-layered threats, such as those which are incorporated within crimeware 'toolkits'.

Many IS professionals will now be aware that widely-publicised recent industry reports and white papers [43] are sending a message that 'individual hackers operating independently or groups of hackers with common goals' [44] have been replaced by the underground, highly-complex, sophisticated, technically-advanced and predominantly profit-driven professional organisations such as the *Russian Business Network (RBN)*. These industry reports warn that such organisations are threatening e-commerce and other business sectors at all levels by successfully undertaking the production and

distribution of crimeware such as malicious code on a mass scale, [45] by becoming more collaborative and mimicking or creating similar business models and strategies to those of legitimate markets. [46]

One noticeable trend among some accounts is a tendency to associate online organised crime business models with the hierarchical structures of terrestrial organised crime groups (TOCGs) such as the Mafia. [47] The change among online offenders to employing more strategic and aggressive large-scale tactics led to Keith Laslop of *Prolexic Technologies* (whose network protection company was targeted as part of the Distributed Denial of Service campaign which brought down *The Blue Security Team*) remarking:

'We used to call the Internet a sort of Wild West. Now it's more like Chicago in the 1920s with Al Capone.' [48]

The idea that there are similarities between legitimate and illegal corporate activity is also not new. For instance, in his 1905 essay concerning Marxist capitalism, Bonger [49] quotes a proverb, 'No commerce without trickery' and observes that:

'… with the ancients, Mercury, the god of commerce, was also the god of thieves.'

More contemporary authors have questioned what, if anything, differentiates 'white collar' crime from the activities of 'traditional' crime organisations. [50] Chambliss finds that: 'one of the reasons we fail to understand organised crime is because we put crime into a category that is separate from normal business. Much crime does not fit into a separate category. It is primarily a business activity'. [51] Specific associations between organised crime and commerce are made by Cressey, whose view is that the Cosa Nostra is 'both a business organisation and a government.' [52]

The concept that commerce and crime are closely linked is epitomised by the title of Misha Glenny's book, '*McMafia – Seriously Organised Crime'*, [53] which plays on similarities between the organisational structures and strategies of the underworld and global corporations such as *McDonald's*. Likewise, '*Tony Soprano on Management*' by Anthony Schneider, [54] advertised as an 'offbeat leadership guide' to management techniques, uses the language and imagery of organised crime and applies it at operational level. The role of the 'Mafia accountant' [55] is extant in both fact and fiction

and the term 'the firm' itself, while meaning any corporate enterprise, has a more specific meaning that applies to a criminal organisation.[56]

With regard to OOCGs, the *Russian Business Network* (*RBN*), as its name implies, identifies with the goals of the legitimate corporate world to the extent that it is a profit-driven, multi-national organisation that is structured similarly to a legitimate business.

The similarities between legal and illegal online organised crime activity have particular relevance within the context of IS, for instance because of:

- the tactics which OOCGs employ to mimic legitimate business strategies and models for the purpose of committing online crimes
- the difficulty which people find in distinguishing between real and fake web content, even when they are security-aware [57]
- the psychological propensity for people to trust Internet content more than its terrestrial equivalent [58] by taking the public content of the Internet at face value.

These factors, together with poor authentication techniques and the ease with which e-mails, URLs and other content can be 'spoofed' leave users vulnerable and demonstrate that the adage 'On the Internet, no-one knows you're a dog' continues to apply. [59]

3.1.9 The Challenge of Synthesising Divergent Views

The above examples give a flavour of the wide diversity of mindsets and approaches which can legitimately be applied to this complex subject. All of them have validity and will be recognised within their own fields. A pressing challenge which faces law enforcement and the public and private sector organisations which wish to engage with the 'joint working' approach to combating organised crime at the corporate level is how to understand and synthesise the most significant findings about organised crime from all these disciplines (and others) in order to create a new, relevant and comprehensive holistic frame of reference.

The current challenges for IS/ business professionals at corporate and operational level with regard to all types of organised crime, include:

- Acquiring a clear understanding of the true nature of organised crime as it affects information
- Understanding how to risk assess the extent to which organised crime may be a threat to their particular organisation so that they can implement adequate and appropriate countermeasures if there is a requirement to do so
- Understanding the boundaries of their role and the point at which they may need to involve law enforcement.

It is a premise of this paper that the current tendency for organised crime to use or mimic legitimate techniques provides an opportunity as well as a problem for law enforcement agencies and IS/business professionals by allowing them to apply new management skills and techniques in the risk analysis of criminal situations. As Gilligan states:

'Organised crime, with its multiple character and capacity for adaptivity, is perhaps best thought of as a type of organisational crime and part of a continuum between business and crime. The nature of much illegal enterprise means that many questions about its structures are analogous to those asked of legal enterprise (although of course there are other questions which cannot be asked of legal enterprise). Consequently, an anti-organised crime strategy should prioritise issues of conventional strategic management.' [60]

Choosing to use such an approach opens up a wealth of possibilities, including the use of conventional 'tried and tested' strategic management analysis tools and methodologies. Furthermore, it creates an opportunity for IS/ business professionals to contribute their specific skills and expertise in IS and corporate management to the multi-disciplinary anti-organised crime agenda.

3.1.10 The Multi-Disciplinary Perspective

The multi-disciplinary work undertaken by Gilligan, Gottschalk and others has provided a distinct starting point for investigating these possibilities. Gottschalk takes 'a neutral approach to understanding crime and criminals' and attempts to contribute to 'the

bridge between entrepreneurship and crime'. [61] He brings together the fields of law enforcement, criminology, economics, organisational theories, business management and entrepreneurship with the purpose of defining a contemporary business model of criminal activity 'to a sophisticated level'.

For both Gilligan and Gottschalk, their primary aim has been to analyse terrestrial organised crime business structures for the purpose of assisting law enforcement strategies. The fifth section of this paper explores the potential for their findings, and those of others who take a multi-disciplinary approach, to be applied within an online IS/ business management context.

3.2 Dispelling the Myths

'Organised crime is both more and less than the average person understands it to be. It is more pervasive, more dangerous and more diverse...'

J O Finckenauer, 'The Mafia and Organized Crime' (2007) [1]

The following sub-sections attempt to extract the fact from the fiction of organised crime, in order to clear the way for subsequent analysis to concentrate on the aspects of organised crime which are genuinely significant to IS/ business professionals.

As suggested in Section 3.1, individual perceptions, in particular the extent to which organised crime is perceived to directly impact on everyday business or personal reality, influence the level of importance which different sectors of society in different countries ascribe to the subject of organised crime. An appreciation of these different perceptions is an important cultural consideration for law enforcement officials, IS practitioners and other professionals with an investment in crime prevention and detection, both in terms of stakeholder engagement (for instance, with their own staff, their colleagues from other disciplines or the public) and also to obtain a fuller appreciation of all the factors which may underpin organised crime activity.

It is the joint responsibility of all professionals who encounter organised crime in their day-to-day role to ensure that their own understanding and representation of the subject remains as up-to-date, proportionate to their role, accurate, unbiased, inclusive and supported by evidence as possible, in particular that they avoid unnecessary imprecision, exaggeration and 'hype'. This may appear to be stating the obvious. However, some of the factors which blur the distinctions about this subject can be quite subtle and pervasive, as demonstrated by the examples immediately below, so it is vital that they are explicitly identified and avoided or addressed where appropriate.

3.2.1 The Limitations of Public Pronouncements and Statistics

Public statements from government, law enforcement agencies, the media and the IS industry are always subject to scrutiny. For instance, in 1984, Reuter analysed the relationship between the New York press and law enforcement agencies and concluded that they were engaged in a vicious cycle which ensured the Mafia's reputation was maintained. He found that the media, who treated organised crime largely as entertainment, would report law enforcement activities that featured the

crime groups that were familiar to the public (namely the Mafia) and that law enforcement, in turn, were encouraged to focus on the Mafia knowing that they received Press attention for their activities. [2]

In 2008, Wall [3] singled out the following statement from a House of Lords Science and Technology Select Committee Report:

'But the Internet is now increasingly the playground of criminals. Where a decade ago the public perception of the e-criminal was of a lonely hacker searching for attention, today's 'bad guys' belong to organised crime groups, are highly skilful, specialised and focused on profit. They want to stay invisible, and so far they have largely succeeded. While the incidence and cost of e-crime are known to be huge, no accurate data exist.' [4]

As well as highlighting the lack of credibility arising from the contradictory statements that 'no accurate data exist' and that the 'incidence and cost of e-crime are known to be huge', Wall suggests that there are implied messages that the offenders in question are all-powerful and that the authorities are powerless against them.

Elsewhere, Wall sounds a warning against 'the danger of confusing the rhetoric with the reality' of cybercrime [5], advising people to 'take a critical view' of the production of cybercrime data [6], due to a number of reasons including the lack of sufficient reliable data, the vested and sometimes contradictory interests of the different parties and the different interpretations which can be applied to statistical data. [7]

Although statistical information is quantifiable and is more credible than anecdotal evidence, in its raw form it can be meaningless or misleading. Wall highlights some of the problems associated with the accurate capture and interpretation of statistical information. He cites the example of the 'Incidents reported' item in the intrusion statistics which were formerly produced by the Computer Emergency Response Team (CERT®) at *Carnegie Mellon University*, among others. This item was discontinued because, as CERT® explained, the attacks were now 'commonplace' due to automation, with the statistics regarded as low-level and not representative of actual crimes.[8]

Thus, citing mere numbers of incidents, for instance in a business case for more funding, although they demonstrate that incidents are taking place and may indicate trends, is very context-dependent and may not be of much value when assessing risk.

From a traditional law enforcement intelligence perspective, filtering the potential supply of statistical information is problematic because anecdotal information may have the potential to reveal insights. All information relevant to a case is deemed to be potentially significant on the basis that individual jigsaw pieces of information, when studied together, may reveal a clue which is not apparent when they are examined by themselves (the 'mosaic effect' [9]).

However, for the reasons indicated by the CERT® example above, such an approach encounters difficulties with regard to the analysis of large-scale and widely-dispersed online crimes (such as electronic security audit logs) because the amount of data available may simply be too overwhelming and complex to analyse quickly, inhibiting rapid identification of the salient factors. Some of it may also be stored on inaccessible servers in countries which may be hostile or unwilling to co-operate with particular law enforcement agencies outside their own jurisdiction.

Another statistical distortion with particular significance for law enforcement is the under-recording of online crime. In the case of all potential victims, they may lack awareness about what constitutes a technology-related offence or they may not have a clear point of contact for reporting incidents. They may also be embarrassed or consider the incident to be trivial, with minimal impact, hence not worth reporting. [10] In some cases, they may be fearful of the consequences of reporting because it will reveal they have made a mistake or because they may be implicated as a perpetrator during the investigation.

For corporate organisations, it is only recently that they have begun to adopt formal Incident Management procedures on a wide scale, with the likelihood that, in the past, many incidents would have remained unidentified. Even where incidents are identified, they may not be formally recorded or escalated.

Recently, two new reasons topped the annual Computer Security Institute '*CSI Computer Crime and Security Survey*'. Each year, CSI asks its respondents to record reasons why they have not disclosed incidents, using a scale of 1 to 7, with 1 being 'of no importance' as a reason and 7 being 'of great importance'. In 2008, the main reason cited for not reporting an incident was 'Incidents Too Small To Bother Reporting' (with an average response of 4.33 on the scale), followed by 'Believed Law Enforcement

Couldn't Help' (4.07), which was cited by 47% of the respondents as opposed to 22% the previous year. 'Negative Publicity' was placed third (3.71). [11]

It is unknown whether the high response to 'Believed Law Enforcement Couldn't Help' reflected the participants' belief that law enforcement was powerless to help, whether they felt that some incidents were not criminal and so did not require the assistance of law enforcement, a combination of both or something else entirely. Including these categories in future CSI surveys might clarify the issue.

Once again, for law enforcement, potentially valuable data which could contribute to a 'mosaic effect' may be being discarded as having little significance. Capturing important information by encouraging businesses and the public to disclose incidents, while managing the large response that could result, is one of the reasons why governments and law enforcement are placing a heavy emphasis on collaborative working with the public and private sectors, including raising awareness about the benefits of instigating formal Incident Response procedures.

As well as issues associated with the under-recording of incidents, there is the added difficulty that, in some cases, more data may exist than can be released into the public domain, for instance where law enforcement agencies are following leads from one organised crime group which has been apprehended and which is public knowledge, to another group which is still in operation. A related critical issue is that any serious, in-depth study of organised crime is a risky undertaking, [12] which involves a high proportion of classified data that must be protected and only disclosed on a 'need to know' basis.

Furthermore, serious organised crime, as the quotation at the opening of this section suggests, attracts some of the most dangerous individuals in the criminal fraternity, with most large groups retaining some members whose value is their capacity for resorting to violence. If compromised, information about such groups could jeopardise a criminal investigation that may have been in place for several years or, worse, endanger the life of individuals. Aside from information which is known and undisclosed, since most organised crime activity is covert, there may be little conclusive evidence of a threat until an organisation is actually targeted by an attack.

In terms of threat types, a situation is developing whereby sample collection for new types of threats is becoming 'almost impossible', due to the sheer volume increase in the number of threat types which have combined to form blended, targeted attacks, further complicated by the proliferation of variations of type of threats. [13] For instance, aside from the 'traditional' polymorphic viruses and worms, there are at least 4 different variations of spam type alone. [14] At the same time, whereas many of the earliest IS attacks comprised a single attacker (or a small group) and a single target (from which further attacks could be launched), the current threat landscape often comprises multiple attackers targeting multiple targets simultaneously, as in the case of distributed Distributed Denial of Service attacks. [15]

Therefore, as with all types of statistics, the capture of online crime incident data is not an exact art and interpretations of the same information will vary, depending on the skills, experience and objectives of the people processing the information. Since governments and law enforcement agencies are obliged to rely on statistics to a certain extent as justification for their actions and the headline statistics will be picked up by the press, there is potential for bias and 'hype' in interpreting the data.

Hence, although statistics remain an essential analytical tool (and are recognised as such within this paper), the amount of significance which is given to any individual set of statistics, as Wall highlights, in particular statistics which concern complex subjects such as organised crime, must take into consideration the different elements of the totality of the context in which the statistics are collected. Writing in 2007, it is his view that there is, as yet, insufficient data to support definitive statements about the current cybercrime threat landscape. There are also too many 'unknowable unknowns'. Therefore, (in 2007) there can be no 'experts' and statistical results must be considered with caution. [16]

Unsubstantiated, abstract references to 'organised crime' as an indiscriminate danger to society may also distort a situation. They may place 'organised crime' in the same category as threats from 'weapons of mass destruction', a concept which is currently perceived as 'crying wolf' due to repeated warnings which are to date unsubstantiated by empirical evidence. [17]

Despite the issues surrounding high-profile security incident public statements, they do appear to have some impact. In this year's '*2009 e-Crime Survey*', 42% of respondents said that knowledge of high-profile incidents in other organisations had been the main driver for increased security investment last year. [18] As with other professions, the IS industry has capitalised on the reporting of 'signal events' such as '*Conficker*' (signal events are perceived to be of particular significance and impact) by governments and the media, in order to raise awareness of its activities and concerns. This is a double-edged sword in that, while it is true that media accounts are a fast and successful way to engage the attention of the public, media interests and values are not necessarily the same as those of the IS industry, which can lead to distortion between the source of the information and its media portrayal.

In the case of the reporting of all technology-oriented crime, the potential for exaggeration or distortion is compounded by the inherently-dramatic associations with the entertainment industry which were described in Section 3.1.2.

Although statements such as the following, from *Baselinemag.com*, and the examples provided in the References [19] are legitimate journalistic techniques to make articles more eye-catching and entertaining, they may create a side-effect which may detract from the seriousness of an event and reinforces the 'glamorous' stereotypes that are derived from the imagery applied to TOCGs:

'*ShadowCrew* is a Web mob, say law enforcement officials: a highly-organised group of criminals. Unlike the American Mafia or the Russian syndicates, however, these Web mobs work solely in the online world…. Members …. commit their crimes in the darkness of cyberspace.' [20]

(The statement that these 'Web mobs work solely in the online world' and are not associated with terrestrial groups is not necessarily the case, as will be highlighted within Section Five of this paper.)

Bearing in mind the above examples, it is important for IS professionals involved in media handling and IS awareness-raising to choose the way they express their statements about organised crime with care, to avoid sending mixed messages, reinforcing distorted organised crime group and ethnic stereotypes, infringing

intellectual property rights (for instance, those of films or television) and attracting accusations of trivialisation, exaggeration or sensationalism.

3.3 Defining the Realities

(The problems in defining organised crime are) *'…not from the word "crime" but from the word "organised"… The fact that organised criminal activity is not necessarily organised complicates that definition process.'*

US President's Commission on Organised Crime (1986, P 25) [21]

The exact definition and nature of 'organised crime' (or even whether 'organised crime' can be defined at all) is a popular topic that has occupied the thoughts of academics for over fifty years. As there are many substantial, easily-accessible resources on the subject widely available elsewhere, with much of the pertinent literature pre-dating the age of the Internet, in-depth analysis and justification of generic organised crime characteristics is not undertaken in this paper.

Nevertheless, as Kaspersky points out, organised crime must be understood before it is addressed. [22] Since there can be no single consensus, it is necessary for any paper about 'organised crime' to choose its terms and theories from among the many which are available, to clearly define and explain them and to demonstrate that the sources for these terms and theories are reliable, traceable and supported by fact. Failure to do so can lead to misunderstandings, confusion and flawed decision-making due to the plethora of possible interpretations.

Additionally, in the context of this paper, the following questions require clarification before more specific consideration of possible countermeasures can be undertaken:

- What is an organised crime group?
- What is a technology-oriented organised crime group? How is it different to a terrestrial organised crime group? Are technology-oriented organised crime groups 'new forms of criminal organisation' as has been claimed? [23]
- How serious is the threat from technology-oriented organised crime groups to valuable information? What tools do organised crime groups employ?
- To what extent can the structure of technology-oriented organised crime groups be said to resemble those of their terrestrial equivalents? How significant is this observation to IS/ business professionals?

These are important questions at a practical level for IS/ business professionals. Currently, there is a lack of clarity as to what exactly constitutes an OOCG, the

measures which are appropriate for IS/ business professionals to take to identify and respond to potential OOCG activity and, most importantly, whether this type of threat requires any specific precautions in addition to those which may already be in place for other types of online crime.

3.3.1 Organised Crime Groups

Although a single consensus among academics and other sources about the definition of organised crime is probably not achievable and may not be appropriate because of the huge scope of the subject, Article 2 of the *United Nations Convention on Transnational Organised Crime* (UNTOC) definition [24] has achieved a certain measure of acceptance at international level.

UNTOC recognises that global networks of organised criminals exist in both the terrestrial and the online communities. Their sphere of influence far exceeds that which applied to the 'traditional' organised crime groups that existed throughout most of the last century, with the United Nations 1999 Global Report on Crime and Justice stating that: 'From the perspective of organised crime in the 1990s, Al Capone was a small-time hoodlum with restricted horizons, limited ambitions and merely a local fiefdom.' [25]

Articles 2(a) – 2(j) (*Use of Terms*) of the Convention provide high-level definitions for a range of organised crime aspects, [26] with the negotiators of UNTOC opting for a broad definition in order to capture both the hierarchical and the less formally-structured organised crime groups. [27] As with all high-level definitions, those of UNTOC can only be a starting point and cannot address all eventualities. However, they do express some useful concepts, namely:

Organised Criminal Group:

- Defined minimum size of an organised crime group ('three or more persons')
- Continuity ('existing for a period of time')
- Collaboration ('acting in concert')
- Criminal intent ('with the aim of committing one or more offences')
- The use of direct or indirect methods ('direct or indirect')
- Financial or other material goals ('financial or other material benefit').

Structured Criminal Group:

- Formed for a planned purpose ('not randomly formed for the immediate commission of an offence')
- Fluid, changeable roles, membership and structure ('does not need to have formally-defined roles for its members, continuity of its membership or a developed structure').

Article 5 (*Criminalisation of the Participation in an Organised Crime Group*) of the Convention adds further detail about the types of activities which are deemed to be criminal and within its scope, including:

Article 5 (b): ' Organising, directing, aiding, abetting, facilitating or counselling the commission of serious crime involving an organised crime group'.

Article 5 recognises that associated activities must be included within the crime, as well as the crime act itself.

The Convention takes into consideration other important international organised crime factors such as corruption, money-laundering activities and extradition arrangements. However, by necessity, it does not incorporate all the characteristics which are usually associated with organised crime, particularly at 'operational' level, for instance the use of violence.

In order to provide a slightly more practical and detailed picture, some of the most prevalent terrestrial/technology-oriented organised crime group characteristics identified by a representative sample of sources have been extracted and summarised, via a 6-stage reductive process, within ***Table 1*** to ***Table 5*** in Appendix A. These characteristics are then mapped against real-life OOCG criteria in ***Table 6***.

Tables 1 to 5 comprise the following:

Table 1 – Raw data extracts which identify typical terrestrial/ technology-oriented organised crime group characteristics, from well-established sources

Table 2 – Rationalised version of the raw data from ***Table 1***, with sources cited

Table 3 – Raw data extracts which specifically identify typical technology-oriented organised crime group characteristics, from a typical range of sources, with sources cited

Table 4 – Comparison between ***Table* 2** data and rationalised version of the raw data from ***Table 3***, with sources cited

Table 5 – Comparison between typical terrestrial/technology-oriented and specific technology-oriented organised crime group characteristics in summarised form.

Perhaps the most important point to make about the sources for the first 2 tables is that they do not strictly represent terrestrial crime group characteristics per se. It is perhaps more accurate to say that they represent characteristics which have been identified as definitely applying to TOCGs (for instance, in the case of the earlier sources) and which, for some of the sources (eg UNTOC), may also apply to technology-oriented groups as well.

As is typical of 'organised crime' discussion, most of the items have been the subject of debate between different schools of thought (for instance, about the exact nature of 'organised crime' structures), which are outside the scope of this paper.

The intention of all the tables is to define some initial theoretical parameters for organised crime group criteria, by creating representational snapshots from attributed sources, for the purpose of using these parameters as a basis against which to map actual examples and case studies.

The tables also demonstrate that, despite differences of opinion about detail, there is in fact some agreement among the different sources as to the nature of organised crime groups. In particular, they agree that terrestrial organised crimes have some sort of structure (although they may disagree as to the exact nature of that structure), that violence and corruption are significant organisational strategies and that TOCGs have a tendency towards continuity.

For business professionals, ***Tables 5*** and ***6*** can provide an initial indication of the true nature of 'organised crime' without unnecessary levels of detail. From a multi-disciplinary perspective, the tables include items which may be of specific interest to different sectors. In particular, the under-representation of items within the 'Organisational Culture' category may indicate that this is an area which requires further research, or where existing research and findings may need to be aligned more closely with other disciplines.

For IS professionals, use of ***Tables 5*** and ***6*** may assist rapid identification of significant factors suggesting online organised crime involvement within an IS incident. (This idea is further explored within Section Five.)

The items in each table have also been mapped against the following 6 categories:

1. **Organisational Structures**
2. **Organisational Goals**
3. **Organisational Strategy/Tactics**
4. **Organisational Maturity**
5. **Organisational Culture**
6. **Organisational Environment**.

These 6 categories have been created to demonstrate that all the table characteristics can be mapped within a business organisational context. This, in turn, provides a context for simple analysis of each item from a business and IS perspective, in addition to the more usual criminological and sociological perspectives.

This framework, together with the items within it, provides the basis for the analysis which takes place in subsequent sections of this paper.

Considered collectively, the items in the tables include many characteristics which could equally be applied to legitimate businesses, such as 'Having a commercial or business-like structure' and 'governed by explicit rules and regulations'. However, other items, such as 'code of secrecy' and 'uses illegal violence or bribery' are not typical of legitimate business structures and strategies and show that, fundamentally, the groups remain distinctive and dissimilar excepting in circumstances such as borderline 'white collar' crime, where there may be some overlap.

From an IS/IT perspective, it is also interesting to note that, even for the more recent sources, distinguishing types of communications content and levels of technical/non-technical ability or usage are not identified as significant factors for TOCGs.

3.3.2 Technology-oriented and Online Organised Crime Groups (aka 'Cybergangs'[28])

'It is not clear, at this stage, whether there are 'traditional' organised crime groups operating within the technology-enabled crime environment, or whether there are simply criminal groups who happen to be organised,'

'Future Directions in Technology-Enabled Crime: 2007 – 2009' Report, Australian Institute of Criminology [29]

'These aren't geeks. These are serious and organised criminals.'

Serious Organised Crime Agency (SOCA) (April 2008) [30]

Having established some parameters for terrestrial/technology-oriented organised crime characteristics, the next step is to identify some real-life case studies against which to test the items in ***Table 5***, in order to begin to determine to what extent the characteristics of technology-oriented organised crime groups are distinct from those of terrestrial groups. As before, the purpose of this exercise is not to provide a conclusive set of items but to provide a baseline of potentially significant criteria as a starting point for further analysis in this paper or elsewhere.

It is also important to mention that, in reality, the notion of clear demarcation lines between terrestrial and technology-oriented organised crime groups is somewhat artificial. As information technologies become more accessible and more countries and societies incorporate information technologies within their business structures, so that increasing volumes of valuable information and transactions take place electronically, some of the activities of many more TOCGs will inevitably become 'technology-oriented'.

However, at the moment, by comparison with their terrestrial equivalents, the technology-oriented groups remain either in a transition state (where the groups are evolving from terrestrial sources to a more technology-oriented focus) or are still in an early stage of evolution (where the groups have been created specifically in response to advancements in technology). Both types have relevance within the context of this paper.

The other contextual issue in relation to the tables which must be mentioned concerns the definition of 'organised crime' yet again, this time in relation to the definition of technology-oriented organised crime. Partly due to the comparative newness of the subject, there is a common tendency across the literature, including some of the IS

sources, to refer to technology-oriented organised crime in the abstract without attempting to explain what they mean by it (this is somewhat understandable given the general difficulties with pinning down the subject).[31] Thus, whereas the terrestrial characteristics for this paper were extracted from a wide potential pool of possibilities, there were fewer specific definitions of the technology-oriented organised crime group characteristics from which to choose.[32]

Another important point to highlight at this stage is the rapid evolutionary nature of the technology-oriented organised crime groups whereby, by comparison with the historic terrestrial groups, they can form and disperse very rapidly on a 'virtual' international basis with relative anonymity due to the information and communications benefits of the Internet, in many cases without any requirement to physically meet. Also, the risk and effort involved in committing their crimes, especially if directed specifically at information stored on the Internet, may be much less than undertaking a physical equivalent. Some of the factors which assist online organised crime groups to commit their crimes are discussed further in Section Four.

Consequently, although comparisons can be made between the characteristics of terrestrial and technology-oriented groups, they do not start from a level playing field because of the huge advantages which the technology-oriented crime groups currently enjoy. This point has not been lost on the TOCGs and they are diversifying their activities to exploit these advantages, which again blurs the distinctions between the two types of groups.

Up to this point, the paper as a whole has taken a very theoretical and high-level approach to both terrestrial and technology-oriented organised crime characteristics and activities. The next step is to begin to ascertain to what extent the items identified in the tables are supported by empirical evidence from real-life case studies.

Although there will continue to be references to terrestrial organised crime where relevant, the focus from hereon in will be to consider specific threats which technology-oriented organised crime activities can pose to the valuable information assets of businesses, the relevance of their business models and the possible countermeasures which IS/business professionals can take to counter them.

---

4 TECHNOLOGY AND ORGANISED CRIME

4.1 Online Organised Crime Groups and Information Technology

'*Technology is increasingly becoming a facilitator for organised crime. New types of fraud such as data streaming of payment cards have emerged in recent years, and traditional forms of crime such as money laundering, drug sales, the dissemination of child abuse material and prostitution have evolved as a result of technological developments. The internet has had an especially profound effect on crime.*'

2006 Europol Organised Crime Threat Assessment (OCTA)
(Quoted on Page 53, EU High Tech Crime Centre Report, 2007)

'There are 'new crimes, new tools' committed against computers and IT networks … and there are 'old crimes, new tools' … traditional crimes, supported by the use of the Internet and high technology …'

Len Hynds, UK National Hi-Tech Crime Unit (February 2006) [1]

Having examined some of the theoretical concepts of organised crime, this section will consider online organised crime from an IS perspective, within the context of key information technology developments in the real world, drawing on data from international reports and IS white papers. [2]

A range of representative, high-profile, real-life online organised crime scenarios to accompany this and subsequent sections is provided in **Appendix B**. This section further discusses ***Table 6*** of **Appendix A**, which provides data for analysis in both Sections Four and Five.

Within ***Table 6***, the 2 columns which represented the terrestrial/OOCG characteristics in ***Table 5*** have been reconciled into one. The characteristics from the real-life scenarios have then been mapped against these consolidated theoretical equivalents. This process demonstrates that, between them, the real-life scenarios, although a small sample, embody most of the terrestrial/online organised crime characteristics which were identified in ***Table 5*** and that many of the theoretical terrestrial items continue to be relevant within the online environment. At the same time, the OOCGs exhibit some additional distinctive characteristics, in particular their transnational nature and their reliance on using the Internet and the Web.

At this stage of the paper, the case studies and ***Table 6*** highlight 3 important points:

a) Although the sample group of case studies is small (12 cases), within each case study there are so many numerous individual types of crimes and actual incidents that the full extent of the activities will never be known. This supports the notion discussed in Section Three whereby measuring crimes by number of incident or crime type may not be a true reflection of the situation.

b) Of the 12 cases, only 3 of the groups (*The HangUp Team, The RBN* and *Rock Phish*) are known to be still operating under the same identity. Members of the other groups have either been apprehended, or they dispersed when their forums and other enterprises were deactivated. Whilst it is true that disbanding OOCGs often has an immediate high impact (for instance, in the case of the dissolution of *ShadowCrew*), the membership of large groups may take years to investigate and arrest, during which time the group may continue to be extremely resilient by, for instance, going underground and re-emerging or regrouping under a different guise (as may have happened in the case of the *RBN*).

c) The sources for five of the 12 examples cite associations with 'traditional' TOCGs such as the Mafia or the Triads (Item 2). However, although in one instance the activities of the group are formally Mafia-led, these online groups are all composed of a composite of international terrestrial and OOCG members (Item 22), creating organisations which, although they have many recognisable terrestrial organised crime group characteristics, are also distinct in themselves.

Before undertaking further analysis of elements within ***Table 6*** in Section Five, it is necessary to explain how such groups have evolved and why they choose the attack vectors that they do. For this, it is useful to trace their evolution alongside that of modern information technologies.

4.1.1 Specific Threats Posed by Online Organised Crime Groups

Just as the legitimate world has undergone a technological revolution since the late 1970s, driven largely by the evolution of the micro-chip and the Internet, 'so too has organised crime evolved, adapted and, in some cases, innovated.' [3] The new information technologies, as with all innovations, have created opportunities and risks for both legitimate and illegal enterprises, some of which are categorised in Section 4.1.2. [4]

OOCGs pose specific threats to electronic information simply because they undertake activities of greater complexity and on a much larger scale than those of individual offenders. Working as a dedicated team or on a casual basis with other offenders, OOCGs can maximise their exploitation of the vulnerabilities within information technology (in particular the Internet), human behaviour and international legislative frameworks.

As well as exploiting existing vulnerabilities, these groups are at the forefront of designing the current wave of crimeware and associated techniques, as exemplified by *the RBN* and *Rock Phish* groups in the case studies. It is the online environment, and websites in particular, which provide the most successful and lucrative targets for them. [5]

Although the types of information and technology attributes which can be exploited by all types of offenders is too extensive to list here, some of the more important items are provided in **Appendix D**. The section below outlines some of these attributes which have been specifically targeted by OOCGs.

4.1.2 Key Attributes of Information and Technology exploited by OOCGs

4.1.2.1 Anonymity

One reason why offenders can exploit anonymity is that, while strong authentication techniques such as RSA SecureID and SSL Certificates [6] are widely-available and popular within some environments such as e-commerce, they are sometimes not employed in order to save money, to speed up transactions or where information is deemed to be low-risk, hence not worth protecting. In the case of SSL, it is often deployed one-way, to verify the website and not the claimant. Thus, as with many vulnerabilities outlined here, mitigating security controls do exist but are often not implemented.

Distributed technologies, as opposed to centralised, tightly-controlled systems, also contribute to the complexity of design which in turn facilitates anonymity. This complexity can be exploited to launch mass 'swarming' attacks against networks or websites from anonymous machines located across the world. Organised crime groups

have used the threat of DDoS attacks and 'ransomware' against online businesses to support their extortion demands. [7]

The automated mass production capabilities of 'botnets' (networks of compromised machines), when combined with the worldwide membership profile of OOCGs, greatly increases the anonymity and complexity of the potential attacks and reduces the likelihood of apprehension. Some of the most prolific 'botherders' are said to be part of OOCGs in Russia [8] and a large proportion of spam (currently estimated to comprise 97 per cent of all business e-mail) [9] is said to be linked with them.

As well as using 'botnets' directly in random or targeted attacks, OOCGs have been identified as orchestrating the 'bot market' trade, whereby 'botnets' are sold or hired for profit, in a structure that has been said to resemble that of the illegal drugs business. [10]

Along with terrorist organisations, these groups are also reported to be customers for the 'bot market' services. Recently, a joint report from an internet compliance company and an internet service provider reported that 90 per cent of the sponsored advertisements for online pharmacies generated by *Microsoft's* '*Bing'* search engine were probably associated with Eastern European and Russian organised crime and illicit drug networks. [11]

For all organised crime groups, anonymity is also a major factor in the success of electronic money-laundering. As demonstrated by the *Triad Gang (Australia)* case study example, the funds to be laundered are converted, often via an international trail of electronic transactions involving complicit and/or unsuspecting 'mules', into desirable currencies such as e-gold [12] and US dollars.

4.1.2.2 Electronic Currencies, Payment Systems and Online Banking

'Virtual' environments such as e-commerce, online casino and gaming sites can generate greater profit than their terrestrial equivalents, using far fewer resources. As mentioned above, because they deal in 'e-currencies' (aka 'e-cash'), they can also be used to money-launder illicit funds.

A report by *Kaspersky Labs* in 2007 [13] described the problem of counterfeit versions of online games, which are used to generate real-world profits, as well as outlining how

virtual passwords and virtual property are 'stolen', through malware and other means, for resale to the original owner or elsewhere. Likewise, a CERT® [14] report warned in 2007 that 'protection rackets' among online game players had been reported in South Korea, whereby vulnerable players were being targeted by organised crime group 'gamers', who threatened them with adverse consequences unless they paid the group real or virtual currencies.

Within the financial markets, 'an increase in online transactions has been matched by an increase in fraud,' facilitated by increased direct customer interaction with their online accounts, 'the lack of contact between parties' (exacerbated by the use, in some circumstances, of insecure authentication techniques), the automation of the process and the continuing reliance on the input of bank card numbers and other credit card credentials to verify transactions. [15]

Despite widespread security awareness campaigns about the issue, users continue to be easily tricked into revealing their online financial account details through social engineering techniques using spam and phishing attacks, trusting strangers' website, e-mail and telephone communications without question. 2009 figures from *APACS*, the UK payments association, showed a 132 per cent increase in online banking fraud over the previous year, amounting to £52.5 million, with an increase in both phishing and malware incidents. [16] The success of phishing and malware is largely attributable to OOCGs, as demonstrated by the pioneering activities of the *Rock Phish* online crime group in the case studies.

As with other types of scam, such as fake online dating and job scams, collaboration between offenders, for instance by asking a user to go through a series of processes whereby they are contacted by different people, greatly increases the chances that the user will believe that they are engaging with legitimate entities.

