Transnational Organised Cyber Crime: Distinguishing Threat from Reality

By Rob McCusker[1]

'Will we see the emergence of cybercrime cartels?'[2]

Abstract

Cybercrime has become an integral part of the transnational threat landscape and conjures up pressing images of nefarious and increasingly complex online activity. More recently, the concept of 'organised crime' has been attributed to cybercriminality. There has been subsequent disagreement and confusion concerning whether such crime is a derivation of traditional organised crime or an evolution of such crime within the online space. This opaque state of affairs has been exacerbated by the relative lack of clear evidence attesting to and supporting either scenario. Technological advances have always been used to the advantage of the criminal fraternity. The crucial question that remains is whether those advances have merely *facilitated* the commission of physical crime or whether in fact they have led to the *creation* of a new wave of traditional, but virtual, organised crime.

Introduction

In broad terms, the debate surrounding the actual and/or prospective involvement of traditional organised crime groups in cybercriminal activity is characterised by a tension between logic and pragmatism. Logic would dictate that traditional organised crime groups will engage with cybercriminal endeavours as fervently as they will with any low risk, high profit non-virtual criminal activity. Pragmatism on the other hand would suggest that it remains questionable whether such groups either need that engagement or indeed have the capacity to exploit the cyber environment to the extent that their capital investment would produce the desired and appropriate financial gains.

Defining 'cybercrime'

Yar[3] argues that '[i]t has become more or less obligatory to begin any discussion of "cybercrime" by referring to the most dramatic criminological quandary it raises, namely, does it denote the emergence of a "new" form of crime and/or criminality?' Grabosky[4] sought at a relatively early juncture to address that question by suggesting that cybercrime was simply a case of 'old wine in new bottles', that is '…less a question of something completely different than a recognizable crime committed in a completely different way.' In a similar vein, Nisbett[5] has argued that '[c]yber crime is on the increase. This does not necessarily mean that there are in fact any new crimes; rather there are new methods of committing existing crimes and better ways of

detecting them'. Interestingly, Wall[6] has noted that '…when so-called cases of cybercrime come to court, they often have the familiar ring of the "traditional" rather than the "cyber" about them'.

Crime, like nature, however, abhors a vacuum. It has accordingly always seemed inevitable perhaps that traditional organised crime groups would positively rush to fill the void for illicit product placement deemed to present itself in the context of cyberspace. It might be assumed, therefore, that an evaluation of the purported involvement of traditional crime groups in cyber crime would be a relatively simple affair. Certainly, the literature, broadly defined, is replete with references to 'cybercrime' and more recently to 'organised' cybercrime. Unfortunately, the mere assertion in much of that literature that such crime exists (both in a general sense and in an organised form) has been routinely transmuted, as if by osmosis, into tangible fact. Arguably, however, in many cases those 'facts' appear to rely as much upon anecdote, hearsay, extrapolation and assumption as they do upon objectively obtained and verified evidence.

At the basic level of analysis there is no discernible control mechanism in place insofar as terminology is concerned. Thus, one might speak of 'cybercrime', 'high tech crime', 'computer crime', 'technology crime', 'digital crime' and 'IT crime' and be discussing the same and/or different concepts, respectively. Achieving any vestige of comparative analysis of the impact of cybercrime therefore is fraught with difficulties. Beyond that, the increasingly common conflation of cybercrime with the prefix 'organised' infers the involvement of traditional organised crime groups but ultimately alludes to 'ordinary' criminals who happen to operate in cyberspace in an organised manner. Equally, it seems common to refer to cybercriminal 'groups' as if they were of equivalent size, complexity, 'stature' and duration as their traditional, non-virtual counterparts. This effectively allows cybercriminal groups to achieve the *semblance* of the organisational evolution *actually* achieved by those traditional organised crime groups they are deemed to emulate. In short, there remains a confused and confusing plethora of terminology, purported parameters and alleged participants of cybercrime as well as concerns over the provenance and quality of evidence elicited in support of such activity. These are certainly subtle differences but they are important differences nevertheless.

In consequence the term 'cybercrime' has rapidly become a generic descriptor for any malfeasant online behaviour (whatever the relative differences in complexity and seriousness) ranging from spam emails and denial of service attacks to malware and botnet infiltration. Indeed, a recent IBM survey[7] on cybercrime globally did not in fact define 'cybercrime' and yet sought information from business participants on every continent on the impact of such crime. The net effect of such surveys is that the myth of cybercrime is perpetuated and the facts of cybercrime become sacrificed at the altar of public

perception. It is the very imprecision of the term which has given rise to the hyperbole and opacity that surrounds it.

Beyond the broad non-specificity of definition lies an equally amorphous conundrum, which forms the heart of this piece, namely, whether 'organised' cyber crime is crime committed by traditional organised crime groups or 'merely' that it is crime committed online in an organised manner. Even at this juncture the question is fraught with difficulty. The term 'organised', when applied to traditional organised crime groups, *is* defined (see, *inter alia*, the UN Convention against Transnational Crime[8]) and subsequently assessments of organised crime can gravitate to and from a fixed point. However, 'cybercrime' is seemingly deemed to be 'organised' once the perpetrator ceases to be the archetypal lonely hacker and gravitates instead towards a group of fellow lonely hackers. If acting in illegal concert were the *sole* arbiter of 'organised' crime then *any* form of criminal behaviour which necessitated *any* degree of planning might be deemed *de facto* to be organised crime.

Ultimately, however, the Council of Europe[9] has argued that '[d]ata on connections between organised crime and cybercrime are still scarce and do not permit a reliable analysis.' Thoumi[10] suggested that technology can democratise crimes because '[t]he fact that smaller players have an easier time entering the market is one reason why the notion of the great crime "cartels" may increasingly be a myth as the contemporary criminal market places changes in origin.' The definitional waters have been muddied somewhat by comparisons of cyber criminals with traditional organized crime groups. FBI agent Thomas Grasso Jr. argued[11] that Carderplanet '…organized [itself] into the same structure as the Italian Mafia'. Grasso[12] also suggested that the International Carders' Alliance, to which Carderplanet, Mazafaka and IAACA (the International Association for the Advancement of Criminal Activity) belonged '…is really the heart of organized cybercrime.' Christopher Painter,[13] of the Computer Crimes and Intellectual Property Section at the US Department of Justice, noted in 2006 that '…[w]e are seeing organized criminal groups' but that they were in fact '…groups that are organized online targeting victims via the Internet.' These assertions are somewhat incongruous and consequently both sets of assertions do little to clarify the distinction between traditional organised crime involvement in cyberspace and criminals who simply operated in the online space.

The law enforcement perspective

In truth, fewer terms are destined to create a greater state of apoplexy within law enforcement agencies than 'cybercrime', a fact reflected in part by their usual depiction of such crime as 'high tech' rather than 'cyber' in nature. Indeed, even the term 'high tech' crime has drawn criticism. Hynds[14], for example, noted that '[h]igh tech crime is an oxymoron; a classic contradiction in terms…It's not about technology, it's about people.' The dislike of the term

'cybercrime', and particularly its increasing association with the term 'organised', reflects a common belief in such quarters that cybercrime is nothing more than ordinary traditional crime enhanced in terms of its distribution and impact by the facilitation of technology. Nisbett[15] (2002) maintained that '[e]very advance in technology appears to create a new crime alongside it' and indeed, technological advances from the mobile telephone to the police scanner have historically been used by the criminal fraternity. That the complexity of such technology has increased, and continues to increase, exponentially does not detract from that fact.