As well as direct attacks on financial data, the capture of a single individual's identity can lead to other types of crime, for instance the forgery of passport information using real credentials which can then be sold or used to commit further offences.

4.1.2.3 Extraterritoriality

'Extraterritoriality' is 'the notion that the Internet has no geographic boundaries'. [17] This concept formed part of the original model for the Internet, which was designed for open communication and not security.

4.1.2.4 Globalisation

Increased economic co-operation (for instance, with the increased membership of the European Union) and the dominance of multinational corporations increases the amount of information traversing the Internet, with the result that organisations are increasingly reliant on their international communications mechanisms. Communications and transactions flowing across the Internet are cheaper, faster, more efficient, simpler to execute and can be accessed easily by many more people than has ever been possible before.

However, the awareness and implementation of security technologies has not matched the commercial development, creating vulnerable 'hot spots' where illegal activities can focus.

As Gilligan [18] remarks, such 'contemporary realities of globalisation' have contributed 'to an increasing economic element in debates about organised crime', with this trend being very noticeable in IS industry reports. Gilligan argues that it is 'the increasing anonymity of market forces in a globalising economy' which are facilitating 'the assimilation of organised crime groups into … late-modern capitalism', for instance within the financial services sector. [19]

4.1.2.5 Increased Commoditisation of Information

The data-centric aspect of the Internet has encouraged the commoditisation of all types of information, including personal information (for instance, in the form of biometrics) and commercially-sensitive data which, together, comprise some of the most prized assets for offenders to target for intelligence-gathering, fraudulent use or resale.

In addition to the overt data, the Internet has accumulated huge stores of discreet, ancillary background data, including cached data (data stored in a temporary location for later reuse) and metadata (information about the properties of data files), due in

part to variable housekeeping practices and the relatively inexpensive cost of online storage.

As well as being vulnerable to social engineering attacks, such as those associated with phishing, many users still do not appreciate that their personal information has a monetary value, together with a non-financial value, and is vulnerable to exploitation. As an example, although the impact of ID theft, a popular attack vector for OOCGs, on victims can be very significant, far-reaching and complicated, there remains a disparity between the security awareness of different types of victims with regard to the value of their own personal information. [20]

Offenders, including organised crime groups, who understand the value of personal data very well since, in many instances, they are setting the prices, simply harvest personal information to sell via illegal online auction forums. Information stored on the Internet provides an entry point for access to a much larger pool of potential victims than was previously possible and, because the information is publicly-available to anyone, it can be extremely difficult to establish a trail of evidence between the original information compromise and any subsequent criminal activities.

Targeted attacks bring the OOCGs into closer contact with their victims than may have been possible in the past. There is a possibility that, in situations where the attack has involved an element of personalisation, for instance where sensitive personal data which the victim believed to be confidential has been compromised, the emotional impact on victims may be greater than if they had been targeted randomly by an automated attack or by a single individual because they may feel powerless against a group, leaving them vulnerable to extortion or blackmail attempts.

As well as creating new opportunities to generate profit entirely via the Internet, this commoditisation of information has also resulted in ‘profound’ changes in the traditional activities of serious organised crime communities, as mentioned in the OCTA report quote at the opening of this section. Paedophiles and other traders in illegal contraband have established complex international online communities where digital information, for instance in the form of sexually-explicit photographs, are viewed, shared and bartered. [21]

4.1.2.6 Interoperability and Interconnectivity

Modern interoperability and interconnectivity capabilities of hardware and software enable individuals and organisations to communicate across the world with interconnected networks, as well as to incorporate different applications within a single device.

From a security perspective, complex interconnectivity erodes the concept of a traditional 'security perimeter', whereby individuals and systems are either within a distinct security perimeter or outside it. This creates difficulties for security analysts, for instance when deciding whether to strategically place firewalls within the security perimeter or within the Demilitarised Zone (DMZ).

As emerging hardware and software technologies such as Voice over IP (VoIP), *Blackberries* and *iPhones* become increasingly compatible and interconnected, successful unauthorised access at one source may lead to other information compromises within linked systems, for instance where levels of security design quality are variable across different applications.

Across the Internet, Web 2.0 services provide greater control and media-rich options for users when interacting with web content than ever before, for instance when using social networking sites. Greater choice introduces greater complexity, for instance when choosing which security controls are appropriate.[22] Additionally, placing services on the Internet further complicates the capacity to define a distinct security perimeter.

The blurring of security perimeters is reflected at the human level as well, whereby employees of an organisation and third parties will often share the same computer equipment. This factor, in addition to those outlined immediately above, can create legal corporate governance accountability issues if the information on that equipment is compromised.

Perhaps most significantly, the potential for increased access across multiple systems poses a potential significant risk if any of the individuals using the equipment are working against the interests of their employer. Several of the case studies in **Appendix B** mention that the organised crime groups used the assistance of insiders to infiltrate the organisation's systems, thereby completely bypassing any controls at the security perimeter.

Insider threats can arise at any level of the organisation, from senior management teams through to technical network systems administrators. In the latter case, these administrators may have permissions which formally allow them to access any information on the organisation's network. In March 2009, CERT® published a report investigating the connection between malicious insiders and the Internet underground economy. [23] The report found that the threat from such insiders was 'very real', that they were often motivated by revenge and that it could be difficult to identify them. [24] Additionally, a separate industry survey in June 2009 reported that 74 percent of 400 senior IT UK and US professionals volunteered the information that they could circumvent their organisation's security controls. [25]

Recent security reports have also highlighted the potential threat from the current economic climate, whereby many skilled Information Technology professionals in formerly prosperous economies are being made redundant. There is a possibility that an increase in the number of disaffected ex-employees and low morale among the employees that remain in an organisation could lead to similar issues as those which apply in some countries of the former Eastern Bloc and elsewhere, [26] namely that, due to a lack of legitimate opportunities, these individuals will add their skills to the existing criminal 'underground economies'. [27]

The above categories demonstrate how many modern information technologies continue to have inherent vulnerabilities which can easily be exploited by OOCGs. The next sub-sections focus more closely on 2 of the elements which OOCGs have combined to gain a competitive advantage over other offenders, namely crimeware and the Web.

4.2 The Problem of Crimeware

The total threat volume from malware is an increasing problem. Approximately 700,000 new types of malware are being identified per month, with one in four US computers estimated to be infected. [28] Currently, offenders are eschewing the former pattern of high-impact, single event attacks [29] which can completely destroy the value of the assets, in favour of devising more long-term strategies which employ more complex, covert, technically-proficient, scalable (across different platforms), resilient and effective methods than ever before.

In 2008, the OECD estimated that, over the previous 5 years, although there had been a decline in worm-related incidents by 25%, there had been a 30% increase in Trojan-related incidents, with a 500% increase in malicious programmes. [30] This figure supports the trend highlighted by the UK Home Office (previously mentioned) which identified a 250% increase in 'malicious programmes' between 2007 and 2008 alone. Industry analysts have identified that malware is now often located on legitimate websites, including government and news websites, which act as unknowing 'parasitic hosts'. [31] This is a trend away from relying on a user to access a malicious website (for instance, containing attractive illicit material) of their own accord. Together with 'drive-by downloads', the use of legitimate websites makes it more difficult for the user to distinguish between innocuous and malicious websites because the fake websites appear 'very convincing'. [32]

The emergence of 'crimeware' as a sub-set of malware has been a major milestone in the commercialisation of online organised crime attack vectors and is a significant factor behind the growing trend towards deploying blended attacks. This was identified early in the 21st Century, when 'a marked shift occurred in the online threat landscape', whereby offenders diversified from writing malicious code ('malware') to new and more concerted profit-driven criminal techniques ('crimeware'), created with the specific intent of yielding large financial returns. [33]

A joint report sponsored by the US Dept of Homeland Security Science and Technology Directorate in 2006 observed that most crimeware attacks were being undertaken by organised criminals and that the growth of keylogger-specific crimeware and the sites distributing such crimeware reflected the 'growing commoditisation of crimeware technology and the use of multiple hosts, such as botnets, for distribution and data collection'. They also found that the multiple web sites per attack increased the difficulty of 'shutting down malicious web sites to stem the spread and impact of crimeware.' [34]

These new types of crime groups form an industry of dedicated organised criminals who 'treat their malicious activities as a full-time job rather than a hobby', resulting in many different types of new and sophisticated products. [35]

Although it is difficult to assign exact figures to the crimes that are being committed, for the reasons discussed in Section Three, industry reports indicate that the problem

continues to increase and is a serious issue for businesses. [36] For instance, one 2009 industry report has found that '91 percent of all compromised records,' obtained from a sample of 90 confirmed breaches comprising 285 million individual records, 'were linked to organised crime groups.' [37] Although the IS industry is continually developing new strategies to combat the threats behind such statistics, due to the sheer number which are emerging and the mass industrialisation of the crimeware process, it remains impossible to address every single new variation on an individual basis.

From the offender's perspective, with so many new and 'traditional' malicious code options available, in many circumstances they do not even need to adapt or create a new product. Instead, they can simply 'recycle' old threats (for instance, in 2007/8, the Master Boot Record (MBR) rootkit was reconfigured to prevent detection) [38] or employ existing products that are considered legal such as adware, spyware and keyloggers, with malicious intent. [39]

For these reasons, malware and crimeware remain valuable and successful assets for offenders, who buy and sell different variations, often packaged together within simple to use crimeware 'toolkits' (thus creating a blended threat at the same time as increasing the potential customer base), through their illegal terrestrial and online markets. [40]

The latest crimeware is mainly distributed via the exploitation of human and technical vulnerabilities, for instance via dedicated social engineering (such as including a malicious attachment in a seemingly benign e-mail about a topical news item), exploitation of servers, browsers and workstations (for instance, via the propagation of viruses and worms) and by manual means, or through a combination of these schemes. [41]

Once installed on the equipment, the malware, in particular if it is part of a 'package' installed via a rootkit, can launch many overt and covert attacks against its host or another system, either on its own or as part of a botnet.

Although it has been noted that statistics must be treated with caution, the evidence is overwhelming that the current malware distribution environment of choice for offenders is the Web, which is discussed in more detail overleaf.

4.3 The Internet and the Web as Attack Vectors

The predominant tool and target for launching malicious attacks is now clearly the Web, [42] with 90% of all attacks arriving via Web threat vectors by the end of 2008 [43] and a new webpage infected every 4.5 seconds. [44] Between them, China, Russia and the US currently account for 'almost three quarters' of the websites spreading malware, with 85% of the pages affected residing on legitimate websites, as mentioned previously. [45]

Reasons why the Web is an attractive target include its popularity with users (with 93% of UK companies in the 2008 BERR [46] survey reporting that they had a corporate website), its continuing relative novelty as a technology, the variations in the level of security applied to publicly-accessible websites which hold valuable information, the amount of valuable information which is stored there and the improved security controls which are now routinely applied at e-mail gateway level, [47] thereby making them less vulnerable targets.

The Internet provides both a target in itself and a new set of techniques [48] within the offenders' criminal 'toolbox' for facilitating crimes within both the terrestrial and online environments. Traditional 'tools' adapted for the Internet include tools that support money-laundering, fraud and extortion. [49] These were already well-established and versatile and have translated easily to the online environment, which they can exploit for large rewards with minimum effort.

The Internet has also provided many new tools for offenders, most of which are incorporated within the latest crimeware, as described previously. Because these new tools, such as web-hosted services, are not tried and tested, they include vulnerabilities which can be exploited. In the case of Web 2.0 services, although they offer many commercial advantages, for instance in terms of scalability and cost efficiencies, it may be extremely difficult to track exactly what is happening to the information. [50]

Increasingly, information on the Internet is being stored or transferred outside the core business. The technologies which support these strategies 'are changing the entire nature of who has what information at what given time and who controls it'. [51] Where third parties who may be hosting the data, either on the Web or on other network

infrastructures, are located abroad, it may also be difficult or expensive to audit their activities to the necessary level. [52]

Finally, offenders exploit the curiosity or fear of users and the immediacy of information provided by the Web and newsworthy events occurring in the physical world. [53] 'Scare-ware' is estimated to have affected over one million users worldwide, [54] with the number of rogue anti-malware programs in circulation rising from 2,850 in July 2008 to 9, 287 by December 2008, a three-fold increase in 6 months. [55] As well as causing serious problems to users, fake security applications can undermine trust in legitimate security products and adversely affect the reputation of the IS industry.

Having considered some of the tools and techniques which OOCGs use to threaten individuals, legitimate businesses and information, the next section further addresses the types of crime which take place, from a business perspective.

---

5 THE BUSINESS OF ORGANISED CRIME

5.1 The Importance of Online Organised Crime Business Models

'*… Now it would be too difficult to conduct business … DarkMarket was our bridge to business and if that bridge is broken then that business is broken …*'

'Iceburg' (*sic*), participant in the illegal *DarkMarket* online forum (September 2008) [1]

There are many approaches which can be taken when analysing the structures which underpin OOCG business models, some of which are based on academic terrestrial organised crime models applied to the online environment. [2] This section takes as its starting point Gottschalk's 'enterprise paradigm' approach (based on the ideas of Symeonidou- Kastanidou [3]), whereby an organisation has 'entrepreneurial structure' if it has the following 3 elements:

a) Allocation of roles – Whereby the members of a group are 'exclusively tasked with planning and preparation activities' (ie each is allocated specific duties)
b) Hierarchy – 'When a predetermined superior-inferior relationship exists among members of the organisation.'
c) Concrete structure – 'When a group possesses its own assets.' [4]

With regard to business models as a concept, as with the organised crime group structures, although many different types have been identified, this section will restrict itself to discussing those which have been applied to the activities of OOCGs. In particular, it will explore the extent to which claims in industry reports that OOCG business models are similar to those of 'traditional', hierarchical organised crime groups such as the Mafia have validity and relevance for IS/ business professionals.

Gottschalk's overall approach is based in part on Albanese's 'consensus definition' (2004 version) of organised crime group characteristics [5] which argues that the enterprise model of organised crime grew out of dissatisfaction with both the hierarchical and ethnic models that had previously dominated the criminology landscape, [6] a theory that focuses on economic considerations, as opposed to hierarchical, network or ethnic issues. [7] Gottschalk also mentions that this theory has been adopted by the FBI within their law enforcement strategy to combat transnational

organised crime and that it 'assumes that legal and criminal organisations have similarities.' [8]

The major characteristics of the illegal enterprise, as defined by Albanese and Gottschalk and accepted by this paper with specific reference to the online environment are that:

- Organised crime and legitimate businesses both involve similar activities at 'different ends of a spectrum of legitimacy of business enterprise'
- Violence and ethnic exclusivity are not necessary in order to enhance profit
- Violence and corruption are means to the end of profit and market share
- The criminal organisation is 'rarely centrally-organised due to the nature of the markets and activities involved.'

These characteristics are consistent with the findings in ***Table 6***, where violence, corruption and ethnic exclusivity, although present in some of the case studies, are not defining characteristics for most or all of the groups. In particular, a strong tendency against ethnic exclusivity is indicated by Item 24 ('Includes both national and foreign members').

One slight variation between Gottschalk's approach and that of this paper arises because Gottschalk and Albanese's analysis is predominantly about organised crime groups in general, as opposed to OOCGs in particular. The full range of criteria captured in ***Table 6*** of **Appendix A** may be more representative of the diversity of OOCGs than any single set of criteria within it (for instance, Albanese's), irrespective of how useful these single sets of characteristics may be in other contexts. Consequently, this paper will continue to use ***Table 6*** in **Appendix A** (which includes Albanese's 2008 set of criteria) as representing a broad consensus definition of OOCG characteristics as they are currently formed, whilst recognising that this stage of their evolution may be temporary. [9]

Gottschalk also mentions the findings of Lyman and Potter who distinguish between 'criminal groups', (reactive structures that respond to fluctuations in market supply and demand) and more long-term 'criminal businesses' which, although they have many similarities with legitimate businesses, are essentially criminal in nature and bound by the constraints that apply to all illegal enterprises. [10]

Although it is possible to allocate the case studies in **Appendix B** between Lyman and Potter's categories, thereby providing a snapshot as to the structure of those groups at that point in time, the fact that some of the groups were apprehended before their plans came to fruition renders the exercise inconclusive. This is because there is a possibility that, if the enterprises had been successful, some of these particular groups might have then evolved from 'criminal groups' to 'criminal businesses' which capitalised on their initial successes, whereas others might have chosen to dissolve.

A closer approximation may be to apply Evans' distinctions, also mentioned by Gottschalk, which differentiate between criminal 'enterprises' (whereby 'a group provides an illegal good or service on an ongoing basis'), criminal 'networks' ('an enduring association of criminals', possibly across different groups, which may utilise the skills of any or all of the members when committing any specific crime) and criminal 'ventures' (a single 'criminal episode usually engaged in for profit by a group'). [11]

Even so, several of the groups in ***Table 6*** (for instance, *ShadowCrew* and the *CardersMarket* conglomerate), because of their organisational structures, whereby sub-groups may have their own identities within the main group, could qualify for both the 'Criminal Enterprises' and 'Criminal Networks' categories. Although a similar arrangement might also exist for some TOCGs, the OOCGs have an advantage in that they can exploit the benefits of the infrastructure of the Internet and Web 2.0 services, as mentioned in the previous section, which enables their own structures to be very flexible, depending on the demands of particular situations, inhibiting the capacity to define them precisely.

The above observations continue the trend described in previous sections of the paper whereby different aspects of organised crime are too elusive to define within narrow boundaries. However, at the same time, adopting a broader approach, based on established opinions and evidence, whereby it is accepted that there may be several different types of organised crime group, all of which may have some validity at this time, appears to be supported by the data in the tables and the case studies.

Such an approach, although it remains evident that there are many areas of this subject which continue to require further analysis, enables IS/business professionals to move beyond a starting point where organised crime may appear to be an overwhelming and complex subject towards a position where aspects of the subject

may be quantifiable within the context of their own businesses, as long as they are defined within agreed parameters.

The next step of the process is to consider some of the main business-related characteristics of OOCGs which are highlighted by the case studies and ***Table 6***.

5.1.1.1 Organisational Structures (Category 1)

Within Category 1, the key factors which emerge are that all the examples demonstrate a formal structure, with a strong bias towards collaboration, division of labour and specialisation. From the evidence, links with established TOCGs (where these groups follow the structure of organisations such as the Mafia) are apparent, although they do not appear to be an essential component for online success. (However, this particular definition does not incorporate the transition economy structures of Eastern Bloc 'mafiya' organisations, which are believed to have links with *The RBN*, among others.)

Within the industry literature, some reports [12] directly associate the structure of OOCGs with those of the Mafia, often borrowing from R C Lindberg's *Structure of a Mafia Crime Family*. This was one of the first essays to highlight the similarity between modern Mafia structures and modern corporations and which places the 'Capo' at the top of an eight-stage, rigid, structured 'chain of command' hierarchy which includes 'advisors', 'financial advisors' and 'enforcers'. [13]

However, Finckenauer [14] refutes this approach as an interpretation of the methods of Russian organised crime, finding 'no evidence of a complex hierarchy or set of hierarchies' and, specifically, no evidence 'of mafia-like structures or activities'. Instead, he states that they 'often create flexible, project-oriented structures similar to some licit organisations.' Furthermore, he warns that identification of Russian organised crime activity with that of the traditional Mafia 'may actually create a self-fulfilling prophecy', pointing out that:

'A criminal group gains stature when it is called 'mafia', which only heightens its power.' [15]

The evidence in ***Table 6*** supports Finckenauer's findings by suggesting that hierarchical structures might apply in some specific situations (in particular, in the *Banco di Sicilia* incident which involved the Sicilian Mafia directly, as well as any money-laundering activity such as that conducted by the *Triad Gang (Australia)*) and

not in others. In the case of the *RBN*, their structure and activities, although originating in Russia, were more service-based and laterally-distributed across the world, with varying degrees of central control.

The case studies demonstrate both hierarchical and network structures, with a strong tendency towards 'swarming' activities (for instance, where multiple attacks may come from all directions). The inclusion of network structures, together with the variation within the structures themselves, supports Gottschalk's appraisal that: 'Organised crime can best be understood in network terms', with a key characteristic of large networks being that they may display strong ties at the centre, with weaker ties at the borders. Gottschalk also mentions that trust, a characteristic that does not feature at all in the tables, is a fundamental characteristic of networks. [16]

This trend is supported by *Symantec's 'Report on the Underground Economy'* characteristics, represented in ***Table* 6**, which identified that web-based forums tended to be loosely-structured. [17]

In addition, there is the issue, as discussed before, that legitimate and criminal organisational structures share many similarities. In this case, roles are assigned at different levels with the management roles at the summit and the least-status, less-skilled roles at the base for both types of organisations, thus reducing the extent to which such structures can be said to be distinctively associated with groups such as the Mafia. Applying such roles to a situation may yield useful information in terms of how a criminal business operates. However, there is nothing about the placement of the roles themselves that suggests they are intrinsically 'criminal'.

5.1.1.2 Organisational Goals (Category 2)

All the case studies were formed for a 'planned purpose' (as opposed to haphazardly) that included 'financial or other material goals' such as obtaining 'valuable data.' There is some evidence of monopolistic tendencies in 5 of the groups (cross-referenced with Category 6) although the defining characteristic of this category is 'exploitation of the online market'.

The evidence from industry reports is fairly conclusive that the activities of many OOCGs are currently focussed on 'financial or other material goals'. [18] Although OOCGs may be involved in a wide variety of endeavours within both legitimate and

illegal markets (in particular where they participate in the 'shadow economies' that have arisen in countries which are in transitional economic states, [19] where their activities, although deemed officially illegal, may also be unofficially state-sanctioned), within the context of the Internet and the Web, most of their activities are currently targeted against the financial and service industries, for the reasons mentioned previously in Section Four.

From a business perspective, this trend is evident from the types of business models with which OOCGs are currently associated, as demonstrated in industry reports [20] and the case studies, where employing collective, subscription and online auction business models have proven to be particularly successful strategies. Even at the basic level of representation within the case studies, it is evident that the structure of the groups which evolved was closely aligned with their business model choices, as opposed to being aligned with the ethnic or other cultural factors which played a significant role in the evolution of 'traditional' TOCGs. It also follows that the activities of these groups are (or were) strongly business-focussed as opposed to being, for instance, ideologically-focussed.

As with legitimate organisations, the choice of an appropriate business model for contemporary OOCGs is a fundamental key to their success. It is evident from the choices they make that, in some circumstances, they are mimicking successful business models from the legitimate sector, for instance that of *eBay*.

Each business model type identified, including the detailed information about specific tactics within them (as highlighted within the 'Category 3' section below), contains a wealth of potential clues for law enforcement and IS/business professionals to analyse. As demonstrated by the work already undertaken in some IS industry reports, for instance by *Symantec*, it is possible to create a baseline profile of specific OOCGs from the clues they leave in the information about them on the Internet and elsewhere. As mentioned in Section Four, digital information includes large amounts of cached data and metadata, the latter being a property which is not available within its terrestrial equivalent. Both cached data and metadata can potentially be monitored and analysed alongside the more overt information.

Both legitimate and illegal enterprises must protect the information which ensures the integrity and viability of their business processes as well as their technical systems. [21]

They both rely heavily on the Internet when conducting their activities. Currently, both are obliged to use some of the same infrastructure routes and types of applications to communicate, where they will both leave logical audit trails. Therefore, just as OOCGs scrutinise legitimate business structures, strategies, data and communication paths for signs of vulnerabilities, employing collaboration and specialisation as tactics, so too can these same tactics be employed by groups of legitimate multi-disciplinary professionals, each sector specialising in the skills most appropriate to them.

Furthermore, as expressed in the quotation at the beginning of this section, where the business model collapses, the whole criminal enterprise may collapse as well. This vulnerability is an additional feature which may be exploitable by multi-disciplinary teams. In particular, although they cannot employ the same illegal methods as offenders, business professionals can employ the same tactics that they use to evaluate business competition to identify potential vulnerabilities within criminal business structures. Similarly, IS professionals may be able to utilise their risk assessment skills to identify some of the potential risks to the information of criminal organisations, as part of the work of a multi-disciplinary team.

The ability to interpret business models is an important analytical tool for multi-disciplinary law enforcement and public/private sector teams. Within those teams, it is the business community which has the most skills and experience to theoretically analyse the business models of criminal organisations. Furthermore, it is IS professionals, among others, who may be able to provide an early detailed, risk analysis of a developing online organised crime threat, based on evidence from their knowledge of the risks to information, their roles as first-line contacts for Incident Management processes or the monitoring activities they undertake which can identify irregularities in security audit logs or other security processes.

Additionally, as alluded to in the quotation from Wall at the beginning of the Introduction section, it is unrealistic (for instance, due to limited resources) for the police to take responsibility for addressing every aspect of a problem that is as large and complex as organised crime. Consequently, the most effective way to counter the problem is to distribute the tasks involved to the sectors that have the most relevant experience to assume them.

5.1.1.3 Organisational Strategy/Tactics (Category 3)

This category is by far the largest, containing the most identified characteristics, with 10 characteristics which are displayed by all the groups. Most of the groups comprise both national and international members, although the degree of influence which non-national members may hold varies (for instance, in the *Banco di Sicilia Incident* example, the group was managed by the Mafia), depending on local culture or the purpose for which the group was formed (for instance, in the *Triad Gang (Australia*) example, Australian Triad members had links with individuals in Malaysia, as well as Russia, which facilitated money-laundering activities).

OOCGs systematically mimic detailed features within legitimate business models in order to engender trust in their victims (for instance, when mimicking legitimate websites in phishing attacks), as well as to blur the distinction between their own activities and those of the legitimate sector (as demonstrated by the *McColo* example in the case studies, where the whole business was ostensibly legitimate yet which, on further inspection, proved to be a 'front' for illegal activities). The *ShadowCrew* and *CardersMarket* examples from the case studies, in particular, also demonstrate how mimicking a legitimate business model can foster a sense of legitimacy among the criminal community.

Other examples of innovative tactics which OOCGs and other offenders have borrowed from the legitimate commercial sector include: [22]

- Establishing 'rogue ISPs' to co-ordinate the distribution of illegal content such as malware and hard-core pornography
- Creating 'misleading applications', in particular the 'scareware' security applications, which may do the opposite of the stated purpose
- Creating 'instructional videos' as part of a criminal product package
- Applying 'Copyright Notices' to their malware (eg to Trojans)
- Including 'Terms and Conditions' statements with their products which include reporting non-compliance to legitimate anti-virus companies.

By comparison, bribery, corruption and violence, key criminal tactics of terrestrial groups, are less evident in the case studies for the online groups. This disparity may arise because OOCGs behave in a different way to terrestrial groups, although it may also be the case that further analysis needs to take place into these factors before a

clear trend can be deduced. Finckenauer's [23] observation that violence is a typical tactic of Russian organised crime groups but that monopolisation and corruption are not, may also be indicative that this is an area where terrestrial and online organised crime tactics diverge.

Any evidence of characteristics such as corruption, violence and extortion is significant within an online context because they mark the cross-over points between legitimate and illegal enterprises. [24]

5.1.1.4 Organisational Maturity (Category 4)

The primary factors identified within Category 4 are continuity and innovation, together with professionalism and sophistication. There are strong elements of social engineering (for instance, through phishing attacks) and proficient concealment of money transfer activities.

Gottschalk identifies 4 basic stages of growth for a criminal organisation, with each stage focused on either:

Opportunity (Stage 1), Activity (Stage 2), Knowledge (Stage 3) or Strategy (Stage 4), with Stage 4 being future-oriented. [25]

One aspect of OOCGs, as demonstrated by the case studies, is that, because they are able to muster resources and skill sets very quickly from a wide range of sources, they are able to achieve Stage 4 of this maturity model much more quickly than their terrestrial counterparts. For instance, *ShadowCrew* was able to establish itself as a 'market leader' within 2 years of its inception and all the case studies, irrespective of the length of time they existed, qualified as 'professional and sophisticated' (Item 54).

5.1.1.5 Organisational Culture (Category 5)

Although in theory 'Organisational Culture' could be a broad category containing many items, in practice the evidence in ***Table 6*** suggests that it may be under-represented in academic literature at the moment with regard to online organised crime. There is some evidence that some online groups manipulate their characteristics (for instance,

in the case of *The HangUp Crew* who have a strong online identity) to create a strong brand image.

5.1.1.6 Organisational Environment (Category 6)

As with Category 5, there are relatively few criteria cited for 'Organisational Environment' by comparison with some of the other categories. However, there has been a strong tendency for the groups to take advantage of jurisdictional arbitrage, together with evidence that they are exploiting the web-based marketplace.

There is also some evidence of monopolistic tendencies in 5 of the groups (cross-referenced with Category 2) although the evidence appears to support the modern supposition that criminal markets are more likely to be based on competition than monopoly. [26]

Within the 6 categories of ***Table 6***, the case studies tend to 'cluster' against specific items such as jurisdictional arbitrage and exploitation of the online market, whilst being much more thinly distributed or not represented at all against others (in particular, some items in Categories 3 and 5). This may suggest that there are some factors which are more favourable to the success of the groups than others or perhaps that additional research might be beneficial.

Up to this point, this paper has considered different aspects of online organised crime, with a specific emphasis on the multi-disciplinary, academic, IS and business perspectives. The final part of this section proposes a model which can synthesise key characteristics from across the paper, in particular data extracted from ***Table 6***, within an established strategic analysis problem-structuring methodology, for the purpose of leveraging the multi-disciplinary approach to organised crime.

5.2 Strategic Analysis and Online Organised Crime Groups

As previously stated, the overall purpose of this paper is to demonstrate how practical methods drawn from the multi-disciplinary approach to organised crime can assist IS/ business professionals in identifying key factors within potential online organised crime situations which may be of relevance to their specific environments. This section offers one such tool, Morphological Analysis, as an example of this premise. [27]

Because the multi-disciplinary approach to organised crime is very much in its infancy and, at the moment, continues to be strongly influenced by a criminology ethos, there are as yet few widely-available tools and techniques available for use by multi-disciplinary teams for the specific study of online organised crime. Although many crime analysis software applications currently exist, [28] some require specialist skills to use, which may not be appropriate for the commercial sector, or their use may be restricted to intelligence or law enforcement authorities.

In circumstances where there is a possibility that online organised crime activity is involved and which requires further investigation, IS/ business professionals need access to simple-to-use, generic tools which can help them quickly identify the key elements of the situation, from which position they can undertake more in-depth risk analysis procedures as necessary. In particular, they require tried and tested tools which they can utilise immediately without 'reinventing the wheel'.

There are a number of business approaches and techniques which have been identified for use with law enforcement and which can easily be extended for use within multi-disciplinary environments. Most notably, Gottschalk [29] and Ratcliffe [30] demonstrate how established strategic analysis techniques such as maturity models, trend analysis, morphological analysis (MA), process mapping and SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis are relevant to the organised crime environment. All of these tools will already be familiar to many business professionals and, although they may have been devised for terrestrial environments, can be applied equally to known factors within online legitimate and illegal business environments.

Furthermore, Albanese [31] who has been a major influence within the field of organised crime, has proposed a risk analysis methodology for organised crime, within the

context of a 'market and product-based model'. Albanese's basic premise is that, rather than targeting organised crime individuals and groups (an approach which has limitations because of the diversity of crime group types and because the incentive for undertaking the crimes is not eliminated as new crime groups will always emerge to fill any gaps), a more productive contemporary approach may be to identify the highest-risk specific products and markets, 'knowing that these markets will attract the offenders that law enforcement seeks.' [32]

One of the intentions of this paper is simply to raise awareness of the relevant literature about online organised crime which already exists, together with the commonly-available established tools and techniques which can be used in multi-disciplinary anti-online organised crime environments, such as those mentioned above. This section of the paper will conclude with a practical illustration of how one of these techniques, morphological analysis (MA) [33] can assist any sector within a multi-disciplinary anti-organised crime team, either individually or working together, to undertake initial assessments of potential online organised crime incidents.

The following section is a summary of the explanatory information which is provided in **Appendix C**. In addition, the Appendix applies the methodology within a theoretical scenario.

5.2.1 Employing Morphological Analysis within a Multi-Disciplinary Context

Morphological Analysis (MA) 'is a qualitative method used to explore a range of different possible explanations for a number of issues' by dividing the problem into different elements and displaying them in the form of a matrix that visually represents the 4 steps of the analytical process. [34]

As its purpose is to provide a holistic interpretation of a situation, MA requires multi-disciplinary input to be truly effective. One of its key benefits is that the MA processes ensure that all input is managed and that input and decisions are trackable to their source.

MA is intended to be used during the early stages of exploratory analysis, for instance within multi-disciplinary situations where, although some data is available, the quantity

may be insufficient to undertake meaningful quantitative analysis or, as often occurs when considering organised crime, there are a wide range of possible scenarios which need to be reduced to those which are most feasible for the given situation.

The 4 steps of the MA process are:

1. Break down the problem (identify the broad elements and categorise them)
2. Create a morphological matrix
3. Develop possible explanations or outcomes
4. Grade the explanations (eg from most feasible to least feasible).

The first step of the process is to identify the problem to be identified (for instance, how might online organised crime activity be affecting our business?).

The categories within the matrix can be composed from any set of issues affecting the problem. Items within the categories are listed horizontally. Once the matrix is completed, it is read downwards and across to create pairs of associations. Where the pairs are not inherently consistent or may not be relevant to the situation they are discarded.

Professional judgment is exercised in order to extract the most significant possibilities from within the matrix, with these items being further assessed against additional factors, such as feasibility.

At the end of the process, a list of scenarios has been identified through a process of systematic analysis and elimination which, although brief, between them capture the key issues which need to be addressed.

The value to multi-disciplinary professionals, in particular IS/ business professionals, is that this is a straightforward, simple method which enables them to pool their skills and expertise to solve a problem. The method is 'tried and tested' over several years and has been proven to work within a variety of diverse contexts, including scientific and business contexts.

The particular benefit of applying this method to an online organised crime scenario is that it can utilise criteria from other sources (for instance, the items in ***Table 6*** or any list of items which categorise organised crime characteristics) and it can also form the

foundation for subsequent work using other complementary methods, including risk and impact assessment tools.

Therefore, morphological analysis is a useful tool for any environment and is well-suited for the analysis of online organised crime information.

---

6 CONCLUSION

'There's a war out there …A world war. And it's not about who's got the most bullets. It's about who controls the information. What we see and hear, how we work, what we think – it's all about information. … The world isn't run by weapons anymore, or energy, or money. It's run by little ones and zeros, little bits of data. It's all just electrons.'

Cosmo, hacker character in the film 'Sneakers' (1992) [1]

This paper began by highlighting some of the issues, including widely diverse interpretations of the term 'organised crime' and distortions associated with media portrayals and statistical processing, which have inhibited the work of law enforcement and other anti-online organised crime professionals. It described some of the multi-disciplinary initiatives which are being devised to counter the problem and demonstrated that it is possible to define a broad range of organised crime characteristics which are representative of online organised crime activity, based on traceable, established sources.

The paper then explored some of the threats which online organised crime poses to the business community, from a non-technical IS perspective, before focusing on the business strategies and tactics which are used to commit the crimes. Within this process, the paper highlighted how OOCGs, in part because of the transnational nature and scale of their activities, as well as their ability to use advanced strategic and technical skills to successfully exploit the vulnerabilities within information technology, pose a genuine threat to the valuable assets of all types of business, as current industry reports indicate.

The paper observed that, as with the legitimate sector, reliance on the Internet's communication mechanisms, as well as sound business models, underpin the success of OOCG enterprises. It noted that, as well as providing a powerful tool, OOCGs' reliance on well-known business strategies and public information travelling across the public Internet may create vulnerabilities which can be exploited by the legitimate sector.