The tension between the law enforcement perspective on the one hand, and the assertions within oft-accessed and cited literature on cybercrime on the other, may appear to be a little odd given the accepted use of technology by criminals generally. It might be argued that to admit the involvement of traditional organised crime groups in cybercriminal activity would place law enforcement agencies in the unenviable position of having to investigate yet more complex virtual crimes within a still predominantly physical law enforcement environment. Whilst at the helm of the Federal Bureau of Investigation, J. Edgar Hoover refused to acknowledge the existence of organised crime until the Kefauver[16] and McClellan[17] committees and the highly visible Appalachian[18] meeting rendered continued denial superfluous. For Hoover to have admitted the arrival of organised crime would have necessitated a concerted response designed to curb it and this was something Hoover could not at that time guarantee. Given the general advantage transnational crime groups have over law enforcement agencies in terms of the distance they are able to place between the commission of crime and its ultimate resolution at the hands of the criminal justice system, it might be suggested that a Hoover-like dread currently rests upon the heads of law enforcement agencies. However, this would be a tad disingenuous given the fact that unlike organised crime in the 20th century, cybercrime in the 21st century is arguably more akin to an *adaptation* of existing crime to new technology than the *creation* of a brand new crime type and/or structure. Equally, one might assume that in order to operate effectively within the relative complexity of the online environment one would have to be organised as a matter of course. In this sense, the debate as to whether criminality is organised or not might be deemed somewhat redundant. However, given the finite nature of law enforcement resources it remains important strategically and logistically for cybercrime efforts to be directed at the *actual* rather than *supposed* criminals. That, in turn, renders the question as to whether one is confronting traditional organised crime in an online context, or online criminals who happen to be organised, a practical and serious one.

The generic relationship between technology and crime

In 1992 the United Nations Economic and Social Council observed[19] that '[i]nternational experience shows that organized crime has long ago crossed

national borders and is today transnational…It should be noted that aspects of the evolutionary process undergone by society may make powerful criminal organizations even more impenetrable and facilitate the expansion of their illegal activities.' An integral feature of that societal evolution has of course been the development and utilisation of technology and its associated components. More than a decade ago it was suggested that information and communication technology would play a prominent role in defining what was likely to become of greater value to a criminal in the future and might dictate that 'electronic property', such as video-on-demand, knowledge and information such as copyrights or trademarks, or identity devices such as biometric smart cards, would be the assets of interest in the future[20]. Naylor[21] had suggested that there had been a deal of hyperbole over the role of technology and argued that in the early to mid 19th century the impact of the railway, steamship and telegraph was far more revolutionary than the Internet or mass air travel. Indeed, he noted, '…virtually every kind of crime now conducted through modern electronic communications technology had some equivalent in the telegraph age – which saw everything from insider trading to price fixing to financial fraud conducted by and through the telegraph, while telegraph companies faced problems of breaches of security by hackers threatening, in particular, telegraphic money transfers.'[22] Zittrain[23] convincingly argues that '[e]very technological development…has to varying degrees been a source of criminal opportunity, be it as a target or facilitator of criminal or malicious activity. Increasingly, however, we are seeing the compounding of criminal opportunity as technologies converge.' In support of this apparent convergence Sussman[24] suggests that '[t]here is a revolution going on in criminal activity…The revolution lies in the ways that networked computers and other technologies permit crimes to be committed remotely, via the Internet and wireless communications.' Indeed, one might argue that the potential future of cybercrime sits within the broader digital environment, an environment created primarily to facilitate social and business relationships and transactions but one which is increasingly prone to degradation, infiltration and subsequent malfeasant activity. Although the precise future characteristics of cybercrime cannot be accurately determined it remains both possible and appropriate to frame potential cybercrime activities within the context of developments in technology more broadly and of the digital environment it supports and operates within.

The target environment

As suggested at the outset, logic alone would suggest that the digital environment will be increasingly targeted by traditional organised crime groups. The recognition by the business sector of the wealth of product placement opportunities available on the Internet will not have escaped the notice of traditional organised crime entities. Conversely, the extent to which there has been a major development in traditional organised criminal behaviour

and activity, as a direct or indirect result of cybercrime developments per se, is starting to be questioned.

The Internet, for example, was never designed to be a highly developed or intelligent system. The basic purpose of the Internet, a vehicle for conveying packets of data between devices (the "end to end principle"), has remained unchanged and the resultant architecture, whilst embracing the original unfettered communication precept of the Internet, has facilitated an increasing vulnerability to inadvertent technical failings as well as advertent criminal and other malfeasants. It is clear that it is becoming less and less able to cope with the exponential demands, in terms of information storage and exchange, being placed upon it. In addition, globalisation requires, and will continue to necessitate, an increased connectivity of the world's computer, banking and financial systems. Globalisation has increased the free movement of capital between the world's developed and underdeveloped economies. Globalisation operates in cyberspace, which by definition is extraterritorial. This means that the regulatory practices which purport to exist and operate in the land-locked world, and which should be the *sine qua non* of the globalised economy, are missing.