The paper concluded with a demonstration of a strategic analysis tool which can integrate with the other existing analytical and risk assessment tools used by the business, for the purpose of capitalising on the skills and experience of a multi-disciplinary anti-organised crime professional team.

The paper highlighted the following key issues:

1. There is a need for clarity of definition in all reports about 'organised crime'.
2. There is a need for IS/ business professionals to familiarise themselves with a basic understanding of organised crime, so that they are ready for any specific threats they may encounter, as well as to ensure that their countermeasures (including the publication of reports and security awareness materials) deliver the intended results as opposed to reinforcing inaccurate stereotypes.
3. Statistics about the numbers of online organised crime incidents have limited value of themselves when applied to online organised crime activities. They must be evaluated within the total context of the incident or situation. For instance, a single identified online organised crime incident may comprise many thousands of individual data breaches.
4. The real-life case studies corroborate the industry findings that online organised crime is distinctive from terrestrial organised crime. In particular, successful OOCGs are transnational, well-organised and can understand and exploit the properties inherent in all types of information and the continuing loopholes in legislation. They commoditise all types of information for profit and have capitalised on the benefits of modern technology such as Web 2.0 services to utilise the Internet and the Web as both an attack tool and an attack target.
5. OOCGs are largely responsible for the increasing trend towards the commoditisation of malware, for instance in crimeware toolkits, as well as for fostering a commercial business approach among online organised criminals.
6. There is a distinct though fragmented field of academic and industry research which analyses organised crime (and online organised crime to a lesser extent) from the perspective of its business strategies (as opposed to, for instance, employing a criminal law enforcement perspective). These research findings are corroborated by the evidence within the real-life case studies.
7. Some of the elements of organised crime have received much more academic attention than others (for instance, the cultural aspects of online organised crime remain relatively unresearched).
8. Morphological Analysis (MA) is a useful simple tool for helping multi-disciplinary anti-organised crime teams to quickly identify the key issues in a situation and to effectively share and update their skills and experience.

9. There is scope to integrate online organised crime business strategy analysis (such as MA and the other relevant approaches mentioned in this paper) within existing law enforcement and IS risk assessment strategies.
10. A multi-disciplinary approach to countering online organised crime is the most effective and efficient method of capitalising limited resources.

In conclusion, the paper ends with observations from some of the sources. Whereas in the past, intelligence and detection strategies have focussed on identifying individuals (for instance, organised crime leaders) and crime groups, as well as on 'follow the money' tactics, these often result in a temporary reduction in the problem. [2] Just as OOCGs use blended attack strategies for maximum impact, so it is necessary for countermeasure strategies to also incorporate a range of defensive and detective methods, including both technical and non-technical countermeasures, ideally identified by a multi-disciplinary team of professionals.

One of the most effective countermeasure strategies may be to create an environment where the strategies which the OOCGs use are no longer effective or financially lucrative. For instance, IS/ business professionals can continue to work collaboratively with organisations such as ICANN to shut down offenders' access to network and systems infrastructure. [3] The effect of this strategy is that it adds significantly to the transaction costs of the online organised crime businesses and adjusts 'the risk/reward equation' to a level whereby 'these activities become less profitable and attractive', [4] concepts which are based on the theories of Becker and Dick, among others, which were mentioned in Section 3.1. Therefore, the vulnerabilities of the crime group's business may be identifiable via the familiar legitimate business concept of economic analysis.

Additionally, as has been observed by Emigh and Ramzan, [5] because OOCGs are mainly motivated by profit, 'a successful countermeasure need not be bullet-proof, but merely good enough that it renders the attack unprofitable.' Strategic analysis techniques such as Morphological Analysis, when used in conjunction with existing analytical tools and resources, can assist multi-disciplinary teams business teams to identify and target these vulnerable points, thereby maximising the effectiveness of the team's resources and leveraging their multi-disciplinary approach to countering organised crime.

---

7 REFERENCES

All URLs were correct as at 2 September 2009.

Full details of months and years are provided where available.

On occasion, minor punctuation corrections have been made to quoted texts in the interests of clarity and accuracy. UK spelling conventions (eg 'organisation') are used.

---

1. INTRODUCTION

1. D S Wall: P 59, '*Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime'* (International Review of Law, Computers and Technology, Vol 22, Nos 1-2) (2008)
2. D S Wall: Pages 39-44, '*Cybercrime'* ('Crime and Society Series', Polity) (2007)
3. W Chambliss: '*On the Take: From petty crooks to presidents*', Page 53 (Bloomington: Indiana University Press (1978)
4. G P Gilligan, P 1, '*Business, Risk and Organised Crime*' (Journal of Financial Crime, Volume 14, No 2) (2007)
5. G P Gilligan, '*Business, Risk and Organised Crime*' (Journal of Financial Crime, Volume 14, No 2) (2007)
6. P Gottschalk: '*Criminal Entrepreneurship*' (Nova Science Publishers, Inc, New York) (2008)

---

2. EXECUTIVE SUMMARY

1. This quotation is in no way intended to disparage cryptographers. It alludes to the fact that cryptography is a tool of the business, whereas economic strategy is a business driver.

   A Shostack and A Stewart: Chapter 5 headings, Pages 82-106, '*The New School of Information Security*', (Addison-Wesley, Professional) (2008)

2. Bob Packham, Deputy Director General, UK National Crime Squad: NCIS Press Release, '*Launch of the United Kingdom's first National Hi-Tech Crime Unit*' (18th April, 2001)

   Available at: http://www.cyber-rights.org/documents/ncis_1801.htm

---

References

3.0 OVERVIEW OF ORGANISED CRIME

1. Eric Gordy, The Iron Cage.blogspot.com (Notes from the Iron Cage): '*Organised Crime: Mafia symbolism and 'branding*' (Clark University) (February 2006)

   http://the-iron-cage.blogspot.com/2006/02/organized-crime-mafia-symbolism-and.html

2. Time.com – Page 8, '*The Sicilian Connection*' (October 1984)

   http://www.time.com/time/magazine/article/0,9171,923697-8,00.html

3. Gss.co.uk: '*Organised Crime Taking Over Spam – Survey*' (July 2004)

   http://www.gss.co.uk/news/article/1105/go

4. J Albanese, on Page 77 of the '*Handbook of Organised Crime in the United States*' (1994), highlights the issues associated with defining 'organised crime' from the sum of its parts by referring to the Indian parable of the blind men and the elephant:

   (Eg) See Randy Wang, Princeton University: '*The Blind Men and the Elephant*' (1995)

   http://www.cs.princeton.edu/~rywang/berkeley/258/parable.html

5. Susan W Brenner, '*Organised Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships'*, Page 12 (North Carolina Journal of Law and Technology, Volume 4, No. 1 (2002)

6. UK Government: Page 9, '*Extending Our Reach: A Comprehensive Approach to Tackling Serious Organised Crime'* (UK Government Report, Crown Copyright) (July 2009)

7. UK Government: Pages 1 and 2, '*Extending Our Reach: A Comprehensive Approach to Tackling Serious Organised Crime'* (UK Government Report, Crown Copyright) (July 2009)

8. The BBC.co.uk article '*Profile – Ronnie Biggs*' (August 2009) describes the impact of media support on Ronald Biggs, the leader of the Great Train Robbery gang, whereby Biggs and the media exploit his colourful criminal career via overt financial and media exposure exchanges:

   The article describes how he became a 'celebrity fugitive', with his evasion from capture drawing 'a sort of fascinated admiration from the British press and its readers. Less publicised was the fate of one of Biggs's victims …' It also mentions that his 'notoriety meant that he was able to regularly charge newspapers for the "scoop" that he was coming home' and that the punk band, the *Sex Pistols* had 'used him as a vocalist'.

   The article mentions that the media even played a role in Biggs's extradition: 'It was *The Sun* that finally brought Biggs home in May 2001, when he was very ill.' In July 2009, Jack Straw refused Biggs parole on compassionate grounds, stating that he remained unrepentant and had 'outrageously courted the media'. This decision was ultimately reversed in August 2009 to take into account Biggs's acute failing health.

   http://news.bbc.co.uk/1/hi/uk/3548190.stm

9. Jonathan Wild – Wild's activities as 'thief-taker general' in the 17th Century were widely-reported, including satirical accounts by Daniel Defoe and Henry Fielding; Robin Hood – Semi-mythical popular English folk character; Fagin – Fictional character in Dicken's '*Oliver Twist*', based on the real Victorian criminal Ikey Solomon; Al Capone – United States 1930s gangster leader who specialised in smuggling and bootlegging; Bonnie and Clyde – Leaders of a gang of roving United States bank robbers, depicted in popular song and film; 'Ronnie and Reggie' Kray – East End gangsters whose activities have become part of the cultural history of the East End of London; Don Corleone – Iconic fictional character from the film, 'The Godfather' and its sequels, based on the novels of Mario Puzo; Tony Soprano – A fictional character from the successful television series, 'The Sopranos'.

10. IDG News Service - 'PCWorld': '*Viruses: From Russia, With Love?'* (May 2004).

    http://www.google.co.uk/search?client=qsb-win&rlz=1R3GGLL_enGB336GB336&hl=en&q=pcworld,+from+russia+with+love

    Cited in: N Kshetri: Page 8, '*Pattern of Global Cyber War and Crime: A Conceptual Framework'* ('Journal of International Management, Vol 11, No. 4) (December 2005)

11. It is interesting to contrast the BBC article about Ronnie Biggs cited previously with their equivalent article about hacker Gary McKinnon, published in the same month. The BBC.co.uk article, '*How Gary McKinnon Became a Cause Celebre*' (August 2009), documents the impact of the media support for McKinnon, including the lobbying campaign by *The Daily Mail.* The article includes a chart which shows the rise in the number of references in the press to Gary McKinnon between 2002 (18) and the first seven months of 2009 (225).

    http://news.bbc.co.uk/1/hi/magazine/8181100.stm

    D S Wall undertakes an in-depth analysis of the evolution of hackers in contemporary media in: '*Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime* '(International Review of Law, Computers and Technology, Vol 22, Nos 1-2) (2008)

    Wall provides a briefer summary in his book, '*Cybercrime*' (P 14-17, Polity Press) (2007)

12. Neoseeker.com: Games lists over 50 software games with a 'Mob/Organised Crime' theme, including 'Gangsters: Organised Crime', the controversial 'Grand Theft Auto' series (which are believed to have inspired 'copycat' crimes), 'Mafia' I and II and 'Yakuza'.

    http://www.neoseeker.com/Games/themes/22/

13. Prime Minister's Foreword (Gordon Brown): Page iii, '*Extending Our Reach: A Comprehensive Approach to Tackling Serious Organised Crime'* (UK Government Report, Crown Copyright) (July 2009)

14. EU: '*A Secure Europe in a Better World – European Security Strategy*' (December 2003):

    http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf

15. World Federation of UN Associations, The Millennium Project *'2009 State of the Future*' Executive Summary, Page 2:

    http://www.millennium-project.org/millennium/issues.html

    (**Note:** Page 11 of the UK Cabinet Office Report: '*The National Security Strategy of the United Kingdom: Update* 2009', released in June 2009, refers to an older figure of 'one trillion pounds', taken from the '*2007 State of the Future*' Executive Summary.)

16. For instance, the UK Serious Organised Crime and Police Act 2005, the US Racketeer Influenced and Corrupt Organisations Act (RICO) 1970, the 2000 United Nations

Convention on Transnational Organised Crime and the Council of Europe 2000 Convention on Cybercrime. In the UK, the government has set up the Police Central E-Crime Unit (PCEU), the descendant of the National Hi-Tech Crime Unit (NHTCU), to work with the public and be the lead body for police online crime incident response management.

17. Serious Organised Crime Agency (SOCA) website, announcing the publication of the '*Serious Organised Crime Review*' (July 2009):

    http://www.soca.gov.uk/assessPublications/OrganisedCrimeReview.html

18. Some of the most recent high-profile reports are:

    UK Cabinet Office: '*Extending our Reach: A Comprehensive Approach to tackling Serious Organised Crime*' (July 2009)

    http://www.homeoffice.gov.uk/crime-victims/reducing-crime/organised-crime/

    UK Cabinet Office: '*Cyber Security Strategy 2009*' (June 2009)

    http://www.cabinetoffice.gov.uk/reports/cyber_security.aspx

    UK Cabinet Office: '*Security in an Interdependent World*' (June 2009) and '*Security for the Next Generation*' (June 2009)

    http://www.cabinetoffice.gov.uk/reports/national_security.aspx

    US Government: '*Cyberspace Policy Review*' (May 2009)

    http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

19. There have also been historic 'old school' technology training and awareness issues which have inhibited their progress in responding to all online crime, which are only now being addressed. Wall * identifies a prevailing 'cultural dissonance between traditional (*police*) occupational culture and the demands created by the internet, which allows the view to persist among many officers that "cyberspace is like a neighbourhood without a police department." '

    * D S Wall: Page 164, '*Cybercrime'* ('Crime and Society Series', Polity) (2007)

20. G P Gilligan, P 2, '*Business, Risk and Organised Crime*' (Journal of Financial Crime, Volume 14, No 2) (2007)

21. P Reuter: Page 175, '*Disorganised Crime – Illegal Markets and the Mafia*'

    (The MIT Press – Cambridge, Massachusetts; London, England) (Aka '*Disorganised Crime – The Economics of the Visible Hand'*) (1983, Second Printing 1984)

22. K von Lampe: '*Definitions of Organised Crime*' section, 'Organised Crime Research' website: http://www.organised-crime.de/OCDEF1.htm

23. Although there are some notable works from specialised perspectives across the different disciplines (some of which are mentioned in this paper and in the accompanying References), many resources have yet to be cross-referenced, creating a situation whereby it can be difficult to identify the common themes and to capitalise on them. Another reason for this, as von Lampe's 100 plus definitions of organised crime illustrate, is that it can be difficult to distinguish the wood from the trees where there has been vigorous debate about individual aspects of the problem.

    Von Lampe attempts to redress the balance in his paper, advocating a multi-disciplinary approach to organised crime:

K von Lampe: '*Beg, Steal or Borrow – The Study of Organised Crime and the Infusion of Concepts and Theories from Other Disciplines*' (Paper presented at the annual meeting of the American Society of Criminology (ASC) (November 2005)

http://freenet-homepage.de/kvlampe/ASC2005-kvl.pdf

A few of the sources and quotations in this section originate from von Lampe's work. He concludes that what is needed 'is a research program that would allow (*the*) building up of a cumulative body of knowledge'. (Page 10)

Von Lampe's website, together with that of the Canadian Nathanson Centre on Transnational Human Rights, Crime and Security, have extensive resource sections, for instance about the theory and origins of organised crime.

Von Lampe: http://www.organised-crime.de/OCDEF1.htm

Nathanson Centre:

http://www.osgoode.yorku.ca/NathansonBackUp/bibliography/contents.htm

24. For instance, if credit card details are compromised online as a single event, there may be little or no obvious evidence because the compromised data may have been copied, not removed, and the crime may have been commissioned by an organised crime network operating, via several intermediaries, in a distant country.

25. For instance Etges and Sutcliffe cite terrestrial examples from Columbia, Taiwan and Afghanistan where:

    '…. banned products are grown or manufactured simply because a local population does not have any viable alternatives to sustain itself. These products are refined and distributed by transnational crime groups.'

    R Etges and E Sutcliffe: Page 88, '*An Overview of Transnational Organised Cyber Crime*' (Information Security Journal: A Global Perspective, 17) (2008)

26. G S Becker: Pages 169-217, '*Crime and Punishment: An Economic Approach'* (The Journal of Political Economy, Vol 76, No 2, University of Chicago Press) (Mar –April 1968)

    An excerpted article from Becker's book appeared in the Autumn 1995 edition of '*Cross Sections'*, (Federal Reserve Bank of Richmond):

    http://www.richmondfed.org/publications/research/special_reports/economics_of_crime/pdf/economics_of_crime.pdf

    Noveck, reflecting the views of several authors * who evaluate the extent to which Becker's theory can be considered absolute, comments that the economic approach to law enforcement '…relies on the lesser claim that rational considerations are at least one of several factors that can affect the behaviour of some criminals.'

    S M Noveck: Page 6, '*Does Crime Pay? An Economic Analysis of Criminal Behaviour'* (ICPSR Bulletin, Special Edition 2007, Vol XXVII, No. 3, University of Michigan) (2007)

    * For instance, Ehrlich (Pages 551-67, '*Participation in Illegitimate Activities: A Theoretical and Empirical Investigation'*, 'Journal of Political Economy' (May-June 1973) and A Witte (Pages 57-84, '*Estimating the Economic Model of Crime with Individual Data'*, 'Quarterly Journal of Economics', February 1980)

27. For instance, see B McCarthy and J Hagan, Page 1039, '*When Crime Pays: Capital, Competence and Criminal Success*', 'Social Forces', Volume 79, Issue 3 (March 2001):

    '… personal capital is the psychological complement to human and social capital; it includes attitudes, tastes and preferences often evident in 'behavioural characteristics and resources'.

28. K von Lampe: Page 9, '*The Interdisciplinary Dimensions of the Study of Organised Crime*' ('Trends in Organised Crime', 9 (3)) (2006):

    http://www.organized-crime.de/kvlInterdiscDimStudyOC-TOC-9-3-2006.pdf

29. A R Dick: '*When Does Organised Crime Pay? A Transaction Cost Analysis*' ('International Review of Law and Economics 15: 25-45) (1995)

30. A R Dick: ABSTRACT. '*When Does Organised Crime Pay? A Transaction Cost Analysis*' ('International Review of Law and Economics 15: 25-45) (1995)

31. InvestorWords.com - http://www.investorwords.com/5047/transaction_costs.html

32. A R Dick: P 26, '*When Does Organised Crime Pay? A Transaction Cost Analysis*' ('International Review of Law and Economics 15: 25-45) (1995)

33. A Anderson: Pages 33-54, '*Organised crime, Mafia and governments'* (Within 'The Economics of Organised Crime', G Fiorentini and S Peltzman (Eds), Cambridge University Press) (1995)

34. P Gottschalk: Page 46, '*Criminal Entrepreneurship*' (Nova Science Publishers, Inc, New York) (2008)

    Gottschalk, among others *, also distinguishes between the significance of organisational governance and operational production as primary drivers for organised criminal activity. He observes that 'Transaction cost economics describes the organisation not in technological terms (as a production function) but in organisational terms (as a governance structure). Organisation and market are alternative modes of governance that differ in discrete structural ways.'

    * P Gottschalk: P 50, '*Criminal Entrepreneurship*' (Nova Science Publishers, Inc, New York) (2008)

    * Eg K von Lampe: Page 8 and Pages 12-13, '*The Interdisciplinary Dimensions of the Study of Organised Crime*' (Trends in Organised Crime, 9 (3)) (2006)

    http://www.organized-crime.de/kvlInterdiscDimStudyOC-TOC-9-3-2006.pdf

    Extending the concept yet further, Von Lampe notes that economic theories and concepts have also been applied to 'organised crime' at the activity level. As well as characterising crime as a 'market' (in particular, whether 'organised crime' illegal markets tend towards monopolisation, as well as their social costs and benefits), they perceive crime to be a 'business sector' (ie extending the market approach to incorporate other factors from the business environment) and analyse the impacts of the juxtaposition of legal/illegal sectors (for instance, the loss of revenue through non-payment of tax in some transition countries or the establishment of cartels). Eg Nardo:

    'The roles of the 'players' may 'appear in a market perspective just as a trade between the supply of specific illegal goods or services …The existence of the need, or of the opportunity, on the part of the buyer or of the supplier is more decisive an element than the organisational factor (in any of the two parts) for the transaction to occur.'

    M Nardo: Page 2, '*Organised Crime and Networking Economy: Models, Features, Dynamics and Related Approaches*' ('Journal of Money-Laundering Control, Volume 11, Issue 2) (2008)

35. Information-age.com: '*Interview: Len Hynds, National Hi-tech Crime Unit*' (February 2006)

    http://www.information-age.com/articles/289406/interview-len-hynds-national-hitech-crime-unit.thtml

36. CSOonline.com: Maintains an interactive map which displays which US states have enacted laws mandating disclosure of personal data breaches:

    http://www.csoonline.com/article/221322/CSO_Disclosure_Series_Data_Breach_Notification_Laws_State_By_State

37. Out-Law.com: '*The UK Does Not Need a Data Protection Law, Says Government'* (November 2008): http://www.out-law.com/page-9619

38. David Blunkett: Quoted in S Mullin's '*Interim Evaluation of the Business Crime Reduction Centre*' report (February 2008):

    http://www.bcrc-uk.org/filelib/BCRC_evaluation_feb08.pdf

39. The response of business towards online crime has already evolved rapidly since Blunkett's statement, for instance through the work of the BCRC Project itself, as outlined in its final report:

    S Mullins: '*Evaluation of the Business Crime Reduction Centre – Final Report*' (March 2009):

    http://www.bcrc-uk.org/filelib/BCRC%20Final%20Evaluation%20May%2009_1.pdf

    The report highlights the BCRC's approach of encouraging best practice information-sharing between its members and partners (which include the National Counter Terrorist Security Office and the Information Security Awareness Forum), as well as its range of business-focussed e-crime guides and other materials:

    The Sheffield Chamber of Commerce and Industry: Business Crime Reduction Centre webpage describes the specialist business support service which BCRC provides:

    http://www.scci.org.uk/page/show/49

    Organised crime was also debated at the influential World Economic Forum in Davos, Switzerland, in January 2009, which 'called for a new system to tackle well-organised gangs of cybercriminals'. A multi-disciplinary panel warned that the number of attacks were rising sharply, online theft was costing industry $1 trillion a year and that users (ie individuals) remained unaware of how to protect themselves:

    BBC.CO.UK: '*Cybercrime Threat Rising Sharply*' (January 2009):

    http://news.bbc.co.uk/1/hi/business/davos/7862549.stm

    Additionally, sectors which are at the frontline of combating online criminal activity, such as the banking, online gambling and anti-virus software industries, have long been familiar with the realities of terrestrial and online financial organised crime activities such as money-laundering, fraud and extortion (for instance, in the form of large-scale actual/threatened Denial of Service (DoS) attacks, as well as phishing and spamming scams), being among the first to become involved in initiatives such as the Anti-Phishing Working Group (APWG) and the UK 'Get Safe Online' campaign (jointly co-ordinated by the UK Government, the Serious Organised Crime Agency (SOCA) and the private sector).

40. 'The deal was made: around 30,000 Deutschmarks - $18,000 – for printouts and passwords.

    The KGB wasn't just paying for printouts, though. Hess and company apparently sold their techniques as well: how to break into Vax computers; which networks to use when crossing the Atlantic; details on how the Milnet operates.'

    Cliff Stoll: P 365-366, '*The Cuckoo's Egg – Tracking a Spy Through the Maze of Computer Espionage*' (Pocket Books, Simon and Schuster) (1989, 1990)

41. Phil Williams, CERT® Co-ordination Centre paper: '*Organised Crime and Cyber-Crime: Implications for Business*' (2002):

http://www.cert.org/archive/pdf/cybercrime-business.pdf

Interview between J Allen and Tom Longstaff:: '*Evolving Business Models, Threats and Technologies: A Conversation with CERT's Deputy Director for Technology*' (CERT® 'podcast' and transcript) (December 2006):

http://www.cert.org/podcast/show/20061212longstaff.html

42. Jakobsson and Z Ramzan: Page 356, – *Understanding New Attacks and Defences*' (Addison Wesley) (2008)
43. For instance:

    The 2008 '*Symantec Report on the Underground Economy* XII

    http://www.symantec.com/en/uk/about/news/release/article.jsp?prid=20081124_11

    '*Symantec Global Internet Security Threat Report – Trends for 2008*' (Volume XIV, Published April 2009)

    http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf

    Finjan Web Security Surveys, in particular H1/2008 – '*The Current State of Cybercrime and Web 2.0 Threats to Business*'

    http://www.finjan.com/Content.aspx?id=827

    Verizon Business '*2009 Data Breach Investigations Report*'

    http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

    McAfee '*2009 Threat Predictions*'

    http://www.mcafee.com/us/threat_center/white_paper.html

44. Page 2, Finjan '*Web Security Trends Report, Q2 2008*'
45. Page 7, '*Symantec Global Internet Security Threat Report – Trends for 2008*' (Volume XIV) (April 2009)
46. Eg Page 6, Finjan '*Web Security Trends Report, Q2 2008*'
47. For instance, Finjan's '*Web Security Trends Report – Q2/2008*'

    http://www.finjan.com/Content.aspx?id=827

    British Computer Society (BCS): '*Keeping it in da family*' (originally published in 'ISNow' journal, October 2008)

    http://www.bcs.org/server.php?show=ConWebDoc.22658

48. Keith Laslop of the company, 'Prolexic', quoted in Wired: '*Attack of the Bots*' (November 2006)

    http://www.wired.com/wired/archive/14.11/botnet.html?pg=4&topic=botnet&topic_set=

49. Bonger himself took the view that: '… the merchant and the thief are alike in taking account exclusively of their own interest to the detriment of those with whom they have to do.'

    W A Bonger: '*Criminality and Economic Conditions*' (BiblioLife) (2008 Edition). Originally published as a pamphlet in Dutch in 1905, then transcribed into French and

published by the Political Economy Club, Vancouver, BC, Canada in 1916, before its English publication in book form in the US by Boston, Little, Brown and Company (1916).

50. Eg: Gilligan asks: 'How much difference is there between illegal enterprise and organised crime?' and finds that 'legitimate and illegitimate business can share organisational features.'

    G P Gilligan, P 3, '*Business, Risk and Organised Crime*' (Journal of Financial Crime, Volume 14, No 2) (2007)

51. W Chambliss: '*On the Take: From petty crooks to presidents*', Page 53 (Bloomington: Indiana University Press, 1978)

    Tim Newburn, in his book,'*Criminology*' (P 407, Willan Publishing, 2007) quotes Chambliss, as well as Lyman and Potter: ('*Organised Crime'*, 3rd Edition. New York: Prentice Hall, 2004) who are of the opinion that there are three 'often-ignored' facets of organised crime:

    'There is relatively little difference between those perceived as law-abiding and those who are viewed as deviant.

    Corporate finance and corporate capital are characterised by criminality and misconduct at least as much as any poor neighbourhood.

    The distinctions between business, politics and organised crime are in many ways artificial and meaningless. "Rather than being dysfunctions, corporate crime, white-collar crime, organised crime and corruption are mainstays of US political-economic life." '

    Gilligan, (Page 3, '*Business, Risk and Organised Crime*') explores the debate further.

52. D R Cressey: Page 110, '*Theft of the Nation: The Structure and Operations of Organised Crime in America*' (New York: Harper and Row) (1969)

53. M Glenny: '*McMafia – Seriously Organised Crime*' (Vintage) (2009)

54. Anthony Schneider: '*Tony Soprano on Management*' (The Berkley Publishing Group, Penguin Group) (2004)

    http://www.tonysopranoonmanagement.com/thebook.html

    Other similar popular titles include '*The Mafia Manager: A Guide to the Corporate Macchiavelli*' by 'V' (Thomas Dunne, St Martin's Press) (1991, 1996) and '*Leadership Sopranos Style: How to Become a More Effective Boss*' by Deborah Himsell (Black Inc Publishing) (2003).

55. 'The Independent' gives a detailed account of the real business environment in which the Mafia operate, including the roles of Pippo Calo (the 'Mafia accountant') and Roberto Calvi ('God's Banker'). The article demonstrates the extent to which organised crime can infiltrate legitimate structures and the sombre and violent consequences that can occur when things go wrong:

    'Independent.co.uk': '*Calvi Murder: The Mystery of God's Banker*' (June 2007):

    http://www.independent.co.uk/news/world/europe/calvi-murder-the-mystery-of-gods-banker-452056.html

56. For instance, 'The Firm' was the name of a 1960s UK organised crime gang. Also, the main theme of John Grisham's novel, '*The Firm*' is the interrelation between legal and illegal business activity.

    Fiorentini and Peltzman's seminal work, '*The Economics of Organised Crime*' also highlights the significance of 'the firm' within a criminal context in its summarised papers from an economic conference which explored the theme 'Theories of the Firm':

http://www.cepr.org/PUBS/Bulletin/meets/3306.htm

57. R Dhamija, J D Tygar and M Hearst, in their 2006 study, '*Why Phishing Works*' (In 'Proceedings of the SIGCHI Conference on Human Factors in Computing Systems', New York, ACM Press, 2006) used 'trust indicators' such as logos and digital padlocks to assess the extent to which people could be fooled into accessing fake websites. They found that the majority of participants found it extremely difficult to distinguish between the real and fake sites.

    For an innovative suggestion to counter the problem, see: '*Anti-Phishing Phil: The design and evaluation of a game that teaches people not to fall for Phish'* (Carnegie Mellon University, No date provided)

    http://www.chariotsfire.com/pub/soups2007-anti-phishing-phil-final.pdf

    A research prototype version of the game is available at:

    http://cups.cs.cmu.edu/antiphishing_phil/

58. See 'The Online Disinhibition Effect' in the online book, '*The Psychology of Cyberspace*' (John Suler) for a thorough exploration of this subject:

    http://www-usr.rider.edu/~suler/psycyber/disinhibit.html

59. Cartoon Copyright, '*The New Yorker*', Page 61, July 5, 1993 edition (Vol 69, (LXIX), No 20)

    http://www.unc.edu/depts/jomc/academics/dri/idog.html

60. G P Gilligan, P 3, '*Business, Risk and Organised Crime*' (Journal of Financial Crime, Volume 14, No 2) (2007)

61. P Gottschalk: Pages 2-3, '*Criminal Entrepreneurship*' (Nova Science Publishers, Inc, New York) (2008)

3.1.2 Dispelling the Myths

1. J O Finckenauer: Page 1, Ch 1, 'Mafia and Organized Crime' ('Beginner's Guide' Series, Oneworld Publications) (2007)
2. Peter Reuter: Introduction, Page xi - '*Disorganised Crime – Illegal Markets and the Mafia*', (The MIT Press – Cambridge, Massachusetts; London, England) (Aka '*Disorganised Crime – The Economics of the Visible Hand'*) (1983, Second Printing 1984)
3. D S Wall: Page 48, '*Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime'* (International Review of Law, Computers and Technology, Vol 22, Nos 1-2) *(2008)*
4. Abstract from the House of Lords Science and Technology Select Committee 5th Report of Session 2006-7, '*Personal Internet Security*':

    http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf

5. D S Wall: Page 26, '*Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime'* (International Review of Law, Computers and Technology, Vol 22, Nos 1-2) *(2008)*
6. D S Wall: Page 13, '*Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime'* (International Review of Law, Computers and Technology, Vol 22, Nos 1-2) *(2008)*

7. D S Wall: Pages 13-29, '*Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime'* (International Review of Law, Computers and Technology, Vol 22, Nos 1-2) (2008)

8. D S Wall: Page 17, '*Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime'* (International Review of Law, Computers and Technology, Vol 22, Nos 1-2) (2008)

   Similarly, Newman and Clarke, writing about e-commerce crime, also warn against unreliable sources and potential bias from 'both public and private' vested interests.

   They observe that: 'In the realm of cybercrime, however, there (*are*) but a handful of studies conducted that collect anything like first-hand information. The majority of articles on computer crimes are descriptive attempts …'

   At the same time, they acknowledge the valid contribution made by reputable private sector organisations:

   G R Newman and R V Clarke: Pages 23-24, '*Superhighway Robbery – Preventing e-Commerce Crime' (*Willan Publishing) (2003)

   Newman and Clarke's text is an in-depth evaluation of e-commerce crime from a situational crime prevention perspective. It includes a comparison of traditional commerce and e-commerce factors, as well as a table (Table 3.1, Page 54) which estimates the cost and impacts of 'crimes of the computing age' on the e-commerce environment.

9. Within formal forensic techniques, nothing is discarded without a specific reason and physical and electronic forensic techniques meticulously record every small clue from a situation. This information is particularly valuable in circumstances where overt information is difficult to acquire, for instance when combating organised criminal activity which is largely covert.

   For a simple explanation of the 'mosaic effect', see Computerworld Security – Jaikumar Vijayan**,** '*Sidebar: The Mosaic Effect*' (March 2004):

   http://www.computerworld.com/s/article/91109/Sidebar_The_Mosaic_Effect

10. D S Wall: Page 144, '*Cybercrime'* ('Crime and Society Series', Polity) (2007)

11. Page 23, *2008 CSI Computer Crime and Security Survey*.

    The impact of reputational damage is difficult to quantify. Although the respondents in the CSI survey placed it in third place, it can have far-reaching effects. For instance, in the perception of the public, the name of the UK Government Department HMRC has become synonymous with its high-profile data loss of 25 million personal records such that the incident is simply referred to as 'the HMRC incident'.

12. J O Finckenauer and E Waring: Page 4, '*Challenging the Russian Mafia Mystique*' (National Institute of Justice Journal) (April 2001)

    http://www.ncjrs.gov/pdffiles1/jr000247b.pdf

13. Trend Micro: Page 4, '*Trend Micro 2008 Annual Threat Roundup and 2009 Forecast*'

    http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/trend_micro_2009_annual_threat_roundup.pdf

14. Trend Micro: Pages 14-15, '*Trend Micro 2007 Threat Report/ 2008 Threat and Technology Forecast*':

    http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/trend_micro_2009_annual_threat_roundup.pdf

15. In her online essay for the Social Science Research Council, '*Is Cyber Terror Next*?' (November 2001), written shortly after the September 11, 2001 terrorism incidents, D E Denning mentions that the Code Red worm alone infected 'about a million servers in July and August' 2001, causing '$2.6 billion in damages' from 'a single incident':

    http://essays.ssrc.org/sept11/essays/denning.htm

16. D S Wall: Pages 13-29, '*Cybercrime'* ('Crime and Society Series', Polity) (2007)

17. M E Beare: Pages 1-2, '*Structures, Strategies and Tactics of Transnational Criminal Organisations: Critical Issues for Enforcement*' (Paper presented at the Australian Institute of Criminology, Australian Customs Service and Australian Federal Police Transnational Crime Conference, March 9-10, 2000; Nathanson Centre on Transnational Human Rights, Crime and Security)

    http://www.ncjrs.gov/nathanson/aust.html

    A recent study (July 2009), also by *Carnegie Mellon University*, found that users who encountered repeated pop-up warnings about SSL (an encryption protocol) in benign situations became desensitised to them and that additional techniques needed to be employed to ensure the message was assimilated.

    Carnegie Mellon CyLab: '*CyLab Usable Privacy and Security Researchers Release Study on SSL Warning Effectiveness*' (no date provided):

    http://www.cylab.cmu.edu/news_events/cylab_news/cups-study.html

    The significance of this study is already being extended to include discussion about the implications for warnings about national security threats, a category which is sometimes deemed to include both terrorism and 'organised crime':

    ABCNews.go.com: '*Crying Wolf: Do Security Warnings Help?*' (July 2009):

    http://abcnews.go.com/print?id=8205775

    A specific example of the damage to trust which can occur when online crime data is perceived to be exaggerated or unverified occurred in April 2009, when the FBI's Assistant Director of the Cyber Division described predictions about the possible impact of the 'Conficker' botnet (suspected to have been created by an Eastern European online crime group *) as 'hype', saying that such statements could create a false sense of complacency and that the problem was being blown out of proportion.

    News.cnet.com: '*Researchers say Conficker is all about the money*' (April 2009)

    http://news.cnet.com/researchers-say-conficker-is-all-about-the-money/

    "… I think that focusing people on that particular aspect perhaps took their attention away from the overall threat, which is just as great or greater than Conficker itself."