Furthermore, the Internet was never designed to be secure from exploitation. The strength of the Internet in terms of its rapid communication facility has become one of its undermining weaknesses. The criminal fraternity operates online under the same free market principles and the legislative and law enforcement endeavours launched against them suffer from geographical and practical restrictions. The potential for an increase in the number of victims of economic crime, as well as cybercrime more broadly, is likely to rise. The dissemination, storage and protection of information lie at the heart of the Internet, e-commerce and the online environment per se. Personal information about clients and customers is increasingly being lodged in digital documentation and that digital documentation is being routinely disseminated between computer networks. This distributed digital identity places confidential information in the ether with only the security processes of the organisation to prevent its exploitation. The acquisition and abuse of such information is likely to continue to form the basis of the future cyber crime threat. The sheer wealth of information likely to become available (if Google™ and similar search engines are any indication of future provision) to the average private user may, it is suggested[25], lead to the use of "knowbots" (knowledge robots) to navigate on a person's behalf through such data more effectively and even organise part of their daily routine such as scanning email for particular addresses or subject matter. The dangers of such knowbots being controlled by a malicious third party might of course facilitate the navigation of bank accounts etc with equal aplomb. A recent report[26] has suggested that the new threat landscape may be typified by malware attacks which facilitate subsequent criminal endeavours. Attacks are deemed to be moving away from large affairs (such as global spam incidents) to smaller, more focused attacks

upon particular clients. The motivation has become largely profit-oriented and such attacks may facilitate those activities which increase profits most readily such as identity theft, fraud and extortion. Symantec noted[27] that in the latter half of 2005, 80% of the top 50 reported threats could be used for data theft. 'Unfortunately', it went on to observe, 'it appears profit is the new motive for Internet threats, and the pride of one-upmanship – which used to inspire cyberattacks – is giving way to calculated criminal intent.' CipherTrust[28] has supported this assertion by noting that '[w]hen information gained through phishing is sold, profits often get routed to international criminals and activities.'

Corresponding risks have of course been identified with advances in technology. Increasing dependency upon computer systems to control and operate key infrastructure may leave such control systems, and the populations who depend upon their effective operation, prone to the consequences of any subsequent breach. Importantly, the wider dissemination and availability of technology may render it a far easier task for criminals to engage fraud and fraud-related endeavours.

Technology is destined to become increasingly ubiquitous. Established technologies such as mobile phones and computers will continue to widely used but there is likely to be a proliferation of auxiliary devices aimed at improving the performance and flexibility of those established products. The key threat emanating from the ubiquity and complexity of technology in an era of increasing connectivity will be viral contamination. This threat will be exacerbated by the reliance placed by businesses and individuals upon the technology to function in their daily lives. Communication vehicles will increase exponentially and the danger of such communication conduits being breached and exploited by cybercriminals is likely to rise in tandem. As the Commission on Crime Prevention and Criminal Justice once noted[29] '…as the degree of reliance placed on networks increases, the potential harm from criminal offences also increases.'

The fact, for example, that the computer can be left permanently on and connected to the Internet, when coupled with the poor security awareness of many domestic users, renders such computers prone to criminal attack. The potential rationale for such attacks could include the obtaining of personal information for identity theft, the use of the computer as a 'zombie' or storage facility for illegal material (as has been found to be the case with commercial and university systems). These dangers are likely to be exacerbated by activities such as peer-to-peer file sharing programs or the downloading of files from unknown senders. Rapid download times have also facilitated the dissemination of content such as pornographic images and pirated software and music particularly through Peer to peer (P2P) platforms. Most P2P software is free and it is believed may contain overt or covert advertising related software. There is a danger that the software may also contain spyware[30].

The increasing use of mobile phones and PDAs (Personal Digital Assistants), each with ever-increasing storage capacity and ever-diminishing security protocols, constitute another potential threat. Such devices are routinely used to store personal data and corporate information and the advent of wireless networking increases the likelihood of such information being uploaded and downloaded. In 2005, twenty-two percent of people reported losing their mobile devices and of those 81 percent had not encrypted the information contained therein[31]. Wireless networks themselves may bring a number of vulnerabilities. Key amongst these is the fact that the network and its data can be accessed without physical access or presence being required. This facility assists the user but more importantly constitutes a positive boon to the criminal.