    ComputerWorld - Security: '*Conficker hype may have harmed security efforts, FBI cyber chief says*' (April 2009)

    http://www.computerworld.com/s/article/9132089/Conficker_hype_may_have_harmed_security_efforts_FBI_cyber_chief_says

    In this particular instance, as with the warnings about the Millennium Bug, the IS industry found itself in a 'damned if you do and damned if you don't' situation. Although the concerns raised by the security analysts were legitimate (for instance, because 'Conficker' was compromising millions of machines and was based on extremely sophisticated self-evolving code. Also, that it was found to spread aggressively and had proven links with the online organised crime group behind the prolific 'Waledac' worm), the story was blown out of proportion by the press so the fact that there was no major impact on April 1st 2009 meant that the analysts' warnings were interpreted as being unfounded.

Gcn.com, (US) Government Computer News: '*Mergers and acquisitions in the botnet world*' (May 2009)

http://gcn.com/Articles/2009/05/11/Cybereye-cooperating-botnets.aspx?Page=1

18. KPMG: Page 30, '*2009 e-crime survey*':

    http://www.e-crimecongress.org/ecrime2009/documents/e-CrimeSurvey2009_AKJ_KPMG(1).pdf

19. For example:

    Baselinemag.com: '*Geekfathers: CyberCrime Mobs Revealed*' (March 2005)

    http://www.baselinemag.com/c/a/Projects-Security/Geekfathers-CyberCrime-Mobs-Revealed/

    NewsFactor.com: '*The Real-Life Internet Sopranos*' (December 2005)

    http://www.newsfactor.com/story.xhtml?story_id=011000009BW2&full_skip=1

    eWeek.com: '*Return of the Web Mob'* (April 2006)

    http://www.eweek.com/c/a/Security/Return-of-the-Web-Mob-%5B1%5D/

    DarkReading.com: '*Cybercrime, Cosa Nostra-Style'* (July 2008)

    http://www.darkreading.com/security/government/showArticle.jhtml?articleID=211201153

    British Computer Society (BCS): '*Keeping it in da family*' (originally published in 'ISNow' journal, October 2008)

    http://www.bcs.org/server.php?show=ConWebDoc.22658

    Guardian.co.uk: '*Al-Capone' style plan to curb UK's booming £30bn crime industry*' (July 2009)

    http://www.guardian.co.uk/uk/2009/jul/13/organised-crime-fraud

20. BaselineMag.*com*: '*Shadowcrew: Web Mobs'*(March 2007)

    http://www.baselinemag.com/c/a/Security/Shadowcrew-Web-Mobs/1/

---

21. US President's Commission - Quoted in: G P Gilligan, P 2, '*Business, Risk and Organised Crime*' (Journal of Financial Crime, Volume 14, No 2) (2007)
22. E Kaspersky, KasperskyUSA.com: '*The Cybercrime Ecosystem*' White Paper (September 2008)

    http://www.kasperskyusa.com/partners/pdf/The_Cybercrime_Ecosystem.pdf

23. D S Wall: Page 40, '*Cybercrime*' ('Crime and Society Series', Polity) (2007)
24. '*United Nations Convention On Transnational Organised Crime'* (2000)

    http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf

25. Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders Press Release: '*Fighting Transnational Organised Crime*' (March 2000)

    http://www.un.org/events/10thcongress/2088f.htm

26. Organised criminal group - Article 2(a) '... a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more

serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit".

'Structured group' – Article 2(c) '… a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure'

27. United Nations Office on Drugs and Crime: Page 5, '*Results of a Pilot Survey of Forty Selected Organised Criminal Groups in Sixteen Countries*' (September 2002)

28. The terms 'cyberspace' and 'cybergang' retain resonances with science fiction and the image of the early hacking culture. Hence, the more neutral term 'online organised crime group' is used throughout.

    (See D S Wall, 'Page 10, '*Cybercrime*' and the Australian Government's '*Future Directions in Technology-Enabled Crime: 2007-09'*, for the potential implications of using different crime and technology-oriented terms in different circumstances.)

    'Future Directions in Technology-Enabled Crime: 2007-09':

    K R Choo, R G Smith, R McCusker: Pages 2 and 7, '*Research and Policy Series no.78 - Future Directions in Technology-Enabled Crime 2007-09*' (Australian Government, Australian Institute of Criminology) (September 2007)
    http://www.aic.gov.au/publications/current%20series/rpp/61-80/rpp78.aspx

29. *'Future Directions in Technology-Enabled Crime: 2007-09*', Ibid, Page 64.

30. BBC.co.uk: '*Fraudsters' Website Shut in Swoop'* (April 2008)

    http://news.bbc.co.uk/1/hi/uk/7675191.stm

31. For instance, the recent UK Cabinet Office '*Extending Our Reach: A Comprehensive Approach to tackling Serious Organised Crime*' report approaches 'organised crime' in very general terms. In many cases, where some attempt is made to define the nature of the problem, descriptions may be imprecise, implied or dependent on anecdotal as opposed to factual evidence.

    It is quite common for reports to jump between references to 'organised crime', technology-oriented organised crime and technology-oriented crime in general, thus giving the impression that they are still speaking about the previous subject or that the 2 subjects are synonymous, when in fact they are actually referring to something new which is quite different. This creates the potential risk that the audiences for these reports could become desensitised, as identified within *Carnegie Mellon University* study which was discussed previously.

    Although it would not be desirable or viable for the literature to detail every possible interpretation of 'organised crime', there is a great need for reports intended for large-scale audiences, including the IS/ business sectors, to define their scope and terms clearly and precisely as a matter of course, including the reasons behind the decisions why the terms have been chosen. Depending on the situation, it may simply be necessary to cite the sources for the decisions. This action might help to give some of the reports additional authority.

    Published security incident reports themselves, are part of an evolutionary process. For instance, in 2006, the focus of the Garlik '*UK Cybercrime Report*' was typical of the genre until fairly recently, in that it focussed entirely on the types of threats without any

consideration at all about who might be committing them. Nowadays, equivalent reports will usually provide some broad analyses of the types of perpetrators, together with some information about the impact on businesses. However, as this paper discusses, the vast proportion of industry white papers, for instance, have until recently still tended to focus on detailed technical analysis of the threats, with little equivalent detailed analysis of the other elements which (for instance) comprise the International Standard, 27001.

In fairness, it must be said that this lack of precision is not universal. For instance, the sources within the following tables were chosen because they either apply a certain level of intellectual rigour to their methods or have been influential or typical of their genre. An example of the new breed of security incident report is the 2008 '*Symantec Report on the Underground Economy* XII', which provides a detailed analysis of several aspects of the 'underground economy':

http://www.symantec.com/en/uk/about/news/release/article.jsp?prid=20081124_11

32. There may be several reasons why this might be the case. The situation may reflect assumptions that there is no great need to differentiate between different types of organised crime. Alternatively, the difficulty of creating the definitions could be a deterrent so that the subject is avoided altogether. In some cases, there may be insufficient understanding of the issues to identify that definitions may be necessary.

References

4. TECHNOLOGY AND ORGANISED CRIME

1. Information-age.com: Online version of '*Interview: Len Hynds, National Hi-Tech Crime Unit*' (February 2006):

   http://www.information-age.com/articles/289406/interview-len-hynds-national-hitech-crime-unit.thtml

2. Once again, as was the case with the academic discussions about the term 'organised crime', there are many external sources which provide in-depth technical analyses of the various threats and vulnerabilities, hence they are only addressed at a high level here.

   Recent analysis of the online threat landscape from different perspectives is provided in:

   Jakobsson and Z Ramzan: '*Crimeware – Understanding New Attacks and Defences*' (Addison Wesley) (2008)

   For further specific analysis of malware threats and vulnerabilities from a vendor-neutral, international perspective, the reader is referred to the Organisation for Economic Development and Co-Operation (OECD) 'Malicious Software (Malware): A Security Threat to the Internet Economy' 2007/8 report which provides an in-depth assessment of the malware problem, including clear descriptions and diagrams of key threats, together with statistics from a range of Information Security sources:

   http://www.oecd.org/dataoecd/53/34/40724457.pdf

3. R Etges and E Sutcliffe: Page 91, '*An Overview of Transnational Organised Cyber Crime*' (Information Security Journal: A Global Perspective, 17) (2008)

4. Several of the categories in this list are derived from:

   K R Choo, R G Smith, R McCusker: Pages 6-8, 'Research and Policy Series no.78 - Future Direct*ions in Technology-Enabled Crime 2007-09*' (Australian Government, Australian Institute of Criminology) (September 2007)

   http://www.aic.gov.au/publications/current%20series/rpp/61-80/rpp78.aspx

5. For instance, Page 23 of the '*2009 e-crime survey*' by KPMG stated that compromised websites are the 'predominant delivery mechanism' for data harvesting:

   http://www.e-crimecongress.org/ecrime2009/documents/e-CrimeSurvey2009_AKJ_KPMG(1).pdf

   Similarly, Cisco's '*2009 Midyear Security Report*' reported that exploited legitimate websites were responsible for nearly 90 percent of all web-based threats, allowing offenders to target specific groups such as sports fans or students.

6. RSA SecureID - Provides secure two-factor authentication – whereby claimed identities are checked against 2 or more criteria)

   SSL Certificates - (have the ability to provide secure two-way authentication and encryption channels to protect information as it crosses the Internet)

7. In 2004, a group of Russian hackers who had targeted online legitimate gambling sites were arrested by the UK National Hi-Tech Crime Unit and its Russian equivalent, having cost UK bookmakers an estimated £40 million in damages. The group strategically targeted the most popular events in their demands, identifying these as the peaks of business ('Outlaw.com' article) and thus the most likely to have a high impact on both the businesses and their customers. Due in part to the current recession, threats from randomware are expected to increase in the future, with small to medium-sized businesses with minimal IT resources identified as being most vulnerable (Trend Micro report)

   Out-Law.com: '*Russian hackers arrested over bookie blackmail*' (July 2004)

   http://www.out-law.com/page-4752

   Trend Micro Report: Page 3, '*Trend Micro 2008 Annual Threat Roundup and 2009 Forecast*'

   http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/trend_micro_2009_annual_threat_roundup.pdf

8. Terrence Berg, Computer Law: Pages 20 and 21, '*The Changing Face of Cybercrime – New Internet Threats Create Challenges to Law Enforcement*' (Date not published, 2007?)

   http://www.michbar.org/journal/pdf/pdf4article1163.pdf

   'a large proportion' - Although Berg states that 80 per cent of spam is linked with organised crime (Page 3), the source he quotes (cnn.com – '*9 out of 10 e-mails now spam*', November 2006) estimates it as '9 out of 10 e-mails'.

9. Sophos: Page 1, '*Security Threat Report: 2009*'

   http://www.sophos.com/sophos/docs/eng/marketing_material/sophos-security-threat-report-jan-2009-na.pdf

10. Wired: '*Attack of the Bots*' (November 2006)

    http://www.wired.com/wired/archive/14.11/botnet.html?pg=4&topic=botnet&topic_set=

    Quoted in Terrence Berg's paper above.

11. Mxlogic.com, Spam News: '*Bing hosting spam ads for counterfeit drugs*' (August 2009)

    http://www.mxlogic.com/securitynews/spam/bing-hosting-spam-ads-for-counterfeit-drugs405.cfm

12. As well as e-Gold, the e-currency trade also includes other precious 'e-metals' such as e-silver, e-platinum and e-palladium:

    E-gold.com: http://www.e-gold.com/unsecure/qanda.html

    The rise, demise and gradual resurgence of 'e-gold' provided a dramatic demonstration of the vulnerabilities associated with online anonymity, including the potential consequences of using a weak business model.

    The Washington Post – '*US: Online Payment Network Abetted Fraud, Child Pornography*' (May 2007)

http://www.washingtonpost.com/wp-dyn/content/article/2007/05/01/AR2007050101291.html?hpid=moreheadlines

Due to its criminal associations, 'e-gold' was dubbed the 'currency of choice for cybercrooks' by *Businessweek*. For instance, it was a popular currency among *ShadowCrew* members.

BusinessWeek – '*Gold Rush – Online payment systems like e-gold Ltd. are becoming the currency of choice for cybercrooks*' (January 2006)

http://www.businessweek.com/magazine/content/06_02/b3966094.htm

Wired.com – '*Bullion and Bandits: The Improbable Rise and Fall of E-Gold*' (June 2009)

http://www.wired.com/threatlevel/2009/06/e-gold/

13. Kaspersky Lab: '*Online Games and Fraud: Using Games as Bait*' (September 2007)

    http://www.viruslist.com/en/analysis?pubid=204791963

14. US-CERT.gov/reading room: '*Playing It Safe: Avoiding Online Gaming Risks'* (2006, updated 2008)

    http://www.us-cert.gov/reading_room/gaming.pdf

15. McAfee: '*Financial Fraud and Internet Banking: Threats and Countermeasures*' (2009)

    http://www.mcafee.com/us/local_content/reports/6168rpt_fraud_0409.pdf

    The paper includes a useful précis of the main types of threats which currently affect online financial information.

16. ITPro.co.uk: '*Online Banking Fraud Rises by 132 per cent*' (March 2009)

    http://www.itpro.co.uk/610267/online-banking-fraud-rises-by-132-per-cent

17. 'K R Choo, R G Smith, R McCusker: Page 8, '*Research and Policy Series no.78 - Future Directions in Technology-Enabled Crime 2007-09*' (Australian Government, Australian Institute of Criminology) (September 2007)

    http://www.aic.gov.au/publications/current%20series/rpp/61-80/rpp78.aspx

18. G P Gilligan, P 3, '*Business, Risk and Organised Crime*', *Journal of Financial Crime, Volume 14, No 2* (2007)

19. G P Gilligan, P 5, '*Business, Risk and Organised Crime*', *Journal of Financial Crime, Volume 14, No 2* (2007)

20. For instance, a 2008 survey for the US company *CA* found that, although 90% of adults now worry about the security of their personal data, the social networking profiles of 35% of teenagers are viewable by strangers, with 38% posting their education information, 32% disclosing their e-mail addresses and 28% revealing their birth date:

    CA.com, 'Keep America Safe Online' webpage: Pages 1-3, '*Cyber Security Survey*' (September 2008)

    http://home3.ca.com/upload/en_us/kaso/CA_Cyber_Security_Survey-NewsWorthy_Analysis.pdf

21. In 2001, at the start of a worldwide anti-crime operation, British police apprehended members of the Wonderland Club, recovering nearly three-quarters of a million pictures of sexually-abused children. The BBC World Service reported that: 'To join the club, each potential member had to have at least ten thousand pictures of pre-teen children and agree to exchange them with other members.'

    BBC.co.uk: '*International Paedophile Ring Broken Up'* (January 2001)

    http://news.bbc.co.uk/1/hi/world/europe/1110820.stm

    Such groups usually use P2P private networks (eg 'BitTorrent' *), the same types of networks used by music and media file-sharing services, where downloaded files are encrypted and password-protected and can be distributed via a single access point. Use of the Internet enabled these offenders to make contact, communicate and exchange vast amounts of information with ease. It would have been extremely difficult for them to have hidden the scale of their activities had they taken place completely in the physical plane.

    * Terrence Berg, Computer Law: Page 19, '*The Changing Face of Cybercrime – New Internet Threats Create Challenges to Law Enforcement*' (Date not published, 2007?)

    http://www.michbar.org/journal/pdf/pdf4article1163.pdf

22. Techpluto.com: '*Core Characteristics of Web 2.0 Services*' (November 2008)

    http://www.techpluto.com/web-20-services/

23. The CERT® Insider Threat Research section includes several resources about insider threats, including the report mentioned in this paper, '*Spotlight on: Malicious Insiders with Ties to the Internet Underground* Community' (March 2009), as well as the transcript of a conversation between '*Mitigating Insider Threat: New and Improved Practices*' (August 2009):

    http://www.cert.org/insider_threat/

    The report and the transcript both include a series of potential countermeasure suggestions to mitigate against this type of threat.

24. CERT®: Page 11, '*Spotlight on: Malicious Insiders with Ties to the Internet Underground Community'* (March 2009)

    http://www.cert.org/insider_threat/

25. Cyber-Ark: '*2009 Trust, Security and Passwords Survey Research Brief*' (June 2009)

    http://www.cyber-ark.com/landing-pages/downloads/snooping-survey-2009.asp

26. J O Finckenauer and E Waring: Page 3, '*Challenging the Russian Mafia Mystique'* (National Institute of Justice Journal) (April 2001)

    http://www.ncjrs.gov/pdffiles1/jr000247b.pdf

27. For instance, see V3.co.uk, online interview with Eugene Kaspersky: '*Credit Crunch forcing software engineers into crime*' (December 2008)

    http://www.v3.co.uk/vnunet/news/2232084/credit-crunch-force-software

In order to mitigate somewhat against these types of threat, it is imperative that organisations remain vigilant and conduct adequate security vetting exercises before new employees or third parties are allowed to access any sensitive information. The CERT® report mentioned in the paper at this point provides additional countermeasure suggestions to mitigate against this type of threat.

28. Trend Micro: Page 3, '*Trend Micro 2008 Annual Threat Roundup and 2009 Forecast*'

    http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/trend_micro_2009_annual_threat_roundup.pdf

    Trend Micro quoted the Organisation for Economic Co-Operation and Development '*Malicious Software (Malware): A Security Threat to the Internet Economy'* Report (2007/8)

    http://www.oecd.org/dataoecd/53/34/40724457.pdf

29. Trend Micro: Page 4, '*Trend Micro 2008 Annual Threat Roundup and 2009 Forecast*'

    http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/trend_micro_2009_annual_threat_roundup.pdf

30. The Organisation for Economic Co-Operation and Development (OECD): Page 66, '*Malicious Software (Malware): A Security Threat to the Internet Economy'* Report (2007/8)

    http://www.oecd.org/dataoecd/53/34/40724457.pdf

31. Symantec White Paper: Pages 5 and 6, '*Web-based Attacks – February 2009*'

    http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_web_based_attacks_03-2009.en-us.pdf

32. Symantec White Paper: Page 16, '*Web-based Attacks – February 2009*'

    http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_web_based_attacks_03-2009.en-us.pdf

33. Jakobsson and Z Ramzan: Page 1, '*Crimeware – Understanding New Attacks and Defences*' (Addison Wesley) (2008)

34. Joint Report between the US Department of Homeland Security, SRI International Identity Theft Technology Council and the Anti-Phishing Working Group, sponsored by the US Dept of Homeland Security Science and Technology Directorate: Page 5, '*The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond*' (October 2006)

    http://www.antiphishing.org/reports/APWG_CrimewareReportpdf

35. Jakobsson and Z Ramzan: Page 4, '*Crimeware – Understanding New Attacks and Defences*' (Addison Wesley) (2008)

36. Symantec White Paper: Page 4, '*Web-based Attacks – February 2009*'

    http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_web_based_attacks_03-2009.en-us.pdf

37. Verizon: Page 2, '*2009 Data Breach Investigation Report*'

    http://www.verizonbusiness.com/products/security/risk/databreach/

38. Trend Micro: Page 15, '*Trend Micro 2008 Annual Threat Roundup and 2009 Forecast*'

    http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/trend_micro_2009_annual_threat_roundup.pdf

39. Jakobsson and Z Ramzan: Pages 3 and19, '*Crimeware – Understanding New Attacks and Defences*' (Addison Wesley) (2008)

40. These kits come in many different flavours and include many advanced techniques. For instance, they can target victims with timed attacks that reduce the chances of detection:

    Symantec White Paper: Page 11, '*Web-based Attacks – February 2009*'

    http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_web_based_attacks_03-2009.en-us.pdf

    The distribution method of the kits has been dubbed 'crimeware-as-a-service' (CaaS), in recognition that they closely mimic the 'Software-as-a-Service' (SaaS) model whereby software is hosted remotely on the Web and provided to subscribers 'on demand' for a fee:

    Blogs.ZDNet.com: *'The Next Big Thing? Crimeware-as-a-Service'* (April 2008)

    http://blogs.zdnet.com/security/?p=1012

    Having bought their kit, in many cases, offenders no longer need to employ much effort to launch high-impact attacks. Instead, they can place their tools strategically where they are likely to be found and accessed and leave the tool to do the rest.

41. Jakobsson and Z Ramzan: Page 2, '*Crimeware – Understanding New Attacks and Defences*' (Addison Wesley) (2008)

42. Tim Berners-Lee, World Wide Web Consortium (W3C):

    "Q: What is the difference between the Net and the Web?

    A: The Internet ('Net) is a network of networks. Basically it is made from computers and cables …. Lots of different sort of programs use the Internet: electronic mail, for example, was around long before the global hypertext system I invented and called the World Wide Web ('Web). Now, videoconferencing and streamed audio channels are among other things which, like the Web, encode information in different ways and use different languages between computers ("protocols") to provide a service.

    …. The Web is an abstract (imaginary) space of information. On the Net, you find computers -- on the Web, you find document, sounds, videos.... information. On the Net, the connections are cables between computers; on the Web, connections are hypertext links. The Web exists because of programs which communicate between computers on the Net. The Web could not be without the Net."

    http://www.w3.org/People/Berners-Lee/FAQ.html

43. BBC.co.uk: ' "*Boom year" for hi-tech criminals*' (December 2008)

http://news.bbc.co.uk/1/hi/technology/7797280.stm

Some of the main web threat trends observed by Symantec in 2008 were:

- 'Drive-By Downloads' from mainstream Web sites

- Heavily obfuscated (concealed) and dynamically-changing attacks (Symantec estimated that, whereas only a few attacks were obfuscated in 2006, by 2006 most attacks were concealed in this manner.)

- Attacks targeting browser 'plug-ins' instead of only the browser itself

(ie attacks targeting the sources of the components which make up the browser, as well as the browser itself)

- Misleading applications infecting users.

44. Sophos: Page 1, '*Security Threat Report: 2009*'

    http://www.sophos.com/sophos/docs/eng/marketing_material/sophos-security-threat-report-jan-2009-na.pdf

45. Sophos: Page 3, '*Security Threat Report: 2009*'

    http://www.sophos.com/sophos/docs/eng/marketing_material/sophos-security-threat-report-jan-2009-na.pdf

46. UK Department for Business Enterprise and Regulatory Reform (BERR): Page 2, '*2008 Information Security Breaches Survey – Technical Report*':

    http://www.pwc.co.uk/eng/publications/berr_information_security_breaches_survey_2008.html

47. Sophos: Page 1, '*Security Threat Report: 2009*'

    http://www.sophos.com/sophos/docs/eng/marketing_material/sophos-security-threat-report-jan-2009-na.pdf

48. Europol, High Tech Crime Centre: Page 11, '*High Tech Crimes Within the EU: Old Crimes New Tools, New Crimes New Tools*' – *Threat Assessment 2007,* Public Version (August 2007)

    http://www.enisa.europa.eu/doc/pdf/Workshop/cert_mit_cyb_att/threat_assess_high_tech_crimes_2007_open_ver.pdf

    For offenders in general, using the Internet as a tool follows in the tradition of exploiting other high-impact technologies, such as telephones, motor vehicles and, more recently, electronic encryption devices:

    M D Goodman and S W Brenner, Page 1 in online version of '*The Emerging Consensus on Criminal Conduct in Cyberspace*', UCLA Journal of Law and Technology (2002)

    http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.php

Encryption devices can both fortify the protection of illicit information and be used as an extortion tool in 'ransomware', a re-emerging threat originally inspired by the 'AIDS Info Disc/ PC Cyborg Trojan' from 1989:

'AIDS Info Disc/ PC Cyborg Trojan' – The 'AIDS Info Disc' was a virus transmitted via floppy disc which, when installed, encrypted the hard drive of the computer after 90 reboots. The 'company' behind the virus then attempted to extort a fee in exchange for the decryption key. (D Denning: Page 262, '*Information Warfare and Security*', Addison Wesley, 1999).

However, due to its impact on globalisation and the complexity of its design, the potential for damage through using the Internet is much greater than for terrestrial technologies such as motor vehicles:

M D Goodman and S W Brenner, Pages 1 and 2, in online version of '*The Emerging Consensus on Criminal Conduct in Cyberspace*', UCLA Journal of Law and Technology (2002)

http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.php

For instance, modern organised crime groups can combine the benefits of the Internet with the diversity of sophisticated resources at their disposal, such as educated individuals located across the world and cutting-edge technical knowledge.

49. Several authors have drawn comparisons between terrestrial and online versions of crimes.

    For instance, D S Wall, in '*The Internet as a Conduit for Criminal Activity*' (Pages 77-98, Information Technology and the Criminal Justice System, A Pattavina (Ed), Sage Publications, Inc) (2005, 2007) includes a 'matrix of cybercrimes' (Table 4.1) which place terrestrial and digital crimes alongside each other, within categories which identify whether crime type situations create additional opportunities for traditional crimes, new opportunities for traditional crime or new opportunities for new types of crime.

    Albanese also creates a table (Table 4) in which he views most online crime as a variation of traditional crime. For instance, internet gambling is viewed as an adaptation of terrestrial gambling.

    (J S Albanese: '*Risk Assessment in Organised Crime: Developing a Market and Product-Based Model to Determine Threat Levels*' (Pages 273 – 272, Journal of Contemporary Criminal Justice, Volume 24, Number 3) (August 2008)

    http://jayalbanese.com/organized_crime)

50. For instance, it may be difficult to locate where it is backed up or by which route it is travelling. This is because web-based services rely heavily on the infrastructure of the Internet, whereby packets of data can travel across numerous different routes, depending on the data type and the configuration of the protocols:

    Securecomputing.net.au: '*Experts urge caution on cloud computing*' (October 2008)

    http://www.securecomputing.net.au/News/125405,experts-urge-caution-on-cloud-computing.aspx

51. (*Julie Allen: So give me a few examples.*)

Tom Longstaff:

'So, for example, as we move from e-mail to web-based services, from web-based services to things like Ajax where you're going to data models that are being pushed more and more outside of your corporation. These are technologies that are changing the entire nature of who has what information at what given time and who controls it…'

Interview between J Allen and Tom Longstaff:: '*Evolving Business Models, Threats and Technologies: A Conversation with CERT's Deputy Director for Technology*' (CERT® 'podcast' and transcript) (December 2006)

http://www.cert.org/podcast/show/20061212longstaff.html

52. The farther removed in terms of physical or virtual location a service is from the core business, the more likely that an organisation will settle for contractual assurances, for instance in the form of information-sharing agreements, which will often be insufficient in themselves to ensure the adequate protection of the assets for corporate governance and legal purposes. In such circumstances, organised crime groups may be able to infiltrate the third party organisation, either physically (for instance by offering bribes or through extortion) or through the digital network, without challenge.

53. For instance, the prolific 'Storm' worm was first propagated via malicious code embedded in e-mails which contained weather disaster content. Hoax security e-mails can encourage users to buy 'scareware', fake security software, usually promoted via security alert hoaxes, which often has aggressive installation techniques and which is designed to be very difficult to uninstall.

54. The BBC.co.uk article '*"Scareware" scams trick searchers*' (March 2009) summarises some of the main issues surrounding 'scareware':

    http://news.bbc.co.uk/1/hi/technology/7955358.stm

55. BBC.co.uk: *'US Shuts down 'scareware' sellers*' (December 2008)

    http://news.bbc.co.uk/1/hi/technology/7779223.stm

    The BBC article refers to a report from The Anti-Phishing Working Group:

    Page 9, '*Phishing Activity Trends Report – 2nd Half 2008*'

    http://www.antiphishing.org/reports/apwg_report_H2_2008.pdf

    A recent innovation combines 'scareware' and 'ransomware' through the introduction of a fake anti-virus package that 'holds files to ransom' called FileFix Professional. This is accessible from the fake utility, Antivirus 2009 at a cost of $50.

    The Register: '*Scareware Package Incorporates File Ransom Trickery*' (March 2009)

    http://www.theregister.co.uk/2009/03/25/scareware_ransomware/

    In December 2008, the US Federal Trade Commission issued injunctions against 2 major 'scareware' vendors, who were trading on the borders of legality and advertising on legitimate, unknowing websites, to prevent them from making false claims and advertising their wares.

BBC.co.uk: *'US shuts down 'scareware' sellers*' (December 2008)

http://news.bbc.co.uk/1/hi/technology/7779223.stm

References

5 THE BUSINESS OF ORGANISED CRIME

1. Wired.com: '*Notorious Crime Forum DarkMarket Goes Dark*' (September 2008)

   http://www.wired.com/threatlevel/2008/09/notorious-crime/

2. See, for instance, K von Lampe's paper, in which he identifies 3 prevailing schools of thought with regard to organised crime group models, all of which have in common 'a strong orientation to concrete events and settings' (Page 3), based on the work of J Albanese (1994), B Halstead (1998) and P Williams and R Godson (2002).

   K von Lampe: '*The Use of Models in the Study of Organised Crime'* (Paper presented at the 2003 conference of the European Consortium for Political Research (ECPR), Marburg, Germany (19 September 2003)

   http://www.organized-crime.de/modelsofoc.htm

   S Brenner's paper specifically compares the structures of terrestrial and online organised crime groups, differentiating between:

   - 'gangs' (which are considered to have insufficient criteria to qualify as organised crime groups)

   - multi-tiered, terrestrial, hierarchical crime organisations such as the Mafia (and)

   - online organised crime groups, which 'will almost certainly emphasise lateral relationships, networks instead of hierarchies …'

   Susan W Brenner: Pages 36 - 47, '*Organised Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships'* (North Carolina Journal of Law and Technology, Volume 4, No. 1) (2002)

3. E Symeonidou-Kastanidou: Pages 83 – 103, '*Towards a New Definition of Organised Crime in the European Union*' ('European Journal of Crime, Criminal Law and Criminal Justice) (2007)

4. P Gottschalk: P 12, '*Criminal Entrepreneurship*' (Nova Science Publishers, Inc, New York) (2008)

5. 'Hence, Albanese's (2004) definition is the one we have adopted in this book …'

   P Gottschalk: P 10, '*Criminal Entrepreneurship*' (Nova Science Publishers, Inc, New York) (2008)

6. P Gottschalk: P 13, '*Criminal Entrepreneurship*' (Nova Science Publishers, Inc, New York) (2008)

7. P Gottschalk: P 16, '*Criminal Entrepreneurship*' (Nova Science Publishers, Inc, New York) (2008)

8. P Gottschalk: P 13, '*Criminal Entrepreneurship*' (Nova Science Publishers, Inc, New York) (2008)

9. It may be that, over time, online organised crime groups will separate into less heterogeneous groups which can more easily be categorised separately. However, for the moment, until the situation becomes clearer, it is probably more prudent to start from a

position where potential characteristics are included, as opposed to discounting some which be found to have value later.

10. M D Lyman and G W Potter: Page 71, '*Organised Crime*' (Pearson Prentice Hall, Upper Saddle River, New Jersey, 4th Edition) (2007)

    Cited in P Gottschalk: P 13, '*Criminal Entrepreneurship*' (Nova Science Publishers, Inc, New York) (2008)

11. P Gottschalk: P 15, '*Criminal Entrepreneurship*' (Nova Science Publishers, Inc, New York) (2008)

12. See, for instance, Page 3 of Finjan's '*Web Security Trends Report, Q2 2008*'

13. R C Lindberg, online article: '*The Mafia in America: Traditional Organised Crime in Transition – An Overview of Current Conditions*' (2002)

    http://www.richardlindberg.net/articles/mob.html

14. J O Finckenauer and E Waring: Page 7, '*Challenging the Russian Mafia Mystique*' (National Institute of Justice Journal) (April 2001):

    http://www.ncjrs.gov/pdffiles1/jr000247b.pdf

15. J O Finckenauer and E Waring: Page 6, '*Challenging the Russian Mafia Mystique*' (National Institute of Justice Journal) (April 2001):

    http://www.ncjrs.gov/pdffiles1/jr000247b.pdf

16. P Gottschalk: P 120, '*Criminal Entrepreneurship*' (Nova Science Publishers, Inc, New York) (2008)

17. Page 8, The 2008 '*Symantec Report on the Underground Economy* XII:

    http://www.symantec.com/en/uk/about/news/release/article.jsp?prid=20081124_11

18. For instance, there is a consensus view on the issue in the reports from 'Symantec', 'Finjan', 'Sophos' and 'McAfee' which are cited throughout this paper.

19. The definition of a 'shadow economy' is another area which is widely debated. In broad terms, a 'shadow economy' consists of profit-making activities in any country which are either borderline legal/illegal (for instance, because they are unrecorded and so do not generate taxes) or which are known to be illegal yet which, due to the extent to which they are undertaken in the country or because the goods supplied are only available illegally, are viewed by the population to be acceptable.

    A 'transition economy' occurs within a country which is in the process of undergoing a major change process in terms of its economy, for instance the transition from the former Soviet Bloc countries to, in the main, a capitalist culture. During this time, the laws and regulations of the country will be in flux, enabling organised criminals to exploit the situation by, for instance, 'filling the gaps' with their products.

20. For instance, the recent NESTA multi-disciplinary research report by the University of Brighton includes analysis of criminal business models within the financial sector:

'*Crime Online: Cybercrime and Illegal Innovation*' (July 2009), which includes contributions from the Metropolitan Police Service, as well as representatives from financial institutions:

http://www.nesta.org.uk/crime-online-cybercrime-and-illegal-innovation/

21. Tom Longstaff:

'I would say business process *is* the fundamental thing that you're trying to protect these days. The information associated with the business process, the different kinds of access controls and things (*about*) who participates and how do you know who'se participating in those business processes …'

'…you're not protecting a machine anymore. You're not protecting your database. What you're protecting is your business process. You're protecting the integrity. You're protecting the viability of the processes.'

Interview between J Allen and Tom Longstaff:: '*Evolving Business Models, Threats and Technologies: A Conversation with CERT's Deputy Director for Technology*' (CERT® 'podcast' and transcript) (December 2006):

http://www.cert.org/podcast/show/20061212longstaff.html

22. The consensus view in the industry reports cited above that online organised crime groups are definitively mimicking legitimate business tactics, as well as anticipating them, is accompanied in the reports by detailed examples of the types of tactics used. The examples below give a flavour of the range of criminal strategies that have been devised.

'Rogue ISPs' (the 'Pricewert' case)

CNet.com: '*Federal Trade Commission shuts down rogue ISP*' (June 2009)

http://search.myway.com/search/GGmain.jhtml?PG=SEASUSH&SEC=ABMANY&psa=_UkGfRVGZZwhc1yUG6Lgzw&ptnrS=DK&st=kwd&searchfor=federal+commission+shuts+down+rogue+ISP

ComputerWeekly.com: '*Cybercrooks Develop own Search Engines to Burgle Users*' (May 2009)

http://www.computerweekly.com/Articles/2009/05/07/235935/cybercrooks-develop-own-search-engines-to-burgle-users.htm

'Misleading Applications'

The following 'Symantec' report includes a list of 'Top 10' Misleading Applications (at December 2008):

Symantec White Paper: Pages 17-18, '*Web-based Attacks – February 2009*'

http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_web_based_attacks_03-2009.en-us.pdf

'Instructional Videos'

ComputerWorlduk.com: '*Behind the Scenes of an Online Fraudster's Arrest*' (April 2009)

http://www.computerworlduk.com/management/security/cybercrime/in-depth/index.cfm?articleid=2224

'Copyright Notices'

The Register.co.uk: (April 2008)

http://www.theregister.co.uk/2008/04/28/malware_copyright_notice/

'Terms and Conditions'

Fraudwar.Blogspot.com: '*Internet Gangstas Don't Appreciate Software Piracy, Either!*' (May 2008)

http://fraudwar.blogspot.com/2008/05/internet-gangstas-dont-appreciate.html

23. J O Finckenauer and E Waring: Page 7, '*Challenging the Russian Mafia Mystique*' (National Institute of Justice Journal) (April 2001)

    http://www.ncjrs.gov/pdffiles1/jr000247b.pdf

24. G P Gilligan, P 3, '*Business, Risk and Organised Crime*', *Journal of Financial Crime, Volume 14, No 2* (2007)

25. P Gottschalk: P 91'*Criminal Entrepreneurship*' (Nova Science Publishers, Inc, New York) (2008)

    An alternative model (activity-based, knowledge-based, strategy-based and value-based) is proposed. (Pages 92-94) The additional value-based layer recognises the stage at which organisations have 'a strong common sense of shared values' and culture, as demonstrated by some of the case study groups in the 'Organisational Culture' section of Table 6.

    In addition, Gottschalk proposes 6 characteristics, together with lifecycle theory, as additional potential topics for research into the classification and categorisation of criminal organisations. (Page 92)

26. P Gottschalk: P 66, '*Criminal Entrepreneurship*' (Nova Science Publishers, Inc, New York) (2008)

27. The MA methodology approach utilised in this paper is based on:

    C E Heldon: '*Exploratory Analysis Tools*' (Pages 112-114, J H Ratcliffe (Ed), 'Strategic Thinking in Criminal Intelligence' (The Federation Press)) (2004, 2007)

    The origins of this methodology are explained in T Ritchey's paper:

    '*General Morphological Analysis (MA) – A General Method for Non-Quantified Modelling*'

    (Adapted from the paper 'Fritz Zwicky, Morphologie and Policy Analysis', presented at the 16th EURO Conference on Operational Analysis, Brussels) (2003-2009)

    http://www.swemorph.com/ma.html

28. For instance, see the International Association of Crime Analysts (IACA) website:

http://www.iaca.net/Software.asp

29. P Gottschalk:: '*Criminal Entrepreneurship*' (Nova Science Publishers, Inc, New York) (2008)

30. J H Ratcliffe (Ed): '*Strategic Thinking in Criminal Intelligence*' (The Federation Press) (2004, 2007)

31. J S Albanese: '*Risk Assessment in Organised Crime: Developing a Market and Product-Based Model to Determine Threat Levels*' (Pages 273 – 272, Journal of Contemporary Criminal Justice, Volume 24, Number 3) (August 2008)

    http://jayalbanese.com/organized_crime

32. J S Albanese: Page 269, '*Risk Assessment in Organised Crime: Developing a Market and Product-Based Model to Determine Threat Levels*' (Pages 273 – 272, Journal of Contemporary Criminal Justice, Volume 24, Number 3) (August 2008)

    http://jayalbanese.com/organized_crime

    Albanese's risk assessment methodology proposals, although they are aligned with the approach of current reports about online organised crime, have not yet been analysed from such a perspective. To exploit their true potential would require a paper in itself, hence they are only mentioned here as a possible avenue for future research.

33. C E Heldon: Page 112, '*Strategic Thinking in Criminal Intelligence*' (J H Ratcliffe (Ed), The Federation Press) (2004, 2007)

34. The instructions for using the methodology that follow are based on Ritchey's paper, as well as:

    C E Heldon: Page 113, '*Strategic Thinking in Criminal Intelligence*' (J H Ratcliffe (Ed), The Federation Press) (2004, 2007)

References

6. CONCLUSION

1. '*Sneakers*' is a 1992 'comedy-thriller' film inspired by the first generation of hackers. Its plot brings together cryptography, organised crime, the Russian Government and the US National Security Agency, in an early dramatic portrayal of organised crime within a technological context.

   The Internet Movie Database:

   http://www.imdb.com/title/tt0105435/quotes

2. J S Albanese: '*Risk Assessment in Organised Crime: Developing a Market and Product-Based Model to Determine Threat Levels*' (Pages 273 – 272, Journal of Contemporary Criminal Justice, Volume 24, Number 3) (August 2008)

   http://jayalbanese.com/organized_crime

3. McAfee: Page 10, '2009 *Threat Predictions*'

   http://www.mcafee.com/us/threat_center/white_paper.html

4. McAfee: Page 10, '2009 *Threat Predictions*'

   http://www.mcafee.com/us/threat_center/white_paper.html

5. A Emigh and Z Ramzan: Page 28 (*Understanding New Attacks and Defences*' (M Jakobsson and Z Ramzan (Eds), Addison Wesley) (2008)

8 KEY TERMS

8.1 Definitions of Key Terms As Used Within This Paper and its Appendices

Business Model – A business model is a high-level, conceptual representation of a commercial organisation's structure and key activities. It includes components such as the business process, customer identification and markets, as well as products and services. It is usual for businesses to amalgamate relevant features from different business models, according to the needs of their own organisation.

Although there are many different types of business model, to date the literature about online organised crime has tended to focus on certain types, for instance:

Subscription business models, collective business models (whereby resources are pooled between organisations), online auction business models and industrialisation of services business models.

Business and Information Security Professionals – Within this paper, the term 'business and Information Security (IS) professionals' refers to staff at management grade, in particular staff within Senior Management Teams. The term assumes that these staff will have the authority to make the corporate decisions which this paper discusses.

Entrepreneur – Within the context of this paper, an entrepreneur is 'someone who creates value by offering a product or service in order to obtain certain profit.'

(P Gottschalk: Page 43, '*Criminal Entrepreneurship*' (Nova Science Publishers, Inc, New York) (2008))

Jurisdictional Arbitrage – A term to describe the exploitation of legal loopholes.

Leveraging (*Project Title*) – 'Military Dictionary: (US Department Of Defence) In information operations, the effective use of information, information systems and technology to increase the means and synergy in accomplishing information operations strategy.' (*Answers.com*)

Organised Crime – Generic term that may apply to all types of organised crime activity, whether terrestrial or technology-oriented

Online Organised Crime – Potential or actual criminal activity that primarily targets the Internet environment

Terrestrial Organised Crime – Potential or actual criminal activity that primarily targets the physical environment, as opposed to the technology-oriented environment

Technology-oriented Organised Crime – Potential or actual criminal activity that primarily targets any aspect of the Information and Communications Technology (ICT) environment, including the Internet

9 GLOSSARIES

9.1 GLOSSARY OF ACRONYMS

Abbreviation/Acronym	Meaning	Additional Comments
CAAS	Crimeware-as-a-Service	See Glossary of IS and Technical Terms
CARPO	CARDS Regional Police Project	An EU-sponsored initiative
CERT	Computer Emergency Response Team	Based at Carnegie Mellon University in the United States
CSI	Computer Security Institute	
DoS	Denial of Service attack	See Glossary of IS and Technical Terms
DDoS	Distributed Denial of Service attack	See Glossary of IS and Technical Terms
DMZ	Demilitarised Zone	See Glossary of IS and Technical Terms
DNA	Deoxribonucleic acid	A nucleic acid that contains the genetic instructions for all life forms
FBI	(US) Federal Bureau of Investigation	
ICANN	Internet Corporation for Assigned Names and Numbers	ICANN is a non-profit international 'public benefit' corporation which 'promotes competition and develops policy on the Internet's unique identifiers.' http://www.icann.org/en/about/
IRC	Internet Relay Chat	See Glossary of IS and Technical Terms
IS	Information Security	Within the context of this paper, the abbreviation 'IS' refers to 'Information Security'
ISP	Internet Service Provider	See Glossary of IS and Technical Terms
MA	Morphological Analysis	A quantifiable methodology to aid strategic thinking and problem-structuring: http://www.swemorph.com/ma.html
NCIA	National Criminal Intelligence Agency (UK)	Absorbed within SOCA in April 2006
NCIS	National Criminal Intelligence Service (UK)	Absorbed within SOCA in April 2006

NCS	National Crime Squad (UK)	Absorbed within SOCA in April 2006
NHTCU	National Hi-Tech Crime Unit (UK)	Absorbed within SOCA in April 2006
OECD	Organisation for Economic Co-Operation and Development	
OOCG	Online Organised Crime Group	Within the context of this paper, the abbreviation 'OOCG' refers to online organised crime groups
PDA	Personal Digital Assistant	See Glossary of IS and Technical Terms
RICO	Racketeer Influenced and Corrupt Organisations Act 1970	US legislation
SAAS	Software-as-a-Service	See Glossary of IS and Technical Terms
SOCA	Serious Organised Crime Agency (UK)	Launched in 2005 and dubbed the 'British FBI' by the media (Ref), SOCA incorporated the former NCS, the NCIS, the NCIA and the NHTCU within a single organisation
T0C	Transnational Organised Crime	Formally defined by the UN in the '*United Nations Convention on Transnational Organised Crime*' (2000) TOC was identified as the 10th threat in the United Nations list of identified serious world threats (December 2004): http://www.un.org/secureworld/report.pdf
TOCG	Terrestrial Organised Crime Groups	Within the context of this paper, the abbreviation 'OOCG' refers to terrestrial organised crime groups
UNTOC	United Nations Convention on Transnational Organised Crime	
VoIP	Voice over Internet Protocol	See Glossary of IS and Technical Terms
VPN	Virtual Private Network	See Glossary of IS and Technical Terms

9.2 GLOSSARY OF INFORMATION SECURITY AND TECHNICAL TERMS USED WITHIN THIS PAPER AND THE APPENDICES

IS/Technical Term	Meaning
Adware	'Adware displays selected ads in pop-up windows or in the main browser window.' Pfleeger and Pfleeger: Page 623, '*Security in Computing – 4th Edition*' (Prentice Hall) (2007) Of itself, adware, as is also the case with keyloggers and spyware products, is not intrinsically illegal. In all three cases, it is the way in which the product is used which determines its legal status. Most adware is compiled using *JavaScript*, whose functions can be misused so that adware residing on an innocuous website, when accessed, can redirect the user to a malicious destination.
Automatic/ Automated Teller Machine (ATM)	A 'machine where customers use a bank card or debit card to carry out banking operations such as withdrawals, deposits, transfers and bank payments.' Merriam-Webster Visual Dictionary Online: http://visual.merriam-webster.com/society/economy-finance/bank/automatic-teller-machine-(atm).php
Biometrics	A form of authentication based on a person's physical characteristics, for instance their fingerprints.
Cached data	'Caching' is the process of storing data in a temporary location for later reuse.
Carding	'Carding' refers to illegal activities arising from the compromise of an individual's credit or debit card (card fraud), for instance impersonation of their identity.
Crimeware	'Crimeware is a subclass of the more broad category of malware, which refers generally to unwanted software that performs malicious actions on a user's computer.' (Page 3) 'Crimeware is software that performs illegal actions unanticipated by a user running the software; these actions are intended to yield financial benefits to the distributor of the software.' (Page 2) M Jakobsson and Z Ramzan: '*Crimeware – Understanding New Attacks and Defences*' (Addison Wesley) (2008)

Crimeware-as-a-Service (CaaS)	Technically, CaaS refers to viral code which resides 'in the cloud' *, as opposed to on a host, in a similar way to the SaaS model. 'CaaS provides malware on demand to the infected host.' Syscon.com: '*Hidden Dangers: Crimeware-as-a-Service (Caas)*' http://www.sys-con.com/node/678589 * As used here, 'in the cloud' refers to code which resides on the Internet.
Demilitarised Zone (DMZ)	A demilitarised zone is a designated 'buffer' area within a network which separates sensitive systems and data from direct access via the Internet.
Denial of Service (DoS)	A Denial of Service attack comprises any kind of attack on the availability of information.
Distributed Denial of Service (DDoS)	These 'command and control' mass attacks use spam or other messages to overwhelm their target systems via a distributed system of 'zombie' machines, which are compromised corporate or domestic machines that have been infected with malicious code. 'Zombies' lie dormant until they receive a command from the 'botherder These 'command and control' mass attacks use spam or other messages to overwhelm their target systems via a distributed system of 'zombie' machines, which are compromised corporate or domestic machines that have been infected with malicious code. 'Zombies' lie dormant until they receive a command from the 'botherder' (aka 'zombie master'), at which point they respond en masse. Both the 'botherder' and the 'zombies' can be located anywhere in the world and messages can pass through many routers, hubs and open proxy servers (which will mask the sending computer's unique identifier, its IP address) on their way to their destination. A typical contemporary botnet scenario is outlined in: e-Week: '*Pump-and-Dump Spam Surge Linked to Russian Bot Herders*' (November 2006): http://www.eweek.com/c/a/Security/PumpandDump-Spam-Surge-Linked-to-Russian-Bot-Herders/ See also: Terrence Berg, Computer Law: Pages 20 and 21, '*The Changing Face of Cybercrime – New Internet Threats Create Challenges to Law Enforcement*' (Date not published, 2007?): http://www.michbar.org/journal/pdf/pdf4article1163.pdf
Drive-By Downloads	A drive-by download is a type of attack whereby malicious software automatically infects the user's machine covertly if they browse to a malicious website

e-Currencies	'e-Currencies' is a generic term which refers to currencies in digital form such as e-Gold.
Encryption	'Encryption is the process of encoding a message so that its meaning is not obvious.' Pfleeger and Pfleeger: Page 38, '*Security in Computing – 4th Edition*' (Prentice Hall) (2007)
Fast-flux services	'Fast-flux' services aim to enable a fully-qualified domain name (eg www.example.com) … to have hundreds or even thousands of IP addresses assigned to it … with the addresses being 'swapped out' very quickly. The result is that website hostnames can be associated with a new set of IP addresses 'as often as every 3 minutes', which increases the likelihood that these sites will avoid detection by detection software. The Honeynet Project: 'Know Your Enemy: Fast-Flux Service Networks' (August 2008) http://www.honeynet.org/papers/ff/
(Default) Gateway	'A default gateway is the device that passes traffic from the local subnet to devices on other subnets. The default gateway often connects local devices to the Internet …' Compnetworking.About.com: 'What is a Default Gateway?': http://compnetworking.about.com/od/internetaccessbestuses/f/default_gateway.htm
ID 'Theft'	'…Identity theft is taking another person's identity. Use of another person's credit card is fraud; taking out a new credit card in that person's name is identity theft.' Pfleeger and Pfleeger: Page 618, '*Security in Computing – 4th Edition*' (Prentice Hall) (2007)
Internet	The Internet is a public world-wide system of interconnected computers.
Internet Relay Chat (IRC)	'An Internet communications protocol … (*which*) … offers real-time group communications, requires very little bandwidth and the IRC client software is freely available across all operating systems.' Page 5, The 2008 '*Symantec Report on the Underground Economy* XII: http://www.symantec.com/en/uk/about/news/release/article.jsp?prid=20081124_11
Internet Service Provider (ISP)	An Internet Service Provider is 'normally a host which is connected full-time to other hosts and which provides access and other services to its subscribers.'

	C Reed: '*Internet Law – Text and Materials – 2nd Edition*' (Cambridge University Press) (2004)
IP Address	'IP' stands for 'Internet Protocol', a type of network communication protocol which, together with TCP (Transmission Control Protocol), comprises TCP/IP, the network protocol which is used for the Internet. An IP address is a unique identifier allocated to computers using the Internet.
Keyloggers	Keyloggers are hardware or software devices that capture data typed into keypads.
Malware	'In addition to crimeware, malware encompasses legal but malicious software such as adware and spyware, and illegal software without a commercial purpose, such as destructive viruses.' Joint Report between the US Department of Homeland Security, SRI International Identity Theft Technology Council and the Anti-Phishing Working Group, sponsored by the US Dept of Homeland Security Science and Technology Directorate: Page 4, '*The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond*' (October 2006) http://www.antiphishing.org/reports/APWG_CrimewareReport.pdf
Metadata	Metadata comprises properties which are associated with a piece of data, for instance the size of the data or the date it was created.
Obfuscated URLs	'Obfuscation' is a technique which conceals 'an attack by making its operation more complex and thus harder to detect.' Symantec White Paper: Page 11, '*Web-based Attacks – February 2009*': http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_web_based_attacks_03-2009.en-us.pdf Obfuscating a Universal Resource Locator (URL) hides the true address of a webpage so that, for instance, a user is relocated to a different webpage than the one they thought they were accessing.
PDA (Personal Digital Assistant)	External storage and application portable devices which can connect and synchronise their information with PCs, laptops and other equipment. (Eg *Blackberries*)
Phishing	'Attempting to fraudulently acquire a person's credentials, usually for financial gain.' M Jakobsson and Z Ramzan: Page 168, '*Crimeware – Understanding New Attacks and Defences*' (Addison Wesley) (2008)

Ransomware	An attack technique whereby the data is encrypted and a financial demand made to restore it.
Rootkit	'A rootkit is a program or set of programs and files that attempts to conceal its existence … Usually the rootkit contains some malware that is being hidden as well.' A S Tanenbaum: Page 686, '*Modern Operating Systems*' (Pearson International Edition) (2009)
Scareware	'Scareware' refers to malicious tactics which are deliberately intended to cause shock or concern so that, for instance, the victim responds by buying a fraudulent security application. The term is also used to describe the fraudulent security applications themselves.
Software as a Service (SaaS)	SaaS is 'a software delivery method that provides access to software and its functions remotely as a Web-based service.' Users pay a subscription fee to access the software 'on demand'. Webopedia.com: 'What is SAAS'? http://www.webopedia.com/TERM/S/SaaS.html
Spam	'Spam' is an Information Security term that is attributed to a *Monty Python* comedy sketch in which the participants are overwhelmed by repeated chanting of the word 'spam'. 'Spamming' refers to the mass mailing of unwanted e-mail messages which are able to inundate a user's e-mail account.
Spyware	'Spyware' is a generic term for covert surveillance software. Spyware includes remote viewing software applications and keystroke loggers (keyloggers). Pfleeger and Pfleeger: Page 632, '*Security in Computing – 4th Edition*' (Prentice Hall) (2007)
SQL Injection Attack	A description of a SQL injection attack, within the context of the Heartland Payment Systems online organised crime case, is described below: BBC.co.uk: 'US man "stole 130m card numbers" ' (August 2009) http://news.bbc.co.uk/1/hi/business/8206305.stm
Trojan	A Trojan is a digital technique which downloads malicious code alongside a seemingly-innocuous legitimate programme. It is: 'a piece of software in which unauthorised computer instructions have been secretly inserted; or hardware in which unauthorised circuitry or mechanisms have been secretly

	inserted.' D P Parker: Page 72, '*Fighting Computer Crime*' (Wiley Computer Publishing) (1998) The term 'trojan' was inspired by the classical Roman account in Virgil's '*Aeneid*'. The epic poem describes a tactic used during the Trojan War whereby the Greek army tricked the Trojans into bringing a large wooden horse that had been left outside within the walls of Troy. The horse was not as benign as it seemed because it contained Greek soldiers who, once inside, emerged and defeated the Trojan defence. The story has come to represent any strategy which appears benign but which is designed to breach a fortified security perimeter.
Virus	A computer virus is a type of malicious code which relies on a carrier to replicate. A 'polymorphic virus' is a type of computer virus which changes its code each time it infects a new file.
VoIP (Voice over Internet Protocol)	The technology that enables telephone calls to be transmitted over the Internet.
VPN (Virtual Private Network)	A VPN provides a secure channel for communication across the Internet, using encryption.
Web (World Wide Web)	The World Wide Web (WWW) is a sub-division of the Internet which links document files via 'hypertext'. The documents are annotated using the HTML (HyperText Markup Language) protocol. 'Hypertext' – 'A computer-based text retrieval system that enables a user to access particular locations in webpages or other electronic documents by clicking on links within specific webpages or documents.' Answers.com: http://www.answers.com/topic/hypertext
Web 2.0	'Web 2.0' refers to 'the second generation of the design of the World Wide Web', in particular 'the movement away from static webpages to dynamic and shareable content and social networking.' Wiktionary.org: http://en.wiktionary.org/wiki/Web_2.0
Web Hosting	'The service of hosting a site on the Internet making it viewable for others on the Net.' Wiktionary.org:

	http://en.wiktionary.org/wiki/web_hosting
Worm	A 'worm' is a self-replicating type of malicious code which spreads via networks. Pfleeger and Pfleeger: Page 116, '*Security in Computing – 4th Edition*' (Prentice Hall) (2007)
3G Phones	The 'third generation' of mobile phone technology

Appendix A

Terrestrial/Technically-Oriented Organised Crime Group Theoretical Characteristics

Table 1 – Raw data (for characteristics which have been identified as predominantly terrestrial but which may also be technology-oriented by inference *) extracted from a broad range of sources, with sources cited.

Table 2 – Rationalised version of the raw data from ***Table 1***, with sources cited

Table 3 – Raw data (specifically for terrestrial/technology-oriented organised crime group characteristics) extracted from a typical range of sources, with sources cited

Table 4 – Comparison between ***Table* 2** data and rationalised version of the raw data from ***Table 3***, with sources cited

Table 5 – Summary comparison of typical terrestrial/technically-oriented and specific technology-oriented organised crime group characteristics.

Table 6 – Maps technology-oriented organised crime group characteristics against real-life case study examples.

* Perhaps the most important point to make about the sources for the first 2 tables is that they do not strictly represent terrestrial crime group characteristics per se. It is more accurate to say that they represent characteristics which have been identified as definitely applying to terrestrial organised crime groups (for instance, for the earlier sources) and which, for some of the sources (eg UNTOC), may also apply to technology-oriented groups as well, although the inference in each case is implied not stated.

Table 1 summarises characteristics identified between 1990 and 2008. ***Table 2*** further summarises the findings from ***Table 1***, which are somewhat unwieldy in their raw form, and adds the items from UNTOC for comparison purposes. ***Table 2*** then provides a workable synopsis as the basis for comparison with the data from ***Tables 3*** *and* ***4****.*

In addition, ***Table 2*** shows the similarities and differences of interpretation between UNTOC and some of the other sources, with the other sources including more granularity than UNTOC within their definitions.

Table 3 comprises some of the technology-oriented organised crime group characteristics which are commonly cited by sources as significant. Whereas the terrestrial/technology-oriented sources are all well-established (including Albanese, whose 2008 list is an update of an earlier 2001 version), spanning a time range between 1990 (Abadinsky) and 2008 (Albanese et al), the specific technology-oriented sources are much more recent, with a time range between 2001/2 (Williams) and 2009 (some of the additional sources) and are therefore drawn inevitably from fewer case studies. Even so, the technology-oriented sources take the approach that technologically-oriented organised crime is a genuine problem, that it comprises some elements which are unique to the technology-oriented environment and that it is enabled by the online environment (the 'Web') in particular. They also identify many specific elements which fall within the category of 'Strategy/Tactics'.

Table 4 is similar to ***Table 2*** in that it rationalises the elements from ***Table 3*** into a slightly less unwieldy format. However, whereas ***Table 2*** compares the UNTOC definitions with those from other sources, ***Table 4*** compares terrestrial/technology-oriented characteristics and sources with those which may have a particular significance when considering technology-oriented organised crime groups.

Table 5 further rationalises the technology-oriented elements and presents them alongside the terrestrial/technology-oriented characteristics without their sources.

Finally, ***Table 6*** maps the technology-oriented characteristics against real-life case study examples.

Analysis of the tables is subject to the following necessary qualifications:

1. The items in the tables are by no means intended to be in any way definitive, although, between them, they do represent most of the identified main characteristics of the organised crime groups themselves (as opposed to their specific activities) which have been highlighted in the literature. Similar versions of the tables could be constructed using information from other authors, with the items mapped against different categories, according to purpose. Also, some of the items constitute sub-lists in themselves, for instance the UNTOC definitions and those aggregated from other sources by Albanese. A more granular approach could also be applied by including additional criteria to those identified here.

2. Neither are the tables intended to indicate that the authors and organisations do not recognise each other's characteristics as valid. This may not be the case at all (for instance, authors may have cited other characteristics elsewhere than the sources cited here), although a few items are contradictory (for instance, where sources differ from each other in ***Table 1*** as to whether organised crime groups are 'ideological' or 'non-ideological').

3. There are also some minor differences of interpretation and nuance where sources have used the same or very similar terms and the reader is referred to the original sources for further, more precise explanations.

Notwithstanding the above qualifications, the tables remain representative of the main identified organised crime group characteristics, with sufficient similarities between the items for them to enable them to be grouped together for high- level purposes.

Table 1

Raw Data - Range of Typical Characteristics of Organised Crime Groups

Category	Abadinsky[1] (1990)	Maltz[2] (1994)	EU/Europol[3] (2002)	Gilinskiy[4] (2006)	Europol[5] (2008)	Albanese[6] (2008)*	Additional items Identified from other sources
1. Organisational Structures			Collaboration of more than two people (M)				
							Capable of either a centrally-focussed or diffuse structure (Fiorentini and Peltzman, 1995) [a]
							Vertically-integrated structure (Garoupa, 1997) [b]
		Structure	Having a commercial or business-like structure (O)	A complex hierarchical structure with functions assigned to specific units of the organisation	Group Structures	Use of legitimate business structures	
	Hierarchical	Hierarchical		A complex hierarchical structure with functions assigned to specific units		Organised hierarchy continuing (ie a	Hierarchy (Reuter, 1984) [c]

Category	Abadinsky[1] (1990)	Maltz[2] (1994)	EU/Europol[3] (2002)	Gilinskiy[4] (2006)	Europol[5] (2008)	Albanese[6] (2008)*	Additional items Identified from other sources
				of the organisation		continuing, structured enterprise) (MT) *	
			Having a specialised division of labour (O)	A complex hierarchical structure with functions assigned to specific units of the organisation	Specialisation	Specialisation	
2. Organisational Goals			Having as its central goal the pursuit of profit and/or power (M)	The deriving of maximum profits as the key goal of the activity		Rational profit through crime (MT) *	
	Non-ideological	Ideology (or lack thereof) (N)				Non-ideological	
						Public demand for services (MT) *	
3. Organisational Strategy/ Tactics			Suspected of the commission of serious criminal offences (M) Involved in money-laundering ****** (O)	The criminal nature of the activity and associated financial activities			

Category	Abadinsky[1] (1990)	Maltz[2] (1994)	EU/Europol[3] (2002)	Gilinskiy[4] (2006)	Europol[5] (2008)	Albanese[6] (2008)*	Additional items Identified from other sources
3. Organisational Strategy/ Tactics	Governed by explicit rules and regulations	Discipline (N)	Utilising a system of discipline and control (O)				
	Uses illegal violence and bribery Demonstrates illegal violence and bribery	Violence (G)	Using violence and other means of intimidation (O)		Use of violence	Use of force or threat (MT)	
			Operating internationally, across national borders (O)		The international dimension		
		Corruption (G)	Exerting influence over politics, judicial bodies, media, the economy (O)	The corruption of powerful organisations and individuals, especially law-enforcement bodies, as the main means of the criminal activity	Influence	Corruption of public officials to maintain immunity (MT) *	Authority of reputation ** (Finckenauer, 2005)[d]
		Multiple enterprises (G)					Multiple enterprises (Reuter, 1983)[e]
						Restricted	

Category	Abadinsky[1] (1990)	Maltz[2] (1994)	EU/Europol[3] (2002)	Gilinskiy[4] (2006)	Europol[5] (2008)	Albanese[6] (2008)*	Additional items Identified from other sources
						membership	
							Incorporate both national and foreign members (CARPO, 2006) [f]
		Involvement in legitimate enterprises			Use of legitimate business structures		
4. Organisational Maturity							
	Perpetuitous (ie tending towards longevity)	Continuity (G) Sophistication (N)	Taking place over a prolonged or indefinite period of time (M)	A stable association of people, designed for long-term activity	Counter-measures ****	Organised hierarchy continuing (ie a continuing, structured enterprise) (MT) *	Durability (Reuter, 1984) [g]
							Insulation (Royal Canadian Mounted Police)*****
5. Organisational Culture		Bonding rituals (N)				Code of secrecy	Authority of reputation ** (Finckenauer, 2005) [h] Self-Identification (Finckenauer, 2005) [i]
6. Organisational	Monopolistic**			The aspiration to monopoly in a certain		Monopoly over particular market	Lends themselves to monopoly (Schelling,

Category	Abadinsky[1] (1990)	Maltz[2] (1994)	EU/Europol[3] (2002)	Gilinskiy[4] (2006)	Europol[5] (2008)	Albanese[6] (2008)*	Additional items Identified from other sources
Environment				sphere of trade on certain territories			1971) [J]

EU/Europol items: (M) Mandatory (O) Optional; Maltz items: (G) Generic (N) 'Non-Generic' (ie here, meaning characteristics of some organised crime groups which are not necessary nor typical); Albanese: (MT) Most Typical

---

* Albanese – Using his own sample of authors, Albanese conducted a similar exercise to that used to create this table. He identified typical 10 characteristics which he ranked according to the number of times they were cited. He then reduced these to the top 5:

> organised continuing hierarchy; rational profit through crime; use of force or threat; corruption of public officials to maintain immunity; public demand for services.

** Finckenauer – 'Authority of Reputation' is the ability to coerce others by suggestion, through reputation, without the necessity for violence; 'Self-Identification' is the act of identifying with the organisation, evidenced by (eg) initiation rites.

*** Monopolistic – In their introduction, Fiorentini and Peltzman (Page 5) comment that they share Reuter's view, which is opposed to Schelling's, that monopolisation is becoming less of a significant characteristic of organised crime and that this is supported by a growing body of empirical evidence, although it still retains a role in 'cartel' activities which tend to be vertically-integrated, such as money laundering and narcotics. Fiorentini explains the reasoning behind this view in his essay on oligopolistic competition in illegal markets (P 274, '*The Economics of Organised Crime*')

**** 'Countermeasures' as used here, has a different meaning to the usage of the term within Information Security, as explained in Section 2.7, Page 13, 'EU Organised Crime Threat Assessment: 'OCTA 2007'. Within the Report, it describes a wide range of countermeasures which organised crime groups use against police action and detection, including 'false identities, spoofing and encryption'.

***** Royal Canadian Mounted Police (Criminal Intelligence Division) – 'Insulation' refers to 'protection of the organisation's leaders by separating them from the soldiers, cell from cell, and function from function.' (Page 4, '*Transnational Criminal Organizations, Cybercrime and Money Laundering*' (J R Richards, CRC Press LLC) (1999)

****** EU/Europol 2002 – Although 'Money laundering' is included here because it was cited by EU/Europol, will be considered in the paper as a type of threat (as opposed to an organised crime group characteristic).

The table shows organised crime characteristics which were highlighted by a sample of sources as significant between the period 1990 – 2008.

Reading by Row – Identifies where sources concur that individual items are significant.

Reading Vertically – Identifies that, between 1990 and 2008, there is very strong consensus between the sources that:

- Organised crime groups have some sort of structure (although sources may disagree as to the exact nature of that structure)

- Violence and corruption are significant organisational strategies

- Organised crime groups have a tendency towards continuity.

With regard to organisational structures and goals, there is some agreement between the sources that organised crime group structures are analogous with those of legitimate businesses and that profit-seeking is a significant organisational goal.