Traditional organised groups in cyberspace

Brenner[32] has argued that '…nothing has been written about whether organized criminal activity will emerge in cyberspace and, if so, what forms it may take'[33] This may in part be attributed to the fact that traditional organised crime groups '…evolved in the context of real-world endeavors [sic], mankind having lived exclusively in the real world until quite recently.' Nisbett[34] has posited the notion that '[t]he current absence of organized cybercriminality makes a consideration whether organization will likely become an aspect of crime on the virtual frontier particularly topical and appropriate.' Given the assertions made concerning organised cybercrime, however, the capacity for, and desire of, traditional organised crime groups to engage in cybercrime should be evaluated. Brenner[35] ascribes the relative lack of analysis of traditional organised crime intent and/or desire to engage in cyberspace to '…the perception that cybercrime is perpetrated by hackers, who are loners, and are therefore not inclined to engage in group criminality; and the fact that, to date, most documented cybercrime reveals that a majority of incidents involve individuals, not groups.'[36] Given also the fact that it is the application and definition of the word 'organised', which has caused much of the current disquiet, discussion ought to be had as to whether the structures of traditional organised crime groups could, or would, conform to the rather sleeker organisational models deemed essential for the smooth infiltration and exploitation of cyberspace. Nisbett[37] suggests that '…empirical differences between the real world and the cyberworld will prevent the effective transfer of existing forms of real-world criminal organization modalities into cyberspace.' For Nisbett[38] '…the very nature of cyberspace is inconsistent with hierarchy. Cyberspace is a network, or, more properly, a network of networks. Networks are lateral, diffuse, fluid, and evolving. Hierarchies are vertical, concentrated, and tend to be rigid and fixed.' This seemingly presumes, however, that traditional organised crime groups retain the degree of hierarchical structure which Cressey[39] asserted, and Valachi[40] confirmed, in the 1960s.

It is recognised that in fact, flatter, more horizontal networks, comprising cell-like 'crews', have become the norm in much of the organised crime

environment (though Chinese triads and Japanese yakuza have remained traditionally hierarchical in nature) with the United Nations[41] having identified a number of structural variations within organised crime groups. Nisbett[42] suggests that '[l]ogically, the first issue to consider when analysing forms criminal organization may take in cyberspace is the extent to which already-evolved forms of criminal organization are likely to migrate to the virtual frontier. Since the already-evolved forms of criminal organization have proven successful in the real world, it is reasonable to expect that they will enjoy at least a measure of success in the cyberworld.' The flexibility of the organisation and control of traditional crime groups has in part derived from a proactive reaction by such groups to law enforcement endeavours and operations against such groups. Whilst one might argue that such structural changes have resulted more from the necessity of protection than through freedom of choice, this demonstrated ability to make such organisational changes augurs well for similar adaptations to be made by traditional organised crime groups in reaction to, and after reflection of, changes in their operating environment, namely, cyberspace. Olson[43] maintains that '[o]rganized crime is perfectly suited to profit from the information revolution. Its existence relies on innovating, adapting strategies and operations, and evading detection. These attributes complement the ever-changing nature and unpredictability of the information revolution. The Internet offers an array of lucrative opportunities with little or no risk.'

Europol[44] has indeed suggested that, at the meta level, '[t]he advantages the internet offers in terms of information and communication technology are extremely beneficial to [organised crime]. The underground cultures built around some of the high technology phenomena such as hacking and cracking are perfect for support, contacts, recruitment, advice and clients.' By way of tacit support for such a notion, McAfee[45] asserts that '[o]rganised crime gangs are starting to actively recruit skilled young people into cybercrime. They are adopting KGB-style tactics to recruit high flying IT students and graduates and targeting computer society members, students of specialist computer skills schools and graduates of IT technology courses.' For Williams[46], the transition of traditional organised crime from the physical to the virtual environment is as much about a natural progression in criminal behaviour as it is about a determined course of action given the fact that as '[o]rganized crime has always selected particular industries as targets for infiltration and the exercise of illicit influence…[f]rom an organized crime perspective, the Internet and the growth of e-commerce present a new set of targets for infiltration and the exercise of influence…'

Conversely, there has been a degree of rumination over whether the 'organised crime in cyberspace' versus 'crime in cyberspace which is organised' debate is itself being taken over rapidly by events. Clarberg[47] has pointed out that '…high technology crime is often not a crime in isolation, and forms part of a crime which is also occurring within the physical world. It is very difficult to

find a real world crime that does not have a high technology element, even if it is as common and straightforward as the use of a mobile telephone.'