Main Sources

[1] H Abadinsky, ' Organised Crime' (3rd Edition) (Nelson Hall, Chicago, Illinois) (1990)

[2] M D Maltz, pp 21-37, '*Defining Organised Crime', 'Handbook of Organised Crime in the United Sates',* (Greenwood Press, Westport, CT) (1994)

[3] Joint EU/Europol Report - (Sec 2001) 433 Commission Staff Working Paper: Joint Report from Commission Services and Europol: '*Towards a European Strategy to Prevent Organised Crime*' (The organised crime 2001 Report criteria were cited in T Newburn: '*Criminology*', Page 406, Willan Publishing, 2007)

[4] Y Gilinskiy: Pages 259-292, '*Crime in Contemporary Russia'*, 'European Journal of Criminology, 3 (3) (2006)

[5] Europol - EU Organised Crime Threat Assessment: '*OCTA 2008*', P 13;

http://www.europol.europa.eu/publications/European_Organised_Crime_Threat_Assessment_(OCTA)/OCTA2008.pdf

[6] J S Albanese: Page 264, '*Risk Assessment in Organised Crime: Developing a Market and Product-Based Model to Determine Threat Levels*' (Journal of Contemporary Criminal Justice 2008: 24; 263. Originally published online – May 8, 2008)

http://jayalbanese.com/yahoo_site_admin/assets/docs/AlbaneseRiskAssessmentJCCJ2008.44114959.pdf

Additional Items Identified from Other Sources

[a] G Fiorentini and S Peltzman: Page 5, '*The Economics of Organised Crime*' (Centre for Economic Policy Research, Cambridge University Press) (1995)

[b] N Garoupa: ABSTRACT : '*The Economics of Organised Crime and Optimal Law Enforcement'* (Economics Working Papers, No 246, Dept of Economics and Business, Universitat Pompeu Fabra) (1997)

[c] P Reuter: '*Disorganised Crime – Illegal Markets and the Mafia*', Page 175 (The MIT Press – Cambridge, Massachusetts; London, England) (Aka '*Disorganised Crime – The Economics of the Visible Hand'*) (1983)

[d] O Finckenauer: Pages 63-83, '*Problems of Definition: What is Organized Crime? Trends in Organized Crime'*(2005)

[e] Reuter, Ibid: Page P 175

[f] CARPO (CARDS Regional Police Project) Report: Page 16, '*Organised Crime and its Salient Features*' (2006)

http://www.coe.int/t/dghl/cooperation/economiccrime/organisedcrime/projects/CARPO/Pctc_2006_20.pdf

[g] Reuter, Ibid Page 175

[h] O Finckenauer, Ibid

[i] O Finckenauer, Ibid

[j] T C Schelling: Pages 155-166, '*What is the Business of Organised Crime*?' ('Journal of Public Law', 20, 71-84) (1971)

Table 2

Summary Version – Range of Typical Characteristics of Organised Crime Groups, with UNTOC and Sources

Category	Item No	UN Convention on Transnational Organised Crime (UNTOC)	Table 1	Source (Table 1)
1. Organisational Structures	1	Structured Criminal Group	Structure/ Group Structure	Maltz/ Europol (2008)
	2	Collaboration ('three or more persons')	Collaboration of more than 2 people (M)	EU/Europol (2002)
	3	Fluid, changeable roles, membership and structure ('does not need to have formally-defined roles for its members, continuity of its membership or a developed structure')	Centrally-focussed or diffuse structure	Fiorentini and Peltzman
	4		Hierarchical structure	Abadinsky/ Maltz/ Gillingsky/ Albanese/ Reuter/ MT
	5		Vertically-integrated structure	Garoupa
	5		Commercial/ business-like structure	EU/Europol (2002)/Albanese/
	7		Specialised division of labour	EU/Europol (2002)/ Gilinsky/ Europol (2008)/ Albanese
2. Organisational Goals	8	Formed for a planned purpose ('not randomly formed for the immediate commission of an offence')		
	9	Financial or other material goals ('financial or other material benefit')	Pursuit of profit and/or power	EU/Europol (2002)/ Gillingsky/ Albanese
	10		Monopolistic	Abadinksy/ Gillinsky/Albanese/ Schelling
2. Organisational	12		Non-Ideological	Abadinsky/Albanese
	13		Ideological or Non-Ideological	Maltz

Category	Item No	UN Convention on Transnational Organised Crime (UNTOC)	Table 1	Source (Table 1)
Goals	14		Public demand for services	Albanese
3. Organisational Strategy/ Tactics	15	Criminal intent ('with the aim of committing one or more offences')	Involved in serious criminal offences (eg money-laundering)	EU/Europol (2002)/ Gillingsky
	16		Involved in legitimate enterprises	Maltz/ Europol (2008)
	17		Control (eg explicit rules and regulations, discipline)	Abadinsky/ Maltz/ EU/Europol (2002)
	18	Article 1 (Statement of Purpose) – The purpose of this convention is to promote cooperation and combat transnational organized crime more effectively.	Operates internationally	EU/Europol (2002)/ Europol (2008)
	19		Multiple enterprises	Maltz/ Reuter
	20		Includes both national and foreign members	CARPO (2006)
	21		Restricted membership	Albanese
	22		Violence	Abadinsky/ Maltz/ EU/Europol (2002)/ Europol (2008)/Albanese
	23		Bribery	Maltz
	24		Corruption	Maltz/ EU/ Europol (2002)/ Gilinskiy/ Europol (2008)/ Albanese/ Finckenauer
	25	Direct or indirect methods ('direct or indirect')		
4. Organisational Maturity	26	Continuity ('existing for a period of time')	Tending towards continuity	Abadinksy/ Maltz/ EU/Europol (2002)/ Gillinsky/ Europol (2008)/ Albanese/ Reuter
	27		Insulation	Royal Canadian Mounted Police

Category	Item No	UN Convention on Transnational Organised Crime (UNTOC)	Table 1	Source (Table 1)
5. Organisational Culture	28		Bonding Rituals	Maltz
	29		Code of Secrecy	Albanese
	30		Authority of Reputation	Finckenauer
	31		Self-Identification	Finckenauer
6. Organisational Environment	32		Monopolistic	Abadinksy/ Gilinskiy/ Albanese/ Schelling

Table 3

Raw Data - Range of Typical Characteristics of Technically-Oriented Organised Crime Groups

Category	Williams[2] (2001/2002)	Europol High Tech Crime Centre[3] (2007)	Wall [1] (2008) *	Etges and Sutcliffe[4] (2008)	Symantec [5] (2008)	Finjan[6] (2008)	Additional items Identified from other sources
1. Organisational Structures							'Huge number' of people (MessageLabs®, 2008)[a]
	Flexible Adaptable	Very flexible structure	Transient, lateral and fluid forms	Decentralised, loose relationships Transitory relationships			Transient, lateral and fluid forms (Brenner, 2002)[b] Decentralised (ISF, 2008)[c] Loosely-connected (ISF, 2008)[c]
			Lateral Relationships				Lateral Relationships (Brenner, 2002)[b]
						Hierarchical structure	
	Growing relationships between organised crime and intruders who provide the technical expertise	Specialised hackers	Very specialised division of labour Specialised components Specialised skills			Specialisation	Specialised trades (MessageLabs®, 2009)[a] Buy in expertise (Winkler, 2005)[d]

Category	Williams[2] (2001/2002)	Europol High Tech Crime Centre[3] (2007)	Wall [1] (2008) *	Etges and Sutcliffe[4] (2008)	Symantec [5] (2008)	Finjan[6] (2008)	Additional items Identified from other sources
			Networks (ie non-hierarchical)				Networks (ie non-hierarchical) (Brenner, 2002) [b]
			Swarming **				Swarming (Brenner, 2002) [b]
	Growing network connections between hackers or small-time criminals and organised crime					Affiliation networks as distribution channels	
2. Organisational Goals		Money Motive	Profit-oriented				Exclusively profit-driven (Winkler, 2005) [d] Driven by economics (MessageLabs®, 2009) [a]
							To obtain valuable data (ISF, 2008) [c]
							Exploitation of the online market (ISF, 2008) [c]
3.			Depart from traditional thinking				

Category	Williams[2] (2001/2002)	Europol High Tech Crime Centre[3] (2007)	Wall [1] (2008) *	Etges and Sutcliffe[4] (2008)	Symantec [5] (2008)	Finjan[6] (2008)	Additional items Identified from other sources
Organisational Strategy/ Tactics			about organised crime				
					Rely on physical violence (Eastern Europe)		
		International Dimension	International	Transnational			
							Employ stealth (ISF, 2008) [c]
							Minimal hacking skills necessary (Winkler, 2005) [d]
3. Organisational Strategy/ Tactics	Growing relationship between organised crime and intruders who provide the technical expertise Growing network connections between hackers or small-time					Resemblance to terrestrial organised crime organisations (eg *Cosa Nostra*)	May have links with terrestrial organised crime groups (Winkler, 2005) [d]

Category	Williams[2] (2001/2002)	Europol High Tech Crime Centre[3] (2007)	Wall [1] (2008) *	Etges and Sutcliffe[4] (2008)	Symantec [5] (2008)	Finjan[6] (2008)	Additional items Identified from other sources
	criminals and organised crime						
							Not concerned with hiding existence of the group (Jakobsson and Ramzan, 2008) [e]
							May not be personally known to one another and communicate only through the Internet (SOCA, 2006/7) [f]
							Project-oriented (to commit a common act) (Jakobsson and Ramzan, 2008) [e]
3. Organisational Strategy/ Tactics			Skill and knowledge transfers (collaboration of skill sets)		Rely on expertise from other groups (US)		
			‘Slow drip’ tactics				
			Diverse attack vectors				
			Blended attack				

Category	Williams[2] (2001/2002)	Europol High Tech Crime Centre[3] (2007)	Wall [1] (2008) *	Etges and Sutcliffe[4] (2008)	Symantec [5] (2008)	Finjan[6] (2008)	Additional items Identified from other sources
			vectors				
			Strategic selection and use of information	Leverage information and communication technologies in the same manner as legitimate businesses			
							Employ automation (UK Cyber Security Strategy 2009) [g]
	High level of expertise and social engineering						Social engineering (UK Cyber Security Strategy, 2009) [g]
		Easily change tactics					
	Use Internet for communication and other purposes Exploit 'cyber' opportunities	Exploit the Internet as a working tool					May not be personally known to one another and communicate only through the Internet (SOCA, 2006/7) [f]

Category	Williams[2] (2001/2002)	Europol High Tech Crime Centre[3] (2007)	Wall [1] (2008) *	Etges and Sutcliffe[4] (2008)	Symantec [5] (2008)	Finjan[6] (2008)	Additional items Identified from other sources
3. Organisational Strategy/ Tactics					Some correlation between level of organisation and specific regions		
					Affiliation networks as distribution channels		
					Use crimeware toolkits		
				Leverage information and communication technologies in the same manner as legitimate businesses. Respond to the same driving forces.			Has all the attributes of a traditional economy (MessageLabs®, 2007) [a]
	Diversification into various forms of cyber-crime or Internet-related crime						

Category	Williams[2] (2001/2002)	Europol High Tech Crime Centre[3] (2007)	Wall [1] (2008) *	Etges and Sutcliffe[4] (2008)	Symantec [5] (2008)	Finjan[6] (2008)	Additional items Identified from other sources
4. Organisational Maturity			'transient, lateral and fluid forms' Ephemeral	Transitory relationships			
							Protection of 'cyberkingpins' (McAfee, 2009) [h]
		Very well-organised			More organised (Russia and Eastern Europe) Loosely-organised (North America)		Well-managed (ISF, 2008) [c] Increasingly organised and proficient (ISF, 2008) [c]
					Wide range in sophistication and capabilities		Sophisticated (MessageLabs®, 2007) [a] Professional and sophisticated (Jakobsson and Ramzan, 2008) [e]
			High level of expertise and social engineering				

Category	Williams[2] (2001/2002)	Europol High Tech Crime Centre[3] (2007)	Wall [1] (2008) *	Etges and Sutcliffe[4] (2008)	Symantec [5] (2008)	Finjan[6] (2008)	Additional items Identified from other sources
			New type of organisation New patterns of behaviour				
		Very clever at hiding money transfers					
5. Organisational Culture							
6. Organisational Environment							Web-based marketplace (Jakobsson and Ramzan, 2008) [e]
	Jurisdictional Arbitrage ***			Prosper greatly in non-regulated, lawless environments			
				Minimal trust			Fraud and rip-offs are common (MessageLabs®, 2007) [a]

***** As was also the case with Albanese, the characteristics which Wall highlights are taken from various sources. In the case of Brenner, he finds that her predictions were accurate.

** Swarming – Brenner (Page 42) mentions 'swarming' and attributes it to Arquilla and Ronfeldt ('*Swarming and the Future of Conflict*', 2000), who define it as: 'a deliberately structured, co-ordinated strategic way to strike from all directions … Today, the key form of organisation on the rise is the network … The new information technologies render an ability to connect and coordinate the actions of widely-distributed 'nodes' in almost unprecedented ways. Whoever masters this form will accrue advantages of a substantial nature.'

*** Jurisdictional arbitrage – Williams coins the term 'jurisdictional arbitrage' to refer to crimes which are initiated 'from jurisdictions that have few if any laws directed against cybercrime and/or little capacity to enforce laws against cybercrime.' (Page 3)

Main Sources

[1] D S Wall: Pages 39-44, '*Cybercrime'* ('Crime and Society Series', Polity) (2007)badinsky, ' Organised Crime' (3rd Edition) (Nelson Hall, Chicago, Illinois) (1990)

[2] P Williams, CERT®: '*Organised Crime and Cybercrime: Synergies, Trends and Responses*' (2001/2002)

[3] Europol High Tech Crime Centre Report: '*High Tech Crimes Within the EU: Old Crimes, New Tools. New Crimes, New Tools*' (2007)

[4] Y R Etges and E Sutcliffe: Pages 87-94, '*An Overview of Transnational Organised Cyber Crime*' ('Information Security Journal: A Global Perspective', 17) (2008)

[5] Symantec: Page 14, '*Symantec Report on the Underground Economy XII'* (November 2008):

http://www.symantec.com/en/uk/about/news/release/article.jsp?prid=20081124_11

[6] Finjan Q2 2008 Report: Pages 2, 8 and 9, '*Web Security Trends* Report' (Finjan Malicious Code Research Centre):

http://www.finjan.com/Content.aspx?id=827

Additional Items Identified from Other Sources

[a] MessageLabs®: White Paper: '*The Online Shadow Economy: A Billion Dollar Market for Malware Authors*' (2007):

http://www.legis.state.ia.us/lsadocs/IntComHand/2009/IHEGC012.PDF

[b] Susan W Brenner, '*Organised Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships*' (North Carolina Journal of Law and Technology, Volume 4, No. 1, 2002) (Quoted in Wall, '*Cybercrime*', above)

---

[c] Internet Security Forum (ISF): Pages 1-3, '*Profit-Driven Attacks*' (2008)

[d] I Winkler: '*Spies Among Us – How To Stop The Spies, Terrorists, Hackers And Criminals You Don't Even Know You Encounter Every Day*' (Wiley Publishing Inc) (2005)

[e] M Jakobssson and Z Ramzan: '*Crimeware – Understanding New Attacks and Defenses*' (Addison Wesley) (2008)

[f] Serious Organised Crime Agency (SOCA): Page 14, *SOCA Annual Report 2006/7*:

http://www.soca.gov.uk/assessPublications/downloads/SOCAAnnualRep2006_7.pdf

[g] UK Cabinet Office: Page 13, '*Cyber Security Strategy 2009*' (June 2009):

http://www.cabinetoffice.gov.uk/reports/cyber_security.aspx

[h] McAfee: Pages 12-14, '*McAfee Virtual Criminology Report – Cybercrime versus Cyberlaw*' (2009):

http://resources.mcafee.com/content/NAMcAfeeCriminologyReport

Table 4

Range of Typical Terrestrial/ Technically-Oriented Characteristics of Organised Crime Groups, with Sources

Category	Item No	Terrestrial/ Technically-Oriented Organised Crime Group Characteristics *	Source (Terrestrial/ Technically-Oriented Organised Crime Group Characteristics)	*Technically-Oriented Organised Crime Group Characteristics* **	*Source (Technically-Oriented Organised Crime Group Characteristics)*
1. Organisational Structures	1	Structured Criminal Group	Maltz/ Europol (2008)/ UNTOC	*Many people*	*(MessageLabs®, 2008)*
	2	Collaboration ('three or more persons')	EU/Europol (2002)/ UNTOC	*Growing network connections between hackers or small-time criminals and organised crime/ Affiliation networks as distribution channels/ Growing relationship between organized crime and intruders who provide the technical expertise /May have links with terrestrial organised crime groups*	*(Williams, 2001-2002)/ Finjan (2008)/ Williams (2001/2002)/ Winkler (2005)*
	3	Fluid, changeable roles, membership and structure ('does not need to have formally-defined roles for its members, continuity of its membership or a developed structure')	Fiorentini and Peltzman/ UNTOC	*Transient, lateral and fluid forms/ Flexible/ Adaptable/ Decentralised, loose relationships/Decentralised/ Loosely-connected*	*Wall (2008)/ Williams (2001-2002)/Europol High Tech Crime Centre (2007)/ Etges and Sutcliffe (2008)/Brenner/ISF/ISF*
	4			*Lateral Relationships*	*Wall (2008)/Brenner*
	5	Hierarchical structure	Abadinsky/ Maltz/ Gillingsky/ Albanese/ Reuter/ MT	*Hierarchical Structure*	*Finjan*
	6	Vertically-integrated structure	Garoupa		

Category	Item No	Terrestrial/ Technically-Oriented Organised Crime Group Characteristics *	Source (Terrestrial/ Technically-Oriented Organised Crime Group Characteristics)	*Technically-Oriented Organised Crime Group Characteristics **	*Source (Technically-Oriented Organised Crime Group Characteristics)*
	7	Commercial/ business-like structure	EU/Europol (2002)/Albanese/		
	8	Specialised division of labour	EU/Europol (2002)/ Gilinsky/ Europol (2008)/ Albanese	*Very specialised division of labour, Specialised components, Specialised skills/ Growing relationships between organized crime and intruders who provide the technical expertise/ Specialised hackers/ Specialisation/ Specialised Trends/Buy in expertise/*	*Wall (2008)/Williams/Europol High Tech Crime Centre (2007)/ Finjan/ MessageLabs® / Winkler (2005)*
	9			*Networks (ie non-hierarchical)*	*Wall (2008)/ Brenner*
	10			*Swarming*	*Wall (2008)/ Brenner*
2. Organisational Goals	11	Formed for a planned purpose ('not randomly formed for the immediate commission of an offence')	UNTOC		
	12	Financial or other material goals ('financial or other material benefit')	EU/Europol (2002)/ Gillingsky/ Albanese/ UNTOC	*Profit-oriented/ Money Motive/ Exclusively profit-drive/ Driven by economics*	*Wall (2008)/Europol High Tech Crime Centre (2007)/ Winker (2005)/ MessageLabs® (2009)*
	13	Monopolistic	Abadinksy/ Gillinsky/Albanese/ Schelling		
	14			*To obtain valuable data*	*ISF (2008)*
	15			*Exploitation of the online market*	*ISF (2008)*
	16	Non-Ideological	Abadinsky/Albanese		
	17	Ideological or Non-Ideological	Maltz		
	18	Public demand for services	Albanese		
3. Organisational	19	Criminal intent ('with the aim of committing one or more	EU/Europol (2002)/ Gillingsky/ UNTOC		

Category	Item No	Terrestrial/ Technically-Oriented Organised Crime Group Characteristics *	Source (Terrestrial/ Technically-Oriented Organised Crime Group Characteristics)	*Technically-Oriented Organised Crime Group Characteristics **	*Source (Technically-Oriented Organised Crime Group Characteristics)*
Strategy/ Tactics		offences')			
	20	Involved in legitimate enterprises	Maltz/ Europol (2008)		
	21	Control (eg explicit rules and regulations, discipline)	Abadinsky/ Maltz/ EU/Europol (2002)		
	22	Operates internationally	EU/Europol (2002)/ Europol (2008)/ UNTOC	*International/ International Dimension/ Transnational*	*Wall (2008)/ Europol High Tech Crime Centre (2007)/ Etges and Sutcliffe (2008)*
	23	Multiple enterprises	Maltz/ Reuter	*Diversification into various forms of cyber-crime and Internet-related crime*	*Williams (2001-2002)*
	24	Includes both national and foreign members	CARPO (2006)		
	25	Restricted membership	Albanese		
	26	Violence	Abadinsky/ Maltz/ EU/Europol (2002)/ Europol (2008)/Albanese	*Rely on physical violence (Eastern Europe)*	*Symantec (2008)*
	27	Bribery	Maltz		
	28	Corruption	Maltz/ EU/ Europol (2002)/ Gilinskiy/ Europol (2008)/ Albanese/ Finckenauer		
	29	Direct or indirect methods ('direct or indirect')	UNTOC	*Affiliation networks as distribution channels*	*Symantec (2008)*
	30	Insulation	Royal Canadian Mounted Police		
	31			*Depart from traditional thinking about organised crime*	*Wall (2008)*
	32			*Employ stealth*	*ISF (2008)*

Category	Item No	Terrestrial/ Technically-Oriented Organised Crime Group Characteristics *	Source (Terrestrial/ Technically-Oriented Organised Crime Group Characteristics)	*Technically-Oriented Organised Crime Group Characteristics **	*Source (Technically-Oriented Organised Crime Group Characteristics)*
	33			*Minimal hacking necessary*	*Winkler (2005)*
	34			*Not concerned with hiding existence of the group*	*Jakobsson and Ramzan (2008)*
	35			*May not be personally known to one another and communicate only through the Internet*	*SOCA (2006/7)*
	36			*Project-oriented (to commit a common act)*	*Finjan/ Jakobsson and Ramzan (2008)*
	37			*Skill and knowledge transfers (collaboration of skill sets)/ Rely on expertise from other groups (US)*	*Wall (2008)/ Symantec (2008)*
	38			*'Slow drip' tactics*	*Wall (2008)*
	39			*Diverse attack vectors*	*Wall (2008)*
	40			*Blended attack vectors*	*Wall (2008)*
	41			*Strategic selection and use of information/ Leverage information and communication technologies in the same manner as legitimate businesses*	*Wall (2008)/ Etges and Sutcliffe (2008)*
	42			*Employ automation*	*UK Cyber Security Strategy (2009)*
	43			*Social engineering/ High level of expertise and social engineering*	*UK Cyber Security Strategy (2009)/ Wall (2008)*
	44			*Easily change tactics*	*Europol High Tech Crime Centre (2007)*
	45			*Use Internet for communication and other purposes, exploit 'cyber' opportunities/ May not be personally known to one*	*Williams (2001/2002)/ SOCA (2006/7)*

Category	Item No	Terrestrial/ Technically-Oriented Organised Crime Group Characteristics *	Source (Terrestrial/ Technically-Oriented Organised Crime Group Characteristics)	*Technically-Oriented Organised Crime Group Characteristics **	*Source (Technically-Oriented Organised Crime Group Characteristics)*
				another and communicate only through the Internet	
	46			*Some correlation between level of organisation and specific regions*	*Symantec (2008)*
	47			*Use crimeware toolkits*	*Symantec (2008)*
	48			*Frauds and rip-offs are common*	*MessageLabs® (2007)*
	49			*Leverage information and communication technologies in the same manner as legitimate businesses, Respond to the same driving forces*	*Etges and Sutcliffe (2008)*
4. Organisational Maturity	50	Continuity ('existing for a period of time')	Abadinksy/ Maltz/ EU/Europol (2002)/ Gillinsky/ Europol (2008)/ Albanese/ Reuter/ UNTOC		
	51			*Transient, lateral and fluid forms; ephemeral/ Transitory Relationships*	*Wall (2008)/ Etges and Sutcliffe (2008)*
	52	Insulation	Royal Canadian Mounted Police	*Protection of 'cyberkingpins'*	*McAfee (2009)*
	53			*Very well-organised/ More organised (Russia and Eastern Europe), Loosely-organised (North America)/ Increasingly organised and proficient*	*Wall (2008)/ Symantec (2008)/ ISF (2008)*
	54			*Wide range in sophistication and adaptabilities/ Sophisticated/ Professional and sophisticated*	*Symantec (2008)/ MessageLabs® (2007)/ Jakobsson and Ramzan (2008)*
	55			*High level of expertise and social engineering*	*Wall (2008)*
	56			*New type of organisation, New*	*Wall (2008)*

Category	Item No	Terrestrial/ Technically-Oriented Organised Crime Group Characteristics *	Source (Terrestrial/ Technically-Oriented Organised Crime Group Characteristics)	*Technically-Oriented Organised Crime Group Characteristics **	*Source (Technically-Oriented Organised Crime Group Characteristics)*
				patterns of behaviour	
	57			*Very clever at hiding money transfers*	*Europol High Tech Crime Centre (2007)*
5. Organisational Culture	58	Bonding Rituals	Maltz		
	59	Code of Secrecy	Albanese		
	60	Authority of Reputation	Finckenauer		
	61	Self-Identification	Finckenauer		
6. Organisational Environment	62	Monopolistic	Abadinksy/ Gilinskiy/ Albanese/ Schelling		
	63			*Minimal Trust/ Fraud and rip-offs are common*	*Etges and Sutcliffe (2008)/ MessageLabs® (2007)*
	64			*Web-based marketplace*	*Jakobsson and Ramzan (2008)*
	65			*Jurisdictional arbitrage/ Prosper greatly in non-regulated, lawless environments*	*Etges and Sutcliffe (2008)*

***** Many sources do not differentiate between terrestrial and technically-oriented organised crime groups, for instance in the case of the UNTOC criteria. Hence, the items in this column may apply to either group.

** These are characteristics which have been specifically highlighted by sources as applying to technically-oriented organised crime groups.

Due to the heterogeneity that applies to all types of organised crime groups, this table indicates theoretical characteristic tendencies and is not intended to be in any way definitive. Although items in either list could potentially apply in any situation, they have been highlighted by sources from the Information Security industry and elsewhere as having particular significance. Situations which may involve organised crime groups may be high risk and must be assessed on a case-by-case basis, where necessary with involvement from law enforcement.

Table 5

Summary Comparison of Typical Terrestrial/ Technically-Oriented Characteristics of Organised Crime Groups

Category	Item No	Terrestrial/ Technically-Oriented Organised Crime Group Characteristics *	***Technically-Oriented Organised Crime Group Characteristics*** **
1. Organisational Structures	1	Structured Criminal Group	*Many people*
	2	Collaboration ('three or more persons')	*Growing network connections between hackers or small-time criminals and organised crime/ Affiliation networks as distribution channels/ May have links with terrestrial organised crime groups*
	3	Fluid, changeable roles, membership and structure	*Transient, lateral and fluid forms/ Flexible/ Adaptable/ Decentralised/ Loosely-connected*
	4		*Lateral Relationships*
	5	Hierarchical structure	*Hierarchical Structure*
	6	Vertically-integrated structure	
	7	Commercial/ business-like structure	
	8	Specialised division of labour	*Very specialised division of labour, Specialised components, Specialised skills/ Buy in expertise*
	9		*Networks (ie non-hierarchical)*
	10		*Swarming*
2. Organisational Goals	11	Formed for a planned purpose ('not randomly formed for the immediate commission of an offence')	
	12	Financial or other material goals ('financial or other material benefit')	*Profit-oriented*
	13	Monopolistic	
	14		*To obtain valuable data*

Category	Item No	Terrestrial/ Technically-Oriented Organised Crime Group Characteristics *	*Technically-Oriented Organised Crime Group Characteristics* **
	15		*Exploitation of the online market*
	16	Non-Ideological	
	17	Ideological or Non-Ideological	
	18	Public demand for services	
3. Organisational Strategy/ Tactics	19	Criminal intent ('with the aim of committing one or more offences')	
	20	Involved in legitimate enterprises	
	21	Control (eg explicit rules and regulations, discipline)	
	22	Operates internationally	*Transnational*
	23	Multiple enterprises	*Diversification into various forms of cyber-crime and Internet-related crime*
	24	Includes both national and foreign members	
	25	Restricted membership	
	26	Violence	*Rely on physical violence (Eastern Europe)*
	27	Bribery	
	28	Corruption	
	29	Direct or indirect methods ('direct or indirect')	*Affiliation networks as distribution channels*
	30	Insulation	
	31		*Depart from traditional thinking about organised crime*
	32		*Employ stealth*
	33		*Minimal hacking necessary*

Category	Item No	Terrestrial/ Technically-Oriented Organised Crime Group Characteristics *	*Technically-Oriented Organised Crime Group Characteristics* **
	34		*Not concerned with hiding existence of the group*
	35		*May not be personally known to one another and communicate only through the Internet*
	36		*Project-oriented (to commit a common act)*
	37		*Skill and knowledge transfers (collaboration of skill sets)/ Rely on expertise from other groups (US)*
	38		*'Slow drip' tactics*
	39		*Diverse attack vectors*
	40		*Blended attack vectors*
	41		*Strategic selection and use of information/ Leverage information and communication technologies in the same manner as legitimate businesses*
	42		*Employ automation*
	43		*High level of expertise and social engineering*
	44		*Easily change tactics*
	45		*Use Internet for communication and other purposes, exploit 'cyber' opportunities/ May not be personally known to one another and communicate only through the Internet*
	46		*Some correlation between level of organisation and specific regions*
	47		*Use crimeware toolkits*
	48		*Frauds and rip-offs are common*
	49		*Leverage information and communication technologies in the same manner as legitimate businesses, Respond to the same driving forces*
4. Organisational	50	Continuity ('existing for a period of time')	
	51		*Transient, lateral and fluid forms; ephemeral/ Transitory*

Category	Item No	Terrestrial/ Technically-Oriented Organised Crime Group Characteristics *	***Technically-Oriented Organised Crime Group Characteristics*** **
Maturity			*Relationships*
	52	Insulation	*Protection of 'cyberkingpins'*
	53	`	*More organised (Russia and Eastern Europe), Loosely-organised (North America)/ Increasingly organised and proficient*
	54		*Sophisticated/ Professional and sophisticated*
	55		*High level of expertise and social engineering*
	56		*New type of organisation, New patterns of behaviour*
	57		*Very clever at hiding money transfers*
5. Organisational Culture	58	Bonding Rituals	
	59	Code of Secrecy	
	60	Authority of Reputation	
	61	Self-Identification	
6. Organisational Environment	62	Monopolistic	
	63		*Minimal Trust/ Fraud and rip-offs are common*
	64		*Web-based marketplace*
	65		*Jurisdictional arbitrage/ Prosper greatly in non-regulated, lawless environments*

***** Many sources do not differentiate between terrestrial and technically-oriented organised crime groups, for instance in the case of the UNTOC criteria. Hence, the items in this column may apply to either group.

Due to the heterogeneity that applies to all types of organised crime groups, this table indicates theoretical characteristic tendencies and is not intended to be in any way definitive. Although items in either list could potentially apply in any situation, they have been

highlighted by sources from within the Information Security industry and elsewhere as having particular significance. Situations which may involve organised crime groups may be high risk and must be assessed on a case-by-case basis, where necessary with involvement from law enforcement.

Table 6

Summary Comparison of Real-life v Theoretical Online Organised Crime Group Characteristics

Category	Item No	Theoretical Terrestrial/ Technically-Oriented Organised Crime Group Characteristics [1]	Real Life Organised Crime Group Case Study Examples Which Display The Theoretical Characteristic
1. Organisational Structures	1	Structured Criminal Group	*All cases*
	2	Collaboration ('three or more persons')/ *Affiliation networks/ May have links with terrestrial organised crime groups*	Collaboration - *All cases* Affiliation networks – *Banco di Sicilia Incident/ ShadowCrew/ Sumitomo Bank Incident Group/ The RBN/ CardersMarket/ Triad Gang (Australia)/ Heartland Payment Systems et al Group* May have links with terrestrial organised crime groups - *Banco di Sicilia Incident/ ShadowCrew/ Sumitomo Bank Incident Group/ McColo/ Triad Gang (Australia)*
	3	Fluid, changeable roles, membership and structure/ *Transient*, *decentralised*	*Operation IceTrap/ The HangUp Team/ Sumitomo Bank Incident Group/ The RBN/ CardersMarket/ Heartland Payment Systems et al Group*
	4	*Lateral Relationships*	*The HangUp Team/ T J Maxx/ Sumitomo Bank Incident Group/McColo/ The RBN/ Heartland Payment Systems et al Group*
	5	Hierarchical structure	*Operation IceTrap/Banco di Sicilia/ShadowCrew/CardersMarket/ Triad Gang (Australia)/ CardersMarket*
	6	Vertically-integrated structure	*Operation IceTrap/ShadowCrew/ Triad Gang (Australia)/ CardersMarket*
	7	Commercial/ business-like structure	*The HangUp Team/ShadowCrew/ McColo/ The RBN/ Rock Phish/ CardersMarket*

Category	Item No	Theoretical Terrestrial/ Technically-Oriented Organised Crime Group Characteristics [1]	Real Life Organised Crime Group Case Study Examples Which Display The Theoretical Characteristic
	8	Specialised division of labour/ *Specialised skills/ Buy in expertise/*	*Operation IceTrap/Banco di Sicilia Incident/ ShadowCrew/ Sumitomo Bank Incident Group/ The RBN/ Rock Phish/ CardersMarke/ Triad Gang (Australia)/ Heartland Payment Systems et al Group*
	9	*Networks (ie non-hierarchical)*	*The HangUp Team/ T J Maxx Incident Group/The RBN/ Heartland Payment Systems et al Group*
	10	*Swarming*	*The HangUp Team/ McColo/ The RBN/Rock Phish/ CardersMarket/ Triad Gang (Australia)/Heartland Payment Systems et al Group*
2. Organisational Goals	11	Formed for a planned purpose ('not randomly formed for the immediate commission of an offence')	*All cases*
	12	Financial or other material goals ('financial or other material benefit')	*All cases*
	13	Monopolistic	*Banco di Sicilia Incident/ McColo/ The RBN/ Rock Phish/ CardersMarket*
	14	*To obtain valuable data*	*All cases*
	15	*Exploitation of the online market*	*The HangUp Team/ Banco di Sicilia Incident/ T J Maxx Incident/ ShadowCrew/Sumitomo Bank Incident Group/ McColo/ The RBN/ Rock Phish/ CardersMarket/ Triad Gang (Australia)/ Heartland Payment Systems et al Group*
	16	Non-Ideological [2]	*All cases except The HangUp Team*

Category	Item No	Theoretical Terrestrial/ Technically-Oriented Organised Crime Group Characteristics [1]	Real Life Organised Crime Group Case Study Examples Which Display The Theoretical Characteristic
	17	Ideological or Non-Ideological [3]	*No evidence cited*
	18	Public demand for services	*The HangUp Team/ ShadowCrew/ McColo/ The Russian Business Network/ Rock Phish/ CardersMarket*
3. Organisational Strategy/ Tactics	19	Criminal intent ('with the aim of committing one or more offences')	*All case studies*
	20	Involved in legitimate enterprises [4]	*Operation IceTrap/Sumitomo Bank Incident Group/ McColo*
	21	Control (eg explicit rules and regulations, discipline)	*ShadowCrew/CardsMarket*
	22	Operates internationally/ *Transnational*	*All cases*
	23	Multiple enterprises/ *Diversification into various forms of cyber-crime and Internet-related crime*	*All cases*
	24	Includes both national and foreign members [5]	*Operation IceTrap/ The HangUp Team/ T J Maxx Group/ ShadowCrew/ Sumitomo Bank Incident Group/ The RBN/ CardersMarket/ Triad Gang (Australia)/ Heartland Payment Systems et al*
	25	Restricted membership [6]	*Operation IceTrap/ Banco di Sicilia Incident/ T J Maxx Incident Group/ Sumitomo Bank Incident Group/ Rock Phish/ DarkMarket/ Heartland Payment Systems et al*
	26	Violence/ *Rely on physical violence (Eastern Europe)* [7]	*No evidence cited*
	27	Bribery	*No evidence cited*

Category	Item No	Theoretical Terrestrial/ Technically-Oriented Organised Crime Group Characteristics [1]	Real Life Organised Crime Group Case Study Examples Which Display The Theoretical Characteristic
	28	Corruption	*Banco di Sicilia Incident/ Triad Gang (Australia)*
	29	Direct or indirect methods ('direct or indirect')/ *Affiliation networks as distribution channels*	*All cases*
	30	Insulation [8]	*Triad Gang (Australia)*
	31	*Depart from traditional thinking about organised crime*	*All cases*
	32	*Employ stealth* [9]	*All cases*
	33	*Minimal hacking necessary*	*Banco di Sicila Incident/ McColo/The RBN/ Rock Phish/CardersMarket*
	34	*Not concerned with hiding existence of the group*	*The HangUp Team/ ShadowCrew/McColo*
	35	*May not be personally known to one another and communicate only through the Internet* [10]	*All cases*
	36	*Project-oriented (to commit a common act)*	*Operation IceTrap/ Banco di Sicilia Incident/ T J Maxx Incident Group/ Sumitomo Bank Incident Group/ Triad Gang (Australia)/ Heartland Payment Systems et al Group*
	37	*Skill and knowledge transfers (collaboration of skill sets)/ Rely on expertise from other groups (US)*	*All cases except T J Maxx Incident Group/ McColo and Rock Phish*
	38	*'Slow drip' tactics* [11]	*No evidence cited*
	39	*Diverse attack vectors*	*All cases except Banco di Sicilia Incident/ T J Maxx Incident Group and Sumitomo Bank Incident Group and Triad Gang (Australia)*

Category	Item No	Theoretical Terrestrial/ Technically-Oriented Organised Crime Group Characteristics [1]	Real Life Organised Crime Group Case Study Examples Which Display The Theoretical Characteristic
	40	*Blended attack vectors*	*All cases*
	41	*Strategic selection and use of information/ Leverage information and communication technologies in the same manner as legitimate businesses*	*Operation IceTrap/ The HangUp Team/ ShadowCrew/ Sumitomo Bank Incident Group/ McColo/ The RBN/ Rock Phish/ CardersMarket/ Triad Gang (Australia/ Heartland Payment Systems et al Group)*
	42	*Employ automation* [12]	*All cases*
	43	*High level of expertise and social engineering* [13]	*High Level of expertise - All cases except Sumitomo Bank Incident Group and Triad Gang (Australia)* *Social Engineering – The HangUp Team/ ShadowCrew/ McColo/ The RBN/ Rock Phish/ CardersMarket/ Triad Gang (Australia)*
	44	*Easily change tactics*	*The HangUp Team/ ShadowCrew/ The RBN/ Rock Phish/ CardersMarket*
	45	*Use Internet for communication and other purposes, exploit 'cyber' opportunities* *May not be personally known to one another and communicate only through the Internet* [14]	*All cases*
	46	*Some correlation between level of organisation and specific regions*	*Operation IceTrap/ The HangUp Team/ Banco di Sicilia Incident/ McColo/ The RBN/Rock Phish/ Triad Gang (Australia)*
	47	*Use crimeware toolkits*	*The HangUp Team/ ShadowCrew/ McColo/ The RBN/ Rock Phish/ CardersMarket*
	48	*Frauds and rip-offs are common* [15]	*ShadowCrew/ CardersMarket/ Triad Gang (Australia)*

Category	Item No	Theoretical Terrestrial/ Technically-Oriented Organised Crime Group Characteristics [1]	Real Life Organised Crime Group Case Study Examples Which Display The Theoretical Characteristic
	49	*Leverage information and communication technologies in the same manner as legitimate businesses, Respond to the same driving forces*	*Operation IceTrap/ The HangUp Team/ ShadowCrew/ Sumitomo Bank Incident Group/ McColo/ The RBN/ Rock Phish/ CardersMarket/ Triad Gang (Australia)/ Heartland Payment Systems et al Group)*
4. Organisational Maturity	50	Continuity ('existing for a period of time') [16]	*All cases*
	51	*Transient, lateral and fluid forms; ephemeral/ Transitory Relationships* [17]	*No evidence cited*
	52	Insulation/ *Protection of 'cyberkingpins'*	*Triad Gang (Australia)*
	53	*More organised (Russia and Eastern Europe), Loosely-organised (North America)/ Increasingly organised and proficient* [18]	*More organised (Russia and Eastern Europe) - No evidence cited* *Loosely-organised (North America) – No evidence cited* *Increasingly organised and proficient – All cases*
	54	*Sophisticated/ Professional and sophisticated*	*All cases*
	55	*High level of expertise and social engineering* [19]	*High Level of expertise - All cases except Sumitomo Bank Incident Group and Triad Gang (Australia)* *Social Engineering – The HangUp Team/ ShadowCrew/ McColo/ The RBN/ Rock Phish/ CardersMarket/ Triad Gang (Australia)*
	56	*New type of organisation, New patterns of behaviour*	*All cases*
	57	*Very clever at hiding money transfers*	*Operation IceTrap/ Banco di Sicilia Incident/ T J Maxx Incident Group/ Sumitomo Bank Incident Group/ Triad Gang (Australia)/*

Category	Item No	Theoretical Terrestrial/ Technically-Oriented Organised Crime Group Characteristics [1]	Real Life Organised Crime Group Case Study Examples Which Display The Theoretical Characteristic
			Heartland Payment Systems et al Group
5. Organisational Culture	58	Bonding Rituals	*No evidence cited*
	59	Code of Secrecy	*No evidence cited*
	60	Authority of Reputation [20]	*Banco di Sicilia Incident*
	61	Self-Identification	*The HangUp Team/ CardersMarket*
6. Organisational Environment	62	Monopolistic [21]	*Banco di Sicilia Incident/ McColo/ The RBN/ Rock Phish/ CardersMarket No evidence cited*
	63	*Minimal Trust/ Fraud and rip-offs are common* [22]	*ShadowCrew/ CardersMarket/ Triad Gang (Australia)*
	64	*Web-based marketplace*	*The HangUp Team/ ShadowCrew/ McColo/The RBN/ Rock Phish/ CardersMarket*
	65	*Jurisdictional arbitrage/ Prosper greatly in non-regulated, lawless environments*	*The HangUp Team/ Banco di Sicilia Incident/ ShadowCrew/ Sumitomo Bank Incident Group/The RBN/ Rock Phish/ Heartland Payment Systems et al Group*

All Cases = The item applies to all 12 examples in the case studies

[1] Many sources do not differentiate between terrestrial and technically-oriented organised crime groups, for instance in the case of the UNTOC criteria. In this column, items which may apply to either category are shown in plain text, with items identified as characteristic of online organised crime groups shown in italics.