There have also been suggestions that in fact, as with the purported[48] convergence of organised crime and terrorism in light of perceived mutual benefits, the two sides of the 'organised' debate may in fact find greater solace, reward and operational fluidity through a combination of their efforts. Olson[49] maintains that '[e]lements of both the cybercrime and organized crime worlds have encouraged the two to merge. Hackers were traditionally anti-social loners, operating without any monetary motivation. Their motivations have now shifted from mere curiosity to more self-serving and lucrative attacks. But hackers now frequently work together in loosely knit units or cells.' Furthermore, she notes that '[m]any of the characteristics traditionally attributed to organized crime can also be attributed to cybercriminals and hackers. This overlap in skill and motivation has created a natural bond between the two underground networks.'[50]

The possible redundancy of the term 'organised'

More radically still is the notion that the intrinsic nature of cyberspace will in fact alter the very notion of the term 'organised' whether applied within the context of organised crime of the traditional-oriented or cyber-born complexion. Nisbett[51] has observed a truism that '[i]n the cyberworld…one's aptitude as a cybercriminal is a function of his or her technical expertise…While there may be opportunistic reasons to affiliate with a cybercriminal group, such an affiliation is not essential for the pursuit of a criminal career, as it is for members of real-world gangs.' As Brenner[52] has it,'[t]he characteristics of cyberspace, the absence of fixed, empirical constraints and a diffuse, fluid, evolving environment, indicate that hierarchical organizational structures are at once not needed in and not appropriate for activities conducted in cyberspace. What, then, will criminal organization look like in cyberspace?...will organized criminal activity in cyberspace ever actually exist?'

Some authors have posited that cybercrime itself may alter the structure of traditional organised crime groups. The Council of Europe[53] notes, for example, that '[c]ybercrime requires less control over a geographical territory, less violence and intimidation, less personal contacts and thus less relationships based on trust and enforcement of discipline between criminals, in short less need for formal organisations.' Brenner[54] has suggested that '[o]nline criminal organization will tend to de-emphasize formal, hierarchical organizational structures. At the same time, it will emphasize a broader, lateral contextual structure. Online criminal organization has no reason to be circumscribed, in its membership or in its operations, by national, territorial boundaries or by cultural differences because cybercriminals…share a culture that transcends national borders and context. So, as opposed to the localized, rigid, and often

provincial hierarchical organizations that have so far characterized criminal groups, regional, or even global, coalitions will develop.'

Such coalitions are likely to comprise a mixture of '…cybercrime entrepreneurs…' and '…diffuse, loosely-structured opportunity groups…'[55] which are, in a manner currently typical of 'Russian' organised crime groups in the physical environment, likely to collude in relation to a specific offence and thereafter disband. The ties that bind and typify traditional organised crime groups in terms of membership criteria and strategic alliances are likely to become less constricting. The '…traditional indicia of commitment, and of membership, will decline in importance. Instead of multi-generational criminal enterprises, cybercriminal organization will emphasize arm's length, instrumental associative alliances.'[56]

Traditional organised crime online or online crimes which are organised?

The catalyst behind the current debate concerning traditional organised crime online, or online crime that is organised, is the nature and quality of evidence adduced in support of either and/or both camps. As a point of origin, Clarberg[57] has asserted that '[t]here is very little, if any quantitative data available for assessment of the size and impact of high-technology crime…' That of course has not prevented the production of a wealth of information asserting its existence, its composition and its impacts. Williams[58] once suggested that '[t]he synergy between organized crime and the Internet is not only natural but also one that is likely to flourish and develop even further in the future.' He posited that safe havens used in the physical environment are likely to be replaced with similar havens in the cyberworld and that the Internet provides a range of criminal opportunities in terms particularly of the commission of old crimes in new ways as envisaged by Grabosky[59]. In essence, Williams maintained that '…[t]he Internet provides both channels and targets for crime and enables them to be exploited for considerable gain with a very low level of risk. For organized crime it is difficult to ask for more.'

These observations and assertions reflect the logic component of the tension noted above[60] and indeed Williams[61] conceded that '[m]ost organized crime will continue to operate in the real world rather than the cyberworld and most cybercrime will be perpetrated by individuals rather than criminal organizations per se.' This position reflects the oft-neglected issue of motivation, that is, what might prompt organised crime groups to gravitate away from the target- rich physical environment to the relatively unknown quantity of the virtual world? Nevertheless, Williams[62] maintained, '…the degree of overlap between the two phenomena is likely to increase considerably in the next few years' and argued that '…there is growing evidence that organized crime groups are exploiting the new opportunities offered by the Internet.' The potential problem of Williams' assertion is not that it might *not* be accurate (which, given Williams' reputation, is highly

unlikely) but rather that the evidence adduced *publicly* to support that assertion is not conspicuously nor overwhelmingly present. Assertions without *cited* supportive evidence are quickly transformed into hearsay and anecdote which are in turn recycled within other authors' assertions concerning cybercriminal activity. At the point at which citations by one author, of examples provided by another (who may not have provided tangible evidence for those examples), become the norm, the task of distinguishing the true nature of cybercriminal behaviour from its presumed characteristics will becomes an increasingly difficult task. Furthermore, the capacity for law enforcement agencies to engage with the relatively unknown quantity of 'organised' cybercrime amidst a plethora of contradictory and unsubstantiated or under substantiated reports and conjecture will be further diminished.

A number of generic cyber crime threats have been identified[63] consisting of:

(1) offences against the confidentiality, integrity and availability of computer data and systems (via activities such as hacking, deception, interception and espionage)
(2) computer-related 'traditional' crimes (fraud and forgery), content-related computer offences (such as website defacement and dissemination of false information) and
(3) offences relating to the infringement of copyright and related rights (such as the unauthorised reproduction and use of programmes and databases)

Given the accepted precept that opportunity, tempered by an evaluation of relative risk, provides the key incentive to criminal endeavour, logic, if not evidence, would suggest that traditional organised crime groups and/or networks are fully engaged in the exploitation of the cyber environment. An oft-cited example[64] of the systemic nature of transnational organised crime groups' lateral thinking and exploitative powers was witnessed in October 2000 when a Sicilian mafia group, together with twenty other strategically placed individuals, created a digital clone of the Bank of Sicily's online component. Its plan, thwarted at the last moment by an informant, involved the diversion of $400 million allocated to the Bank by the European Union for regional projects within Sicily. The fact that the group tried and failed is not the key issue debated. That they actually conceived the idea is. Sadly, this example has often been cited as evidence of organised cybercrime and whilst it undoubtedly indicates a propensity for such crime by organised crime groups it remains in desperate need of the company of related organised crime endeavours to strengthen and/or clarify the debate. As Morris[65] argues '[d]espite the diverse and often interconnectedness of many of the threats and challenges that have been highlighted [in the Future of Netcrime Survey], this complexity should not obscure the fact that much of what is seen is merely old crimes committed in new ways. Human motivations, needs and frailties are relatively consistent.

Criminals and offenders are largely driven by finding ways of making money…'

Parizo[66] suggests that there is a common misconception in relation to cybercrime that '…organized crime on the Internet manifests itself just like traditional mafia.' According to Peretti[67] (of the US Department of Justice Computer Crime and Intellectual Property Division) '…it is virtually impossible to find any true crime families in cyberspace.' Indeed, in annual reviews and prognoses of future conduct, the level of actual or perceived involvement by organised crime groups in cybercrime remains peripheral to other traditional activities such as the trafficking of arms, drugs and people. However, such reports do note a connection between cyberspace and traditional organised crime but this is largely in the context of using cyberspace to facilitate old physical rather than new virtual criminality. It has been argued[68] that '…only a few cases are known in which organised crime elements have been active in the area of criminal offences against the confidentiality, integrity, or availability of computer data and systems.' Conversely, in relation to computer-related traditional crimes '[o]rganised crime groups are especially involved in acts of sophisticated computer fraud, credit card fraud, and telephone fraud.'[69] The Council of Europe[70] argues that '[i]n the area of content-related offences, organised crime groups are heavily involved in the production and distribution of child pornography.'