Due to the heterogeneity that applies to all types of organised crime groups, this table indicates theoretical characteristic tendencies and is not intended to be definitive. Although items in either list could potentially apply in any situation, they have been highlighted by sources from within the Information Security industry and elsewhere as having particular significance. Situations which may involve organised crime groups may be high risk and must be assessed on a case-by-case basis, where necessary with involvement from law enforcement.

[2] Non-Ideological – Although several of the groups do display ideological tendencies, at least to the extent that they will often identify with each other as criminal entities who work outside the social norms, only *The HangUp Team* was cited as expressing any explicit ideology (the motto on their website is 'In fraud we trust') within the source material. As with many items in these tables, there may be benefit in targeting research towards this aspect of online organised crime groups.

[3] Ideological or Non-Ideological - Once again, there was no specific evidence to indicate this characteristic in the cited sources.

[4] As 'Involved' is a broad term, within this specific context, this item represents the utilisation of legitimate businesses for criminal ends, either through direct physical infiltration of a legitimate business or through incorporating a legitimate business concern within the criminal business model, for instance as a respectable 'front' to money-launder criminal takings. However, it does not include indirect methods of infiltration such as exploitation of a legitimate business's digital assets (for instance, compromising legitimate businesses' websites for phishing purposes).

As an example, in the case of the *McColo Corporation*, although the company presented itself as a legitimate concern, its activities suggested otherwise. Hence, the organisation was a 'front' for the criminal activities.

[5] Although the Banco di Sicilia group intended to transfer the money abroad, the sources do not state that this was an international organised crime group.

[6] Restricted membership – This is an interesting characteristic within an online organised crime group context, in that some criminal concerns, such some online forums, will be open to both legitimate and criminal individuals, whereas others will restrict their membership to offenders, for instance for the purpose of committing specific crimes. In this context, this item is taken to mean groups which specifically restrict their membership, for whatever reason.

[7] Violence – Here, the term refers to physical violence. However, it could also be employed within a digital context, as demonstrated by D Wall in '*The Internet as a Conduit for Criminal Activity*', where *Table 4.1* is a matrix of cybercrimes which maps

terrestrial crimes against proposed online equivalents. For instance, online violence includes 'cyber-stalking' and 'cyber-harassment', as well as targeted hate speeches and child abuse. (D Wall: Pages 77-98, '*The Internet as a Conduit for Criminal Activity'*, Information Technology and the Criminal Justice System, A Pattavina (Ed), Sage Publications, Inc, 2007)

The anonymity of the Internet can also create risks for users answering Web adverts. In a recent incident which is not unique, *The Guardian* reported that a man had been physically assaulted after responding to a classified online second-hand car advert, demonstrating how distinctions between terrestrial and online crime can be blurred:

Guardian.co.uk: '*Man Stabbed after Answering Fake Car Advert*' (August 2009)

http://www.guardian.co.uk/uk/2009/aug/26/man-stabbed-fake-car-advert

[8] Insulation – Any terrestrial criminal organisation that engages in money-laundering through a hierarchical structure of roles creates a distance between the group's leader and the 'footsoldiers'. In the case of Internet activity, the same effect can be achieved via various means, for instance by locating leaders in different countries to the rest of the team, separated by a network of 'mules' or other intermediaries. The leaders may have no overt association with the criminal activity at all.

[9] Stealth – Although *ShadowCrew*, for instance, made no effort to hide its activities, the activities themselves employed stealth, for instance through Trojan and phishing attacks.

[10] Not personally known to one another – This is one of the key differences between some terrestrial organised crime groups and their online equivalents. The Internet enables individuals from across the world to communicate with each other without ever having to meet and services such as Web 2.0 services (eg social networking) facilitate collaboration.

[11] 'Slow drip' tactics – Although none of the cited examples specifically describe the groups as using 'slow drip' tactics, many of the crimeware toolkits sold on the criminal forums, for instance, do have this capability.

[12] Employ automation – The term 'automation' has a wide scope. Most modern information technologies employ automation to differing degrees. Crimeware toolkits, for instance those which include worms, and botnets require automation in order to launch widescale attacks. For this reason, all the cases cited here are deemed to employ 'automation' because all used technologies which had automated aspects.

[13] High level of expertise - One major advantage of the modern crimeware toolkits and their components for offenders is that they are designed for ease of use. Consequently, offenders can 'mix and match' different technical attack vectors with little technical knowledge, including the deployment of the high-impact botnets. However, all the case studies cited here, except Sumitomo Bank Incident Group and Triad Gang (Australia), did require some advanced technical skills (for their time) in order to be successful.

Social engineering – As phishing requires social engineering, all the groups who incorporated phishing within their attack vectors were using social engineering.

[14] As has been discussed in the paper, use of the Internet is largely ubiquitous among modern businesses nowadays. All of the cases cited here specifically used the Internet to capture or transfer information, often in large amounts.

[15] Frauds and rip-offs are common - As used here, this item refers to activities such as double-dealing within the groups themselves. In the cases of *ShadowCrew* and *CardersMarket*, the forums were infiltrated by informers. In the Sumitomo Bank Incident Group incident, Hugh Rodley stole the identity of one of his fellow conspirators for credit and store card purchases. In the Triad Gang (Australia) incident, the naivety of the students who were paid to be 'mules' was exploited such that some were not paid a true reflection of the 'going rate' for their activities.

[16] Within the context of organised crime groups, 'continuity' can have more than one meaning. In this context, all the groups had some level of 'continuity' in that their activities were planned over a period of time.

In the sense of longevity, the term does not apply to the Banco di Sicilia Incident or the Sumitomo Bank Incident Group as, in both cases, although their crimes were strategically-planned and took some time to set in place, they were apprehended before the main events took place. Hence, it can only be speculation to consider whether, if they had been successful, the group would have continued to exist and to commit further crimes.

In all the other circumstances, the groups operated with a medium to long-term strategy and existed for a period of years.

[17] Due to the characteristics of the Internet, it is particularly difficult to distinguish transitory online organised crime activity as groups can form and disappear very quickly. It may be that the groups in the examples which were apprehended were caught, in part, because they were more visible than online organised crime groups with more fluid, temporary structures.

[18] More organised (Russia and Eastern Europe)/ Loosely-organised (North America) - These characteristics have been identified elsewhere (cf sources in ***Table 4***) but not by the sources used for the case studies.

'Increasingly organised and proficient' – All the cases cited demonstrate that organised crime groups are becoming more organised and proficient (at using information technologies and the Internet) than before.

[19] See reference 12 (for Item 43) above.

[20] Authority of reputation – This is a difficult item to gauge with regard to online organised crime groups unless there is direct documentary evidence. It is quite likely, however, that where an online organised crime group has associations with established terrestrial organised crime groups, the 'authority of reputation' of the terrestrial group will transfer by association to the online group.

[21] Monopolistic – This can also be difficult to gauge at the moment with regard to online organised crime groups. Until recently, the Internet, and the Web in particular, was perceived by offenders as a new and unexploited marketplace where they could largely operate with impunity, with little fear of challenge from law enforcement or their peers, hence why organisations such as *ShadowCrew* traded in the open. However, as profits have decreased due to the current recession and serious criminal elements have become more involved, the situation has changed so that, although there continues to be collaboration among some groups, there is also increased competition among others, with more aggressive tactics involved.

All the examples cited in the case studies were able to operate unchallenged in this open and lucrative environment. However, for the reasons above, together with an increase in offenders diversifying their skill sets and techniques to include exploitation of information technologies and increasing security awareness among businesses so that they introduce controls , the situation is likely to change in the future to a more competitive environment.

[22] See reference 15 (for Item 48) above.

Appendix B

Case Studies

Real-life examples of online organised crime group activity, arranged in chronological order.

Known characteristics from each of these examples have been mapped against those in ***Tables 5*** and ***6*** from **Appendix A**.

The case studies comprise a snapshot of each incident. Given the nature and complexity of some of the events, it is possible that additional information may exist in some cases which has not yet been released into the public domain.

CASE STUDY 1 – Operation IceTrap

(Pre-2000 [1])

Type/s of Activity Undertaken:

Online fraud; Network infiltration

In their paper about economic crime, Di Nicola and Scartezzini [2] outline Operation 'Ice Trap', an important early Italian case of international collaboration to solve online crime between law enforcement agencies, which also revealed a high level of organisation and co-operation between the members of the online organised crime group involved, who were dispersed across Italy, the rest of Europe and North America.

As well as capitalising on the lack of international financial regulations governing the Internet at that time, the offenders were able to quickly establish their international network using the latest technologies, structuring themselves with different roles beneath a single leader. They used the Italian public switched telephone network (PSTN) network (eg '*Itapac*') to both communicate and to infiltrate the Italian affiliate firms of *Unilever International*.

Once inside the systems, the group captured credit card pin numbers and passwords which were used to commit fraud via virtual transactions. Di Nicola and Scartezzini pointed out that this was an example of how easily criminal organisations could build international connections using newly-available technology and equipment, quoting one of the former hackers, now working in the Information Security industry, as stating 'Information is power'. [3]

CASE STUDY 2 – The HangUp Team

(Pre-2000 - Present)

Type/s of Activity Undertaken:

Fraud; Virus and Worm creation (eg the *Korgo* malicious code and its variations; the Berbew and *Webber* viruses; *Scob* Worm, all of which involve the theft of sensitive personal information [1]);

Spyware; Webserver infiltration; Renting out software for spam and phishing attacks

The *HangUp Team* has been in operation since before the year 2000 and were originally composed of 3 members from Russia. At that time, they were arrested in Russia for the distribution of malware, for which they received suspended sentences. However, they resurfaced in 2003, launching the *Webber* and *Berbew* viruses. The following year, they were responsible for an attack involving *Scob*, a worm which exploited an unknown vulnerability to insert malicious content onto webservers. The effect was that every webpage served to users was infected with the Trojan. [2] Once installed on the user's computer, the user's activities were monitored by spyware and password and credit card data was covertly transferred to a server in Russia. [3]

By 2005, the membership of the *HangUp Team* was believed to have grown to 4,000 worldwide [4]. Its concerns now include renting out networks of computers for spam and phishing activities and information exchange among peers. [5]

The group is brazen about its activities. The malicious code which it releases has a 'tag' in the signature, 'Coded by HangUp Team'. The group also has a motto, 'In fraud we trust', which is posted on the public website from which it operates. Given the openness of its actions, there is speculation as to why the main perpetrators, although known to the police since 2000, have not been intercepted, with the Russian police saying they are hampered by bureaucratic requirements and the difficulties of communicating with their US and UK equivalents. [6]

CASE STUDY 3 – Banco di Sicilia Incident (2000)

Type/s of Activity Undertaken:

Online Fraud; Corruption; Money-Laundering; Attempted theft; Network infiltration

This case was reported by *NetworkWorld* [1] and *Reuters* [2] in October 2000. A criminal-led organisation with links to *Cosa Nostra* planned to steal 2 trillion lire ($680 million) from Sicily's regional government through online bank fraud. The leader of the group was Antonio Orlando, a close associate of one of Palermo's leading Mafia families, who had previous convictions for fraud, money laundering and receiving stolen goods. The Director of the Palermo police mobile squad organised crime unit said at the time:

'The operation was certainly authorised by the Mafia, because here in Sicily any operation of economic importance requires the Mafia's permission…. The Mafia definitely has an interest in it.' [3]

The group worked with insiders of the *Banco di Sicilia* and technicians from the national carrier, *Telecom Italia SpA* (*sic)*, in order to 'clone' a copy of the bank's computer system. This was intended to be configured to connect to the Italian interbank transfer network outside normal office hours using captured computer files, codes and passwords, for the purpose of transferring funds to bank accounts in Bologna, Italy, then abroad. It was planned that the banking staff involved would switch off the bank's computer at a pre-arranged time to allow the 'clone' to take over its role.

Police stated that telephone interceptions had revealed that the group had also sought accomplices from the Vatican's *Institute for the Works of Religion* bank, with the intention of finding fellow conspirators who would help them conceal the stolen money where it could not be recovered by the Italian state.

CASE STUDY 4 – T J Maxx Incident Group

(2002-2007)

Type/s of Activity Undertaken:

Identity fraud; Credit card compromise; Other personal and commercial valuable data compromise (eg driver licence numbers); Online fraud; Network infiltration

In 2007, the *TJX* case (which incorporated *TJ Maxx* and *TK Maxx*) was termed the 'largest online burglary ever' by *Gartner*. At least 45.7 million credit and debit card holders across the world were exposed to potential identity fraud and other data compromises perpetrated by an international group, with a *TJX* spokeswoman admitting that 'the full extent of the damage might never be known because of the attackers' methods.'

In August 2008, 11 members of the group, from China, the Ukraine, Estonia and Belarus were charged with identity theft. They exploited vulnerabilities in an insecure wireless network by targeting 2 simple devices, a 'telescope-shaped antenna' and a laptop, via cars parked outside *TJX* commercial premises. The devices intercepted data transmitted from hand-held price-checking devices, cash registers and the store's computers and enabled the group to access *TJX*'s central database.

The incident generated adverse publicity for *TJX* and several class lawsuits were launched against them. In June 2008, *TJX* agreed to pay nearly $10m in an out-of-court settlement to 41 US States. This was in addition to millions of dollars already paid to customers and banks in compensation.

CASE STUDY 5 – ShadowCrew
(2002-2004)

Type/s of Activity Undertaken:
Online fraud; ID theft; Forgery; Website infiltration

The apprehension of some of the thousands of members of the *ShadowCrew* organisation as part of the 18-month international undercover operation, *Operation Firewall*,[1] was a watershed event which 'opened the eyes'[2] of the Information Security industry in October 2004. Members of *ShadowCrew* were identified from across the world, from the United States and Canada, to Bulgaria, Poland and Sweden, with 28 members in eight US States and 6 countries arrested in the first round. There were also 'indications' that former Eastern Bloc crime syndicates had links with the venture, possibly because they could employ jurisdictional arbitrage in these countries.[3]

ShadowCrew was a 'web-based marketplace for stolen identities', operating on an auction model similar to that of *eBay*,[4] where members could buy and sell their wares, as well as exchanging information. The site was hierarchically-organised under a clear leader, Andrew Mantovani, a business student, for whom it was important to be recognised as the 'spiritual leader' of the group.[5] The other main roles in the hierarchy were 'Administrators' (strategic organisers), 'Moderators' of online forums, 'Reviewers' and 'Vendors'.[6]

Unlike the activities of the *RBN*, which, in the main, were intended to be covert, *ShadowCrew* members, in part due to the sheer size of their operations, made little attempt to hide their activities.[7] The forum was open to public registration and viewable by anyone online,[8] with the peak hours of operation being between 10 pm to 2 am on Sunday nights, because many of the members held daytime jobs.[9]

At the time of the first apprehensions, law enforcement officials identified the details of 1.7 million stolen credit cards, login information for more than 18 million e-mail accounts, together with 'identity data for thousands of people including counterfeit British passports and Michigan drivers' licences' and a suspect list of over 2,000 names (although some of these names were likely to be aliases – see SOCA

comments below regarding *CardersMarket*). Over its two-year existence, the group had made more than $4.3m in illegal credit card purchases alone. [10]

One crucial factor which led to the arrest of some of the *ShadowCrew* participants and the shutdown of the website was the involvement of 'CumbaJohnny' (real name Albert Gonzalez), an informant for the US Secret Service, who engineered a relocation of some of *ShadowCrew*'s servers to a Virtual Private Network (VPN) in New Jersey that was being monitored by the Secret Service. [11]

Gonzalez was later apprehended in connection with other large-scale organised crime operations (see *Heartland Payment Systems et al* example below). The complexity of 'CumbaJohnny's' involvement in several different major online criminal activities illustrates the difficulties associated with mapping online organised crime group activity against a single crime type or incident.

CASE STUDY 6 – Sumitomo Bank Incident Group

(2004)

Type/s of Activity Undertaken:

Online fraud; Conspiracy to defraud; Conspiracy to transfer criminal property

In this incident, an international group including members from England, Belgium and France, conspired to obtain £229m ($423m) from the UK offices of Japan's *Sumitomo Masui* bank. [1] The group was fronted by ('Lord') Hugh Rodley, a 74-year-old UK ex-convict who, while enjoying an aristocratic lifestyle, was also liaising with members of the Adams crime family, whose considerable fortune had been amassed through drugs and extortion. Rodley's offences included the use of a fellow conspirator's identity for credit and store card purchases and he was apprehended as part of the investigation when one of his colleagues revealed details of the plot in a suicide letter. [2]

Hackers [3] were smuggled into the bank's premises by an internal accomplice who was a security supervisor. They used commercial keyloggers to capture login credentials covertly, with the intention of transferring the funds to 10 overseas accounts set up for the purpose in Spain, Dubai, Hong Kong and Singapore, via the banking SWIFT network. CCTV cameras were also tampered with in an attempt to hide their actions.

As with Example 1 (Online Mafia fraud), the offenders were apprehended by the police before the transfers were able to take place, following a two-year investigation which was triggered when staff were alerted to the repeated mistakes the offenders were making when completing application data fields in the SWIFT system.

The UK National Hi-Tech Crime Unit led the international investigation. They highlighted that the assistance from 'overseas forces' had varied enormously, mentioning that the Abu Dhabi accomplices had never been identified and singling out the co-operation of the bank and French and Belgian police as being particularly helpful.

CASE STUDY 7 – McColo

(2004 - 2008)

Type/s of Activity Undertaken:
Online fraud; Phishing; ID theft; Child pornography distribution

In November 2008, the website of '*McColo Corporation*' [1], a US web-based hosting firm, was disconnected from the Internet by its Internet Providers. *McColo* was alleged to have been hosting command and control centres for 5 major botnets, including *Storm*, [2] and is estimated to have been responsible for more than 75% of the world's spam. Alongside the *RBN*, with which it was said to be associated, it was known to have some of the most 'disreputable' organised crime groups in the world among its client list.

This case was notable for the role played by Brian Krebs, the author of '*Security Fix',* the established online security column in the '*Washington Post*'. He alerted '*McColo*'s' service providers, one of whom was able to begin disconnecting the services within a couple of hours of receiving Krebs' message, following their initial investigations. [3] This incident demonstrated how a collaborative approach may enable a service provider to take swift measures to effectively disable large-scale, distributed threats.

The disconnection of '*McColo*'s' services from the Internet resulted in an immediate 50 to 75 per cent reduction in the volume of worldwide spam. However, the reprieve was shortlived, with spam now making a resurgence [4] as other criminal enterprises fill the vacuum created by its downfall. The US continues to generate the most spam worldwide [5] and *Srizbi*, which was one of the larger botnets linked with *McColo*, was found to have joined a different botnet network, reportedly having activated instructions within its code to do so.

CASE STUDY 8 – Russian Business Network (RBN)

(2004 – 2008 or Present)

Type/s of Activity Undertaken:

Mass spamming; Phishing; ID theft; Software piracy; Web hosting for illegal services; Spyware; Fake security applications; Child pornography; Targeted DOS attacks; Renting of botnets

The *RBN*, known by numerous aliases including *RBNet* and *iFrame Cash* [1] and believed by some analysts to have strong links with the Russian government, provided so-called 'bullet proof' [2] web hosting services for rent which are said to be associated with 60% - 70% of the world's online crimes [3]. The services offered utilised techniques such as targeted DoS attacks, spamming, phishing and spyware (including fake anti-phishing and anti-spyware sites). The *RBN* operated through a network of covert, unregistered, hard-to-find domains in Russia, with suspected bases/servers in Panama, the UK and the Bahamas. [4] Lately, they have also been associated with activity in Iran. [5]

Speculation that the *RBN* might have ceased to exist in late 2007, when its domains suddenly disappeared from the Internet [6] (possibly due to the withdrawal of government support) were believed to be premature as sites in Taiwan and China were found to be hosting very similar malicious 'packing kits' ('development kits for malicious software') to those developed by the *RBN*, such as the popular '*MPack*'. However, soon afterwards, China cut the connections that were being established, with conjecture that the organisation would re-establish itself via smaller, more discreet groupings. [7] In February 2008, *The Shadowserver Foundation*, a volunteer Internet security monitoring organisation, published a report which connected the *RBN* with servers registered in Turkey [8] and, in August 2008, the *RBN* was being linked with the information warfare attacks on Georgia.

Although much of the current discussion about the RBN takes a cautious, retrospective stance, analysts are not ruling out the group from future high-impact activity.

CASE STUDY 9 – Rock Phish

(2004 - Present)

Type/s of Activity Undertaken:

Online fraud; Phishing; Spam; Botnet distribution

Rock Phish are an online organised crime group from the region of Romania or its vicinity [1] which produces 'phishing kits'. The name of the group is derived from their early custom of including 'strings such as "/rock" or "/r" ' in the directories of their phishing webpage URL (Uniform Resource Locator) addresses. [2]

In 2004, *Rock Phish* were the first group to incorporate botnets within their phishing infrastructure with the intent of extending the life of their attacks and to make them more scalable. [3]

In 2006, the group were believed to be responsible for over half the phishing e-mails in the world at that time. [4] They were estimated to have cost banks 'more than US$100m' [5] and to have compromised at least 44 different businesses in 9 countries, tending to target financial institutions such as *CitiBank*, *Barclays* and *Deutsche Bank*. [6]

By 2007, according to figures from Cambridge University researchers, the total amount stolen had risen to US$178m [7] and they were responsible for introducing so-called 'fast flux' techniques into phishing, which vastly increased the number of attacks against financial institutions which could take place at any one time [8] and the length of time the domain could exist.

In 2008, *Rock Phish* diversified their mass-phishing strategies to include the 'sophisticated' *Zeus* Trojan as a malware download in their attacks, [9] as reported by *RSA*, [10] in order to repeatedly capture personal information during inter-website transactions, as well as to spread financial crimeware.

By this time, *RSA* were reporting that the phishing attacks were now worth 'tens of millions of dollars'. [11] They also highlighted a crucial distinction between *Rock Phish* and many other online organised crime gangs, in that it is 'a closed gang operating in Russia', as opposed to participating 'in a broad economic system in which credit cards

are bought and sold openly.' [12] The group's organised self-sufficiency extends to writing their own code and launching its own attacks. In particular, a distinctive characteristic of the group was their ability to 'scale and execute thousands of phishing attacks with as little infrastructure as possible', which increased the difficulty of shutting down the websites. [13] Their strategies also included pooling 'hosted resources and …targeting many banks simultaneously,' co-operative attacks which were shown to be 'far more effective'. [14]

In August 2009. the *Zeus* Trojan, which had now evolved into a 'botnet', was linked with the servers of a company in Latvia called *Real Host*, which were reported to have captured 'around 3.6 million PCs' for use as 'zombies' in the botnet. However, analysts warned that it was not clear how much control the *Real Host* servers had because it was 'extremely difficult' to locate the centre of a botnet of that size. [15]

CASE STUDY 10 – CardersMarket (including DarkMarket)

(2005-2007)

Type/s of Activity Undertaken:
Online fraud; Phishing; ID theft

'Carding', in criminal parlance, involves any criminal activity which arises from the compromise of financial smartcards such as credit or debit cards.

CardersMarket was a web-based forum which came into existence in 2005 when 'Iceman' (aka Max Vision) merged the user accounts from four rival forums he had hacked into his own site. [1] The forums included *DarkMarket*, *TalkCash*, *ScandinavianCarding* and *TheVouched*, all of which exchanged stolen information, with a focus on credit card data. [2]

As in the case of 'CumbaJohnny', 'Iceman', after becoming an informant following his arrest for hacking attacks on US government agencies in 1998, continued to operate his illegal forums using a range of aliases and separating his administrator duties from his illegal activities. [3]

In 2008, it was revealed that *DarkMarket*, one of the forums acquired by 'Iceman', had been an FBI undercover operation since 2006, news which received widespread media attention. [4] Unlike *ShadowCrew* and other similar sites, *DarkMarket* operated on an 'entrepreneurial, peer-reviewed' [5] invitation-only basis and it was through such an invitation that the FBI had been able to infiltrate the group. Products available on the site included stolen personal data for ID theft ('full infos'), credit card strip data ('dumps') to create counterfeit cards, specialised hardware and electronic banking logins for phishing attacks, with vendors encouraged to submit their goods for peer review before sale. [6] The website was shut down in 2006, following an international operation which included the FBI and SOCA, with over 60 arrests being made worldwide. [7]

One of the arrested administrators, 'Cha0' (*sic*), from Turkey, who was alleged to have also been involved in kidnapping, had sold high-quality ATM-skimming hardware which could be attached to cash machines to obtain credit card and PIN details.

The site had been well-regarded in the criminal community for identifying 'rippers' (individuals who steal from their peers) among the group, although 'Iceman' had issued warnings that the FBI were involved and that 'Master Splynter', the main site operator, was working for them. [8] Although this was the case, the message was dismissed as inter-forum rivalry. [9] In a farewell message to the group, 'Master Splynter' wrote:

'It is very unfortunate that we have come to this situation because … we have established DM as the premier English speaking forum for conducting business…' [10]

Following the arrest of one of the UK suspects, SOCA stated that, although it was known that there were 2,000 registered 'nicks' (nicknames) on the site, they could not be assumed to be unique: 'Some will be defunct. In other cases one user will have several different identities on the site.' [11]

CASE STUDY 11 – Triad Gang (Australia)

(2006)

Type/s of Activity Undertaken:

Online fraud; ID theft; Money laundering; Phishing; Corruption

This international fraud group, who operated out of Sydney's Chinatown and who had links with Malaysia and Russia, used school-age children in Sydney as 'mules' to launder money stolen from bank accounts through phishing and hacking attacks [1] via a keylogging Trojan installation installed when users accessed a link to a fake e-mail alert. [2] In return for a commission, reported to be between $200-$500 per day for moving up to $100,000 per day, [3] the money was transferred to the teenagers' personal bank accounts, prior to passing the funds on to 'bagmen' (couriers) for the group, who wired them to the group leaders overseas. [4] The teenagers withdrew 'small amounts of less than $10,000 from different bank branches', in order to evade detection. [5]

One 'bagman', Jonathan Carnie Mullally, from a prestigious private school, was described as a 'Fagin-like character' whose role was to be a go-between, taking money from the student 'mules' to pass on to a Malaysian gang boss. [6] Although the schoolchildren received sums which would have appeared substantial to them, they were not being paid the 'going rate' as the group were exploiting their naivety. [7]

Sixty victims were robbed of more than $600,000 Australian through this scam and some of the school children received jail terms of up to 18 months. [8]

CASE STUDY 12 – Heartland Payment Systems et al Group

(2006-2008)

Type/s of Activity Undertaken:

Online fraud; Online identify theft; Theft from ATM machines; Network infiltration; Conspiracy

At the same time that he was assisting the Secret Service in the *ShadowCrew* case, 'CumbaJohnny' used different online pseudonyms [1] to continue working with another international criminal group who were targeting US retail chain stores and financial institutions, including *Heartland Payment Systems* [2] and *7-Eleven Inc.* [3] This was in addition to his involvement in the *TJX* incident outlined above. [4]

This highly-organised group, which included members from Russia, China, the Ukraine, the United States, Estonia and Belarus, was probably created with the intention to capitalise on the 'specialised services and supplies' which the members provided, [5] being skilled in the capture of credit card details and other sensitive data for fraud-related purposes. The group used strategic tactics such as reviewing the Fortune 500 companies list to identify potential targets, which they then visited to monitor their online payment systems. [6]

The group launched SQL injection attacks, which 'probably' used specially-configured codes, which exploited vulnerabilities in firewall configurations [7], against businesses from their bases in poorly-regulated countries such as Latvia and the Ukraine, where they stored the data they had captured. For instance, one of the members, based in Estonia, infiltrated the servers of a Dallas-based restaurant chain to obtain data. [8]

At the enterprise level, the group compromised poorly-configured wireless networks and installed 'sniffer' programs [9] to intercept and capture network data that was transferred from the Latvia and Ukrainian servers to China, where it was imprinted on blank ATM cards. After processing, the cards were shipped back to North America for use in cash machines. [10]

This incident was quoted as having compromised 130 million credit card numbers [11], which led to the case being dubbed 'the biggest case of identity theft in American history. At the time of his arrest, authorities were aware that 'CumbaJohnny' had $1.6m

in his bank accounts, as well as other valuable assets. [12] He is scheduled to go on trial in 2010. [13]

Appendix B

Case Study References

Case Study 1

[1] Exact date unspecified.

[2] A Di Nicola and A Scartezzini: '*When Economic Crime Becomes Organised: the Role of Information Technologies. A Case Study*' ('Current Issues in Criminal Justice – Journal of the Institute of Criminology, University of Sydney, Faculty of Law, Vol 11, no 3) (March 2000):

http://eprints.biblio.unitn.it/archive/00000188/01/Economic_crime.pdf

[3] A Di Nicola and A Scartezzini: Ibid, Page 2

Case Study 2

[1] Symantec Research Report: Pages 12 and 29, '*An Overview of the Russian Hacking Scene*': (July 2007)

http://www.emea.symantec.com/onlinefraud/viewPDF.cfm?pdfname=An_Overview_of_the_Russian_Hacking_Scene.pdf

[2] Symantec Research Report: Page 12, '*An Overview of the Russian Hacking Scene*': (July 2007)

http://www.emea.symantec.com/onlinefraud/viewPDF.cfm?pdfname=An_Overview_of_the_Russian_Hacking_Scene.pdf

[3] BusinessWeek.com: Page 3 of online version of article, '*Hacker Hunters – An Elite Force Takes on the Dark Side of Computing*' (May 2005):

http://www.businessweek.com/magazine/content/05_22/b3935001_mz001.htm

[4] News.zdnet.co.uk: '*Criminals send malware levels soaring*' (July 2005)

http://news.zdnet.co.uk/security/0,1000000189,39207187,00.htm

[5] BusinessWeek.com: Page 3 of online version of article, '*Hacker Hunters – An Elite Force Takes on the Dark Side of Computing*' (May 2005):

http://www.businessweek.com/magazine/content/05_22/b3935001_mz001.htm

[6] BusinessWeek.com: Page 3 of online version of article, '*Hacker Hunters – An Elite Force Takes on the Dark Side of Computing*' (May 2005):

http://www.businessweek.com/magazine/content/05_22/b3935001_mz001.htm

---

Case Study 3

All items in this summary from:

[1,3] NetworkWorld.com: '*Mafia Caught Attempting Online Bank Fraud*' (October 2000)

http://www.networkworld.com/news/2000/1004mafia.html

[2] CNN.com.Europe – '*Italian police bust online Mafia fraud*': (October 2000)

http://edition.cnn.com/2000/WORLD/briefs/10/04/europe/#3

Case Study 4

All items in this summary from:

ComputerWeekly.com: '*TJX security breach tied to Wi-Fi exploits*': (May 2007)

http://www.computerweekly.com/Articles/2007/05/08/223672/tjx-security-breach-tied-to-wi-fi-exploits.htm

ComputerWeekly.com: '*TJX pays US States $9.75m for data breach*': (June 2009)

http://www.computerweekly.com/Articles/ArticlePage.aspx?ArticleID=236668&PrinterFriendly=true

---

Case Study 5

[1] The 2008 '*Symantec Report on the Underground Economy* XII', Page 9:
http://www.symantec.com/en/uk/about/news/release/article.jsp?prid=20081124_11

[2] Jakobsson and Z Ramzan: Page 356, '*Crimeware– Understanding New Attacks and Defences*' (Addison Wesley) (2008)

[3] The 2008 'Symantec Report on the Underground Economy XII, Page 9:
http://www.symantec.com/en/uk/about/news/release/article.jsp?prid=20081124_11

[4] Jakobsson and Z Ramzan: Page 356, '*Crimeware– Understanding New Attacks and Defences*' (Addison Wesley) (2008)

[5] BusinessWeek.com: Page 3 of online version of article, '*Hacker Hunters – An Elite Force Takes on the Dark Side of Computing*' (May 2005):
http://www.businessweek.com/magazine/content/05_22/b3935001_mz001.htm

[6] BusinessWeek.com: Page 3 of online version of article, '*Hacker Hunters – An Elite Force Takes on the Dark Side of Computing*' (May 2005):
http://www.businessweek.com/magazine/content/05_22/b3935001_mz001.htm

[7] The 2008 '*Symantec Report on the Underground Economy* XII', Page 10:
http://www.symantec.com/en/uk/about/news/release/article.jsp?prid=20081124_11

[8] The 2008 '*Symantec Report on the Underground Economy* XII', Page 9:
http://www.symantec.com/en/uk/about/news/release/article.jsp?prid=20081124_11

[9] BusinessWeek.com: Page 3 of online version of article, '*Hacker Hunters – An Elite Force Takes on the Dark Side of Computing*' (May 2005):
http://www.businessweek.com/magazine/content/05_22/b3935001_mz001.htm

[10] BusinessWeek.com: Page 3 of online version of article, '*Hacker Hunters – An Elite Force Takes on the Dark Side of Computing*' (May 2005):
http://www.businessweek.com/magazine/content/05_22/b3935001_mz001.htm

[11] The 2008 '*Symantec Report on the Underground Economy* XII', Page 9:
http://www.symantec.com/en/uk/about/news/release/article.jsp?prid=20081124_11

[12] The 2008 '*Symantec Report on the Underground Economy* XII', Page 9:
http://www.symantec.com/en/uk/about/news/release/article.jsp?prid=20081124_11

[13] The 2008 '*Symantec Report on the Underground Economy* XII', Page 10:
http://www.symantec.com/en/uk/about/news/release/article.jsp?prid=20081124_11

Case Study 6

[1] TheRegister.co.uk: '*How police busted UK's biggest cybercrime case*': (March 2009)
http://www.theregister.co.uk/2009/03/19/sumitomo_cyberheist_investigation/

[2] Timesonline.co.uk: '*Bogus Peer Hugh Rodley Tried to Pull Off World's Biggest Bank Raid*' (March 2009)
http://www.timesonline.co.uk/tol/news/uk/crime/article5848034.ece

[3] All subsequent items in this summary from 'TheRegister.co.uk':
'*How police busted UK's biggest cybercrime case*': (March 2009)
http://www.theregister.co.uk/2009/03/19/sumitomo_cyberheist_investigation/

Case Study 7

[1] Voices.washingtonpost.com, Security Fix: '*Major Source of Online Scams and Spams Knocked Offline*':

http://voices.washingtonpost.com/securityfix/2008/11/major_source_of_online_scams_a.html

[2] Sophos: Page 7, '*Security Threat Report: 2009*':

http://www.sophos.com/sophos/docs/eng/marketing_material/sophos-security-threat-report-jan-2009-na.pdf

[3] Voices.washingtonpost.com, Security Fix: '*Major Source of Online Scams and Spams Knocked Offline*':

http://voices.washingtonpost.com/securityfix/2008/11/major_source_of_online_scams_a.html

[4] Symantec *'State of Spam'* Report, April 2009:

http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_spam_report_04-2009.en-us.pdf

[5] Sophos: Page 8, '*Security Threat Report: 2009*':

http://www.sophos.com/sophos/docs/eng/marketing_material/sophos-security-threat-report-jan-2009-na.pdf

---

Case Study 8

[1] Webhosting.devshed.com, Web Hosting News: '*Russian Business Network: On the Fly*' (March 2008):

http://webhosting.devshed.com/c/a/Web-Hosting-News/Russian-Business-Network-On-the-Fly/

[2] TheRegister.co.uk: '*Infamous RBN quits China*': (November 2007)

http://www.theregister.co.uk/2007/11/13/rbn_quits_china/

[3] Webhosting.devshed.com, Web Hosting News: '*Russian Business Network: On the Fly*' (March 2008):

http://webhosting.devshed.com/c/a/Web-Hosting-News/Russian-Business-Network-On-the-Fly/

[4] Webhosting.devshed.com, Web Hosting News: '*Russian Business Network: On the Fly*' (March 2008):

http://webhosting.devshed.com/c/a/Web-Hosting-News/Russian-Business-Network-On-the-Fly/

[5] Securehomenetwork.blogspot.com: '*Russian Business Network Deploys in the IP Space of the Islamic Republic*' (March 2009):

http://securehomenetwork.blogspot.com/2009/03/russian-business-network-deploys-in-ip.html

[6] Cnet.com: '*Infamous Russian Malware Gang Vanishes*' (November 2007):

http://news.cnet.com/Infamous-Russian-malware-gang-vanishes/2100-7355_3-6217852.html

[7] TheRegister.co.uk: '*Infamous RBN quits China*': (November 2007)

http://www.theregister.co.uk/2007/11/13/rbn_quits_china/

[8] Shadowserver.org, Home Page of website:

http://www.shadowserver.org/wiki/

[9] The Shadowserver Foundation: '*RBN "Rizing" – Abdallah Internet Hizmetleri (AIH)*': (February 2008):

http://www.shadowserver.org/wiki/uploads/Information/RBN_Rizing.pdf

[10] TheRegister.co.uk: '*Russian cybercrooks turn on Georgia*': (August 2008)

http://www.theregister.co.uk/2008/08/11/georgia_ddos_attack_reloaded/print.html

---

Case Study 9

[1] PCPro.co.uk: '*Half of all phishes from Romanian cyber gang*': (December 2006)

http://www.pcpro.co.uk/news/100351/half-of-all-phishes-from-romanian-cyber-gang

[2] PCPro.co.uk: '*Half of all phishes from Romanian cyber gang*': (December 2006)

http://www.pcpro.co.uk/news/100351/half-of-all-phishes-from-romanian-cyber-gang

[3] Blogs.ZDNet.com: '*The Neospoilt Cybercrime Group Abandons Its Web Malware Exploitation Kit*' (entry dated April 21 2008)

http://blogs.zdnet.com/security/?p=1598

[4] PCPro.co.uk: '*Half of all phishes from Romanian cyber gang*': (December 2006)

http://www.pcpro.co.uk/news/100351/half-of-all-phishes-from-romanian-cyber-gang

PCPro were quoting Ken Dunham, Director of VeriSign's security research unit.