Europol also notes[71] that '[organised crime] groups rely on fast and secure means of communication. E-mail, internet chat rooms and instant messaging all offer new opportunities, as do web-based and client server mail accounts, websites and message boards. It provides speed of communication and, combined with encryption tools, offer unprecedented security for the data they store and exchange.' Furthermore, the Criminal Intelligence Service of Canada (CISC)[72] suggests that '[t]echnology facilitates increasingly secure, anonymous and rapid communication, through tools like encryption software, wireless devices, encrypted cellular phones and anonymous re-mailers that forwards emails without revealing their origins. Criminal groups exploit tools like this to plan and undertake criminal activities, such as drug trafficking, without physical interactions, thereby reducing the risks of detection and prosecution.'

In 2006, a joint US/Canadian organised crime threat assessment noted[73] that criminal enterprises and loosely organised criminal networks perpetrate identity theft throughout Canada and the US. It suggested that '…new technologies and the Internet provide identity thieves with innovative tools for acquiring large amounts of personal data with minimal effort.'[74] Asian Organized Crime Groups are deemed to have successfully combined 'traditional' activities such as extortion to technology related crimes including '…sophisticated credit card fraud, counterfeiting, and thefts of high tech components, such as computer chips.'[75]

In 2005, the CISC argued[76] that '[o]rganized crime groups are broadening their exploitation of technological vulnerabilities by targeting individuals and businesses that rely on technology, e-commerce and the on-line storage of valuable personal, financial and intellectual property data.' In 2006, the CISC reiterated this belief by suggesting that '[c]riminal groups are increasingly targeting communication devices to obtain sensitive personal and financial information in order to undertake theft and fraud.'[77]

Europol noted[78] that '[t]echnology is increasingly becoming a main facilitator of [organised crime]. New types of fraud such as data streaming of payment card details 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.' The Serious Organised Crime Agency has noted[79] that '[s]erious organized criminals are exploiting the Internet as a commercial medium as well as for their communications.' The use of botnets has also been attributed to organised crime groups and Hynds[80] has noted that '[t]he trade of BotNets on compromised machines is becoming an industry in itself. Organized crime is making use of this industry.'

The Financial Action Task Force has indicated [81] a new and prospective avenue for the illicit transfer of money (or more appropriately 'value') is that of new payment methods (NPTs) such as internet payment systems, mobile payments and digital precious metals. Designed primarily to facilitate cross-border funds transfer they contain a number of potential risk factors given that the distribution channel is the internet, that no face to face contact with the 'customer' occurs (a process known as disintermediation) and that the NPM process operates through an open and accessible network.

In 2001, Kubic[82] of the FBI Criminal Investigative Division argued that '[a]s worldwide dependence on technology increases, high-tech crime is becoming an increasingly attractive source of revenue for organized crime groups, as well as an attractive option for them to make commercial and financial transactions that support criminal activity.' Suggestions that organised crime groups recognise the benefits and utility of the Internet may be found in recent reports[83] which argue that criminals are targeting universities, computer clubs and online forums to find students to write computer viruses, commit identity theft and launder money (money mules). McAfee[84] maintains that '[a]lthough organised criminals may have less of the expertise needed to commit cybercrimes, they have the funds to buy the necessary people to do it for them.' Stone argues[85] that '[c]yber criminals have advanced from fairly simple virus writing to more clever attacks, sometimes using more than one attack mechanism. These range from elaborate note phishing scams…;fraudulent spam that launches viruses or spyware; and malware such as Trojans, which

enable criminals to take remote control over thousands of computers for massive, distributed attacks.'

Equally, there are law enforcement representatives and/or reports drawing upon law enforcement assertions which support the notion of traditional organised crime involvement in cybercrime. In 2001 the FBI announced[86] that ongoing computer hacking by organized crime groups in Russia and the Ukraine had resulted in more than 1 million stolen credit card numbers. McCafferty suggested[87] that '[o]rganized criminals work together, with clearly defined roles. The execution is as finely crafted as the best of business plans