[5] InfoSecurity-magazine.com: '*One gang corners the market in phish*' (May 2007)

http://www.infosecurity-magazine.com/view/1152/one-gang-corners-the-maerket-in-phish

[6] PCPro.co.uk: '*Half of all phishes from Romanian cyber gang*': (December 2006)

http://www.pcpro.co.uk/news/100351/half-of-all-phishes-from-romanian-cyber-gang

[7] Infosecurity-magazine.com: '*One gang corners the market in phish*' (May 2007)

http://www.infosecurity-magazine.com/view/1152/one-gang-corners-the-market-in-phish

[8] University of Cambridge Computer Laboratory, Technical Report No. 718: Page 92, '*Cooperative Attack and Defence in Distributed Networks*' (June 2008)

http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-718.pdf

[9] SCMagazineus.com: '*"Rock Phish" gang adds malware download to attacks*' (April 2008)

http://www.scmagazineus.com/Rock-Phish-gang-adds-malware-download-to-attacks/article/109240/

[10] RSA.com: '*RSA, the Security Division of EMC, discovers "Rock Phish" attack evolution'* (April 2008)

http://www.rsa.com/press_release.aspx?id=9347

[11] SCMagazineus.com: '*"Rock Phish" gang adds malware download to attacks*': (April 2008)

http://www.scmagazineus.com/Rock-Phish-gang-adds-malware-download-to-attacks/article/109240/

[12] SCMagazineus.com: '*"Rock Phish" gang adds malware download to attacks*': (April 2008)

http://www.scmagazineus.com/Rock-Phish-gang-adds-malware-download-to-attacks/article/109240/

[13] SCMagazineus.com: '*"Rock Phish" gang adds malware download to attacks*': (April 2008)

http://www.scmagazineus.com/Rock-Phish-gang-adds-malware-download-to-attacks/article/109240/

[14] University of Cambridge Computer Laboratory, Technical Report No. 718: Page 4, '*Cooperative Attack and Defence in Distributed Networks*' (June 2008)

http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-718.pdf

[15] ComputerWeekly.com: '*Zeus Botnet Linked to Latvia's Real Host'* (August 2009)

http://www.computerweekly.com/Articles/2009/08/03/237146/zeus-botnet-linked-to-latvias-real-host.htm

For an in-depth technical analysis of the *Rock Phish* group's techniques, see:

University of Cambridge Computer Laboratory, Technical Report No. 718: Page 4, '*Cooperative Attack and Defence in Distributed Networks*' (June 2008)

http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-718.pdf

Case Study 10

[1] The 2008 *'Symantec Report on the Underground Economy* XII', Page 12:
http://www.symantec.com/en/uk/about/news/release/article.jsp?prid=20081124_11

[2] The 2008 *'Symantec Report on the Underground Economy* XII', Page 12:
http://www.symantec.com/en/uk/about/news/release/article.jsp?prid=20081124_11

[3] Wired.com: '*Notorious Crime Forum DarkMarket Goes Dark'*: (September 2008)
http://www.wired.com/threatlevel/2008/09/notorious-crime/

[4] Eg ZDNet.co.uk: '*FBI agent reveals details of cybercrime sting'* (May 2009)
http://news.zdnet.co.uk/security/0,1000000189,39649176,00.htm

[5] The 2008 *'Symantec Report on the Underground Economy* XII', Page 12:
http://www.symantec.com/en/uk/about/news/release/article.jsp?prid=20081124_11

[6] Wired.com: '*Notorious Crime Forum DarkMarket Goes Dark'*: (September 2008)
http://www.wired.com/threatlevel/2008/09/notorious-crime/

[7] The 2008 *'Symantec Report on the Underground Economy* XII', Page 12:
http://www.symantec.com/en/uk/about/news/release/article.jsp?prid=20081124_11

[8] ComputerWorlduk.com: '*Three Years Undercover with Cyber Criminals*':
(January 2009)
http://www.computerworlduk.com/management/security/cybercrime/in-depth/index.cfm?articleid=2016

[9] Wired.com: '*Notorious Crime Forum DarkMarket Goes Dark'*: (September 2008)
http://www.wired.com/threatlevel/2008/09/notorious-crime/

[10] Wired.com: '*Notorious Crime Forum DarkMarket Goes Dark'*: (September 2008)
http://www.wired.com/threatlevel/2008/09/notorious-crime/

[11] Wired.com: '*Notorious Crime Forum DarkMarket Goes Dark'*: (September 2008)
http://www.wired.com/threatlevel/2008/09/notorious-crime/

[12] BBC.co.uk: '*Police stalking cyber fraudsters*' (October 2008)
http://news.bbc.co.uk/1/hi/uk/7675216.stm

Case Study 11

[1] Sydney Morning Herald: '*Gone Phishing …gangs using Aussie kids to steal millions*' (June 2006)

http://www.smh.com.au/news/technology/gangs-using-aussie-kids-to-steal-millions/2006/06/03/1148956585189.html

[2] iDefense: Page 3, '*Money Mules: Sophisticated Global Cyber Criminal Operations*' (2006)

http://complianceandprivacy.com/WhitePapers/iDefense_MoneyMules_20060329.pdf

[3] The Register: '*Aussie Crooks Recruit Teen Phishing Mules*' (January 2005)

http://www.theregister.co.uk/2005/01/06/phisherman_fagins/print.html

(The Register was quoting a report from Australia's *Daily Telegraph* newspaper.)

[4] Sydney Morning Herald: '*Gone Phishing …gangs using Aussie kids to steal millions'* (June 2006)

http://www.smh.com.au/news/technology/gangs-using-aussie-kids-to-steal-millions/2006/06/03/1148956585189.html

[5] The Register: '*Aussie Crooks Recruit Teen Phishing Mules*' (January 2005)

http://www.theregister.co.uk/2005/01/06/phisherman_fagins/print.html

(The Register was quoting a report from Australia's *Daily Telegraph* newspaper.)

[6] Sydney Morning Herald: '*Gone Phishing …gangs using Aussie kids to steal millions'* (June 2006)

http://www.smh.com.au/news/technology/gangs-using-aussie-kids-to-steal-millions/2006/06/03/1148956585189.html

[7] The Register: '*Aussie Crooks Recruit Teen Phishing Mules*' (January 2005)

http://www.theregister.co.uk/2005/01/06/phisherman_fagins/print.html

(The Register was quoting a report from Australia's *Daily Telegraph* newspaper.)

[8] Sydney Morning Herald: '*Gone Phishing …gangs using Aussie kids to steal millions'* (June 2006)

http://www.smh.com.au/news/technology/gangs-using-aussie-kids-to-steal-millions/2006/06/03/1148956585189.html

---

Case Study 12

[1] NYTimes.com: '*Global Trail of an Online Crime Ring*': (August 2008)
http://www.nytimes.com/2008/08/12/technology/12theft.html

[2] For in-depth, updated reports on the *Heartland Payment Systems* aspect, see:

BankInfoSecurity.com: '*The Latest Updates on the Year's First Major Information Security Incident*':

http://www.bankinfosecurity.com/heartland_breach.php

At 24 August 2009, the site was reporting that more than 650 institutions had been affected by this breach alone.

[3] NYTimes.com: '*3 Indicted in Theft of 130 Million Card Numbers*' (August 2009)
http://www.nytimes.com/2009/08/18/technology/18card.html

[4] NYTimes.com: '*3 Indicted in Theft of 130 Million Card Numbers*' (August 2009)
http://www.nytimes.com/2009/08/18/technology/18card.html

[5] The 2008 *'Symantec Report on the Underground Economy* XII', Page 11:
http://www.symantec.com/en/uk/about/news/release/article.jsp?prid=20081124_11

[6] NYTimes.com: '*3 Indicted in Theft of 130 Million Card Numbers*' (August 2009)

http://www.nytimes.com/2009/08/18/technology/18card.html

[7] BBC.co.uk: '*US man "stole 130m card numbers"* ' (August 2009)
http://news.bbc.co.uk/1/hi/business/8206305.stm

[8] NYTimes.com: '*Global Trail of an Online Crime Ring*': (August 2008)
http://www.nytimes.com/2008/08/12/technology/12theft.html

[9] The 2008 '*Symantec Report on the Underground Economy* XII', Page 11:
http://www.symantec.com/en/uk/about/news/release/article.jsp?prid=20081124_11

[10] NYTimes.com: '*Global Trail of an Online Crime Ring*': (August 2008)
http://www.nytimes.com/2008/08/12/technology/12theft.html

[11] NYTimes.com: '*3 Indicted in Theft of 130 Million Card Numbers*' (August 2009)
http://www.nytimes.com/2009/08/18/technology/18card.html

[12] The 2008 '*Symantec Report on the Underground Economy* XII', Page 11:
http://www.symantec.com/en/uk/about/news/release/article.jsp?prid=20081124_11

[13] BBC.co.uk: '*US man "stole 130m card numbers"* ' (August 2009)
http://news.bbc.co.uk/1/hi/business/8206305.stm

Case Study References

Additional Information

[1] For a comprehensive review of the Russian online crime environment, see:

Symantec Research Report: '*An Overview of the Russian Hacking Scene*': (July 2007)

http://www.emea.symantec.com/onlinefraud/viewPDF.cfm?pdfname=An_Overview_of_the_Russian_Hacking_Scene.pdf

[2] Brief profiles of other online organised crime groups and their modes of operation can be found at:

Baselinemag.com: '*10 Notorious Cyber Gangs*':

http://www.baselinemag.com/c/a/Security/10-Notorious-Cyber-Gangs/

[3] For a detailed description of one member's involvement in an online organised crime group, see:

Wired.com: '*One Hacker's Audacious Plan to Rule the Black Market in Stolen Credit Cards*' (December 2008)

http://www.wired.com/print/techbiz/people/magazine/17-01/ff_max_butler

Appendix C

Morphological Analysis (MA) Methodology and Matrices

Morphological Analysis (MA) 'is a qualitative method used to holistically explore a range of different possible explanations for a number of issues by dividing the problem into different elements and displaying them in the form of a matrix that visually represents the 4 steps of the analytical process. [1]

MA is intended to be used during the early stages of exploratory analysis, for instance within situations where, although some data is available, the quantity may be insufficient to undertake meaningful quantitative analysis or, as often occurs when considering organised crime, there are a wide range of possible scenarios which need to be reduced to those which are most feasible for the given situation.

Originally designed for use within the field of astrophysics,[2] the method has evolved to be used as an analytical tool within a range of scientific and business environments, [3] as well as being proposed as a tool to develop strategic thinking about organised crime in criminal intelligence. [4] Although simple to apply, the method 'is deceptively complex and rich' in its returns [5] and, because it is available as a software application, [6] there is the option to incorporate larger data sets which can be analysed semi-automatically to create inference models. [7]

The 4 steps of the MA process [8] are:

1. *Break down the problem (identify the broad elements and categorise them)*
2. *Create a morphological matrix*
3. *Develop possible explanations or outcomes*
4. *Grade the explanations (eg from most feasible to least feasible).*

Step 1

Break down the problem

The purpose of this stage is to categorise and define the different elements of the problem in broad terms, from a multi-disciplinary perspective.

For this exercise, a scenario is devised whereby different members of a commercial organisation's multi-disciplinary team (for instance, a high-level Incident Management team) are each required to evaluate a set of data items which refer to pre-identified online criminal activity, in order to meet and agree the key issues which, in their view, require prioritisation from the perspective of their own business. In this scenario, the organisation is undertaking this activity alongside the Incident Management procedures which have been activated involving the police. (In other circumstances, the methodology lends itself equally well to use by multi-disciplinary teams composed of different organisations or agencies.)

Although this is the first time that the team have identified an incident that may involve significant online organised crime activity, they have all previously been briefed on the types of threats which such activities can pose to their type of business and have kept up-to-date with reading industry reports on the subject.

As with all early stages of Incident Management, time is of the essence, not only in order to address the problem, but also because the team members need to return to their regular duties as soon as possible. Therefore, the team need to identify and agree their key items quickly, using a straightforward, simple tool, with a view to undertaking more in-depth, targeted analysis at a later stage, for instance by following the guidelines within the ISO/IEC 27005 Risk Management standard.

The team decides that the fundamental question they need to answer at this stage is:

In what ways might this online organised crime group pose a threat to our organisation's vulnerable assets?

In order to do this, they identify that they need to evaluate the threat potential of the possible organisational structure and business model/s which the online criminal group

is utilising. The team uses the items in ***Table 6*** to identify potential online criminal organisational structures which may apply in this situation, then, following initial analysis by the business professionals within the team, add the types of potential business model which are indicated by their existing evidence. The Information Security professionals provide data about potential attack vectors and all members of the team agree the assets which they deem to be most vulnerable.

Step 2

Create a morphological matrix

The outcome of the team's Step 1 processes are depicted in ***Matrix Table A***.

The headings are located on the left-hand side, with the elements listed to the right. Thus, all the identified important features are listed along a row. The features in subsequent rows do not need to relate to the group above and it is accepted that some pairs of conditions may be 'mutually inconsistent or contradictory'.

Morphological Analysis of a theoretical online organised crime group

Step 2 – Create a Morphological Matrix

Matrix Table A

Elements of Problem						
Criminal Organisational Structures	*Collaboration*	*Fluid, changeable roles, membership and structure*	*Hierarchical Structure*	*Network Structure*	*Commercial/Business-Like Structure*	*Specialised Division of Labour*
Criminal Organisational Business Model	*Subscription Business Model*	*Collective Business Model*	*Online Auction Business Model*	*'Other' Business Model Type*		
Criminal Organisation Attack Vectors	*Phishing*	*Distributed Denial of Service (eg botnets)*	*'Drive By Downloads'*	*Insider Corruption*	*Fraud*	*Spyware*
Potential Targets (Sites)	Site Type A – Headquarters	Site Type B – Vancouver Office	Site Type C – Nairobi Office	Site Type D – London Office	Site Type E – Melbourne Office	Site Type E - Home-working sites
Potential Targets (Data)	Personal Data (all types)	Research and Development Data	Intellectual Property	Financial Data	IT-Related Data (eg Network Infrastructure Maps)	Physical Site Maps and Blueprints
Potential Targets (Stakeholders)	Staff (Management)	Staff (Operational)	Third Parties	Existing/ Potential Customers	Shareholders	Other Stakeholders
Potential Targets (Physical/ IT)	Network Infrastructure	Physical Storage Systems (eg Paper files)	Databases	Websites	External Storage Devices (eg PDAs, USB drives)	Physical Assets (eg Keys, Safes, Staff Passes)

Step 3

Develop possible explanations or outcomes

This stage identifies attributes in the situation which may not have been previously apparent and which may require further analysis.

At this point, the team use the matrix to explore the range of possible explanations or outcomes for the problem that is being analysed. They read the matrix by moving down and across the items to establish possible connections between pairs of items and to generate the range of possible outcomes. It is important that the team evaluates the items as objectively as they can, without introducing any interpretative considerations which might arise from their specialist fields.

One important by-product of this and the subsequent stages is that the team members will be informing and updating each other about important aspects of the situation during their focussed discussions.

It is not necessary (and will usually not be feasible) to develop a scenario for every possible combination. Because the number of possible configurations is the product of the number of conditions under each parameter, [9] for the example in this paper, this would equate to 186, 624 possible combinations:

6 x 4 x 6 x 6 x 6 x 6 x 6 = 186,624 possible combinations.

However, juxtaposing the items which can produce these combinations within a morphological matrix allows a professional to quickly identify and extract the elements which they recognise to be important.

Neither is it necessary for every item to have a connection. Within MA, identifying items which are not deemed to have relevance and which can be discarded are equally as important as identifying positive connections. [10] These are the pairs of items which are deemed to have inherent inconsistencies for one of these reasons: logical contradictions, empirical constraints or normative constraints (eg where a political situation might prevail which makes the pairing unlikely). [11] For this particular example, all the items (when read vertically) may have some relevance and may be mutually compatible.

As an example of the process, ***Matrix Table B*** shows the possible links between one set of the attributes.

In this particular example, the links might suggest a potential threat arising from the following associations:

> *An online organised crime group specialist division who obtain their tools, in this case spyware, from a criminal online auction site, with the intention of targeting the personal data within databases that can be accessed remotely by management staff.*

Substituting any single item (for instance, replacing 'Site Type E – Homeworking Sites' with 'Site Type A – Headquarters' or replacing 'Spyware' with 'Distributed Denial of Service' attacks) creates a new and different scenario.

By applying their judgment to extract the most significant possibilities within the matrix, the team obtains a list of scenarios which, although brief, between them capture the key issues that the whole team have decided need to be addressed.

Morphological Analysis of a theoretical online organised crime group

Step 3 – Develop Possible Explanations or Outcomes

Matrix Table B

Elements of Problem						
Criminal Organisational Structures	*Collaboration*	*Fluid, changeable roles, membership and structure*	*Hierarchical Structure*	*Network Structure*	*Commercial/Business-Like Structure*	*Specialised Division of Labour*
Criminal Organisational Business Model	*Subscription Business Model*	*Collective Business Model*	*Online Auction Business Model*	*'Other' Business Model Type*		
Criminal Organisation Attack Vectors	*Phishing*	*Distributed Denial of Service (eg botnets)*	*Ransomware*	*Insider Corruption*	*Fraud*	*Spyware*
Potential Targets (Sites)	Site Type A – Headquarters	Site Type B – Vancouver Office	Site Type C – Nairobi Office	Site Type D – London Office	Site Type E – Melbourne Office	Site Type E - Home-working sites
Potential Targets (Data)	Personal Data (all types)	Research and Development Data	Intellectual Property	Financial Data	IT-Related Data (eg Network Infrastructure Maps)	Physical Site Maps and Blueprints
Potential Targets (Stakeholders)	Staff (Management)	Staff (Operational)	Third Parties	Existing/ Potential Customers	Shareholders	Other Stakeholders
Potential Targets (Physical/ IT)	Network Infrastructure	Physical Storage Systems (eg Paper files)	Databases	Websites	External Storage Devices (eg PDAs, USB drives)	Physical Assets (eg Keys, Safes, Staff Passes)

Step 4

Grade the explanations (eg from most feasible to least feasible)

The final step of the process for the team in this instance is to assess the findings of Stage 3 according to whether they are 'possible, practical and feasible' from a criminal perspective. (The option is also open to them to assess the scenarios against any other potentially-relevant criteria such as effectiveness or precedent within their own industry). It is at this stage that the team members reintroduce pertinent issues arising from their specialist fields.

For the example, each scenario can be assessed as follows:

Scenario	Possible? (Y/N)	Practical? (Y/N)	Feasible? (Y/N)
An online organised crime group specialist division who obtain their tools, in this case spyware, from a criminal online auction site, with the intention of targeting the personal data within databases that can be accessed remotely by management staff.	Yes	Yes	Yes

The scenarios with the highest number of 'Yeses' are retained for further analysis, with the other scenarios being discarded for this exercise (although some of the less likely scenarios may still have revealed valuable information which the business captures and addresses externally).

The remaining scenarios may highlight issues which need to be addressed. For instance, focusing on a scenario which involves a possible interaction between data that is accessed remotely and spyware might prompt an organisation to review its anti-virus and anti-spyware strategies, as well as auditing remote working procedures to ensure that all data processing occurs on authorised equipment.

At this point, additional methodologies can be introduced to further ascertain the likelihood of particular threats, for instance undertaking risk and impact analysis using threat and vulnerability assessment manual or software tools, with the final objective being to provide recommendations for further action.

Thus, using a systematic methodology such as MA assists in the process of reducing a scenario from the abstract to the concrete, which is often an issue where online organised crime activity is concerned, as well as increasing the likelihood that any subsequent analysis is undertaken on the most important set/s of data.

References

Appendix C

The MA methodology approach utilised in this paper is based on:

C E Heldon: '*Exploratory Analysis Tools*' (Pages 112-114, J H Ratcliffe (Ed), 'Strategic Thinking in Criminal Intelligence' (The Federation Press)) (2004, 2007)

The origins of this methodology are explained in T Ritchey's paper:

'*General Morphological Analysis (MA) – A General Method for Non-Quantified Modelling*'

(Adapted from the paper 'Fritz Zwicky, Morphologie and Policy Analysis', presented at the 16th EURO Conference on Operational Analysis, Brussels) (2003-2009)

http://www.swemorph.com/ma.html

The scenario has been devised by Anna Cevidalli.

1. C E Heldon: Page 112, '*Strategic Thinking in Criminal Intelligence*' (J H Ratcliffe (Ed), The Federation Press) (2004, 2007)

2. Page 2, '*General Morphological Analysis (MA) – A General Method for Non-Quantified Modelling*'

   http://www.swemorph.com/ma.html

3. T Ritchey: Page 4, '*General Morphological Analysis (MA) – A General Method for Non-Quantified Modelling*'

   http://www.swemorph.com/ma.html

4. C E Heldon: Page2 112-114, '*Strategic Thinking in Criminal Intelligence*' (J H Ratcliffe (Ed), The Federation Press) (2004, 2007)

5. T Ritchey: Page 4, '*General Morphological Analysis (MA) – A General Method for Non-Quantified Modelling*'

   http://www.swemorph.com/ma.html

6. T Ritchey: Page 2, '*General Morphological Analysis (MA) – A General Method for Non-Quantified Modelling*'

   http://www.swemorph.com/ma.html

   The software program is called '*MA/Casper*: Computer Aided Scenario and Problem Evaluation Routine'. (Page 9, Ritchey)

7. T Ritchey: Page 2, '*General Morphological Analysis (MA) – A General Method for Non-Quantified Modelling*'

   http://www.swemorph.com/ma.html

8. The steps of the methodology that follow are based on Ritchey's paper, as well as:

   C E Heldon: Page 113, '*Strategic Thinking in Criminal Intelligence*' (J H Ratcliffe (Ed), The Federation Press) (2004, 2007)

9. T Ritchey: Page 6,'*General Morphological Analysis (MA) – A General Method for Non-Quantified Modelling*'

   http://www.swemorph.com/ma.html

10. T Ritchey: Page 7,'*General Morphological Analysis (MA) – A General Method for Non-Quantified Modelling*'

    http://www.swemorph.com/ma.html

11. T Ritchey: Page 8,'*General Morphological Analysis (MA) – A General Method for Non-Quantified Modelling*'

    http://www.swemorph.com/ma.html

Appendix D

Information and IT Attributes Exploited by Offenders

(Supplement to Section 4.1.2)

Key attributes of Information and Technology which are exploited by all types of offenders.

'Atomisation'

Information on the Internet, which is fundamentally composed of binary packets ('1's and '0's), can be reduced to miniscule amounts. Equally, electronic currencies can be calculated to infinitesimal decimal places and information within a single web page can originate from many different sources around the world, any element of which can potentially be compromised.

'Atomisation' [1] presents a security concern because most adware is compiled using *JavaScript*, whose functions can be misused so that adware residing on an innocuous website, when accessed, can redirect the user to a malicious destination. The complexity and inter-dependence of these components makes it very difficult to apply comprehensive security controls to them. [2]

Automation

Automated techniques have major advantages over their terrestrial equivalents. Users can instigate complicated processes at the click of a mouse button. Automation is increasingly a feature within crimeware, enabling offenders to launch powerful attacks such as DDOS attacks using minimal technical skills.

Continual Availability

Broadband and wireless connections enables 24/7 access to the Internet. In the 2008 UK BERR 'Information Security Breaches Survey', 84% of companies stated that they were 'heavily dependent on their IT systems', with 97% of the companies surveyed using a broadband connection and 42% using a wireless network. [3]

However, many organisations have not updated insecure legacy wireless protocols in their devices, providing another attack vector for offenders. [4]

Information is available ‘on demand’ from internet search engines which provide fast access to vast, cheap knowledge stores and social networking sites which foster the creation of online information-sharing communities, for legitimate and illegal users alike. In their ‘*2009 Midyear Security Report*’, 'Cisco’ cited the example of a ‘major botmaster’ seeking the assistance of his criminal colleagues through an online forum after his own botnet had been hacked. [5]

Innate Properties of Digital Information

Digital information comprises intangible yet valuable assets such as knowledge, human identities and network-dependent business operations, which can be traded using real and e-currencies. [6] It can be compromised with little obvious evidence that an incident has taken place. Data can either be physically viewed remotely using spyware or copied by malicious code without any indication to the end user that anything untoward has taken place because the copy of the data they are using appears unaltered.

Ancillary data, including cached data and metadata, is a rich source of useful information in itself, for instance when creating profiles of users’ Internet shopping patterns. In some cases, it can also be commoditised, with access to the data being granted at minimal cost in return for a membership fee. It can be further exploited as part of the reconnaissance stage of a targeted attack or to build up a profile of a person’s preferences and activities (via the ‘mosaic’ effect mentioned in Section 3.2 of the paper) which, in the case of vulnerable users such as children, could be scrutinised by all types of offenders and which could lead to a risk of harm or distress.

Innate Properties of Personal Information

Although high-profile data breaches have begun to alert users to considering how the information they provide is processed by governments and the private sector, vast amounts of personal information remain publicly-accessible and unprotected on the Internet, placed there voluntarily by members of the public who may not appreciate the risks, for instance, because they are part of a generation for whom communication via social networking sites such as ‘YouTube’, ‘FaceBook’, ‘MySpace’ and ‘Twitter’ is an integral aspect of their social lives. A major security issue with social networking sites is that membership of the communities is granted entirely on a basis of trust, without employing additional means of authentication.

An example of the potential damage that might occur following a personal data breach was reported by the UK newspaper *The Guardian* in July 2009. [7] The paper described the controversial circumstances which have led to the ongoing court case of Anthony O'Shea who claims he was a victim of identity theft and who was jailed for 5 months as part of *Operation Ore*, a major police operation which targeted thousands of individuals suspected of accessing illegal child-related materials.

Mr O'Shea's solicitor argued that 'hundreds' of people might have been wrongfully convicted because their identities were stolen by paedophiles who used them to make illegal purchases on *Landslide Inc*, a website containing adult pornography and child abuse images, with huge personal consequences such as the loss of their livelihood and health.

The case has divided experts, with some finding evidence of fraud and others certain that the convictions in question are valid. The situation is further complicated by the fact that paedophiles, when apprehended, are particularly adept at using every facet of the law that they can find in their favour. At the same time, the possibility that hundreds of identities may have been deliberately compromised in order to commit crimes of this nature must be thoroughly investigated as a crime in itself. Thus, the possibility that online ID theft was committed (on the surface, a fairly straightforward type of crime) has perhaps affected the lives of hundreds of people adversely and has led to legal boundaries being tested.

Jurisdictional Arbitrage

Unfortunately, the deregulated environment of the original Internet, which was built on mutual trust and which encouraged free market rapid business development, has not proved to be sustainable. Jurisdictional arbitrage is a term to describe the exploitation of legal loopholes which all types of offenders, including organised crime groups, exploit to evade capture.

Offenders can base their enterprises in 'safe havens' where they are unlikely to be prosecuted, for instance in countries where their acts may not be recognised as crimes. Law enforcers in many countries do not enjoy the same freedom and may be hampered by complicated evidence trails, legal red tape and non-co-operation. [8]

Ubiquity

In addition to becoming more interconnected, modern information technology is increasingly ubiquitous (present in many environments). Together, these two factors vastly increase the potential tools which offenders can employ when committing their crimes, for instance when technologies such as web and e-mail access are combined within the new generations of mobile telephony.

For instance, in the UK in August 2009, a serving prisoner was convicted for co-ordinating a cocaine-smuggling operation from his cell using a mobile phone and sim cards which had been smuggled into the jail. His contacts included a fellow prisoner who was serving his sentence in Panama. [9]

In a separate incident, it was alleged by SOCA (and disputed by the UK Prison Service) that imprisoned organised crime group leaders were passing their orders to external group members using 'code words in chat-room facilities on interactive games. [10]

'The Times' quoted Bill Hughes (the Director General of SOCA) as saying that 'organised crime bosses were operating their multimillion-pound empires from behind bars by using internet games to pass on their orders. Some were using code words in chat-room facilities on interactive games to operate from within jails…'

Although the claim was denied by the Prison Service, 'SOCA stood by its intelligence'.

Whether or not this particular allegation is proven, the technique is simple and could be feasible in any environment.

The UK Government has responded to this type of situation by publishing its commitment to tackle the issue in its recent Home Office report, '*Extending Our Reach*'. This includes extending its mobile phone-blocking pilot and updating the legislation which addresses mobile phone smuggling and possession within prisons. [11]

Appendix D

Information and IT Attributes Exploited by Offenders References

---

'Atomisation'

[1] A definition of 'atomisation' within a Web context is provided at DaveChaffey.com: '*Atomisation in Internet Marketing Definition*' (2008)

http://www.davechaffey.com/E-marketing-Glossary/Atomisation-in-Internet-marketing.htm

[2] Symantec White Paper: Pages 6- 8, '*Web-based Attacks – February 2009*'

http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_web_based_attacks_03-2009.en-us.pdf

---

Continual Availability

[3] UK Department for Business Enterprise and Regulatory Reform (BERR): Page 2, '*2008 Information Security Breaches Survey – Technical Report*'

http://www.pwc.co.uk/eng/publications/berr_information_security_breaches_survey_2008.html

[4] The Register: '*Ecommerce standard tightens up wireless security*' (October 2008)

http://www.theregister.co.uk/2008/10/02/pci_dss_update/

[5] Cisco: Page 2, '*2009 Midyear Security Report*' (2009)

http://www.google.co.uk/search?client=qsb-win&rlz=1R3GGLL_enGB336GB336&hl=en&q=cisco,+midyear+security+report,+2009

Innate Properties of Digital Information

[6] R Etges and E Sutcliffe: Page 91, '*An Overview of Transnational Organised Cyber Crime*' ('Information Security Journal: A Global Perspective', 17) (2008)

Innate Properties of Personal Information

[7] Guardian.co.uk: '*Legal Challenge to Web Child Abuse Inquiry*' (July 2009)

http://www.guardian.co.uk/uk/2009/jul/02/web-child-abuse-inquiry-challenge

---

Jurisdictional Arbitrage

[8] Phil Williams, CERT® Co-ordination Centre paper: Page 4, '*Organised Crime and Cyber-Crime: Implications for Business*' (2002)

http://www.cert.org/archive/pdf/cybercrime-business.pdf

For instance, in 2008, due in part to the lack of formal extradition arrangements between the UK and Russia, a known Russian ransomware author evaded apprehension:

TheRegister.co.uk: 'Ransomware Author Tracked Down, but not Nicked' (October 2008)

http://www.theregister.co.uk/2008/10/01/gpcode_author_hunt/

Ubiquity

[9] BBC.co.uk: '*Prisoner ran drugs ring from cell*' (August 2009)

http://www.google.co.uk/search?client=qsb-win&rlz=1R3GGLL_enGB336GB336&hl=en&q=prisoner+ran+drugs+ring+from+cell

[10] Timesonline.co.uk: '*Row over claims that crime lords 'running empires from jail using PlayStations'* (May 2009)

http://www.timesonline.co.uk/tol/news/uk/crime/article6280199.ece

[11] UK Government: Page 23, '*Extending Our Reach: A Comprehensive Approach to Tackling Serious Organised Crime'* (UK Government Report, Crown Copyright) (July 2009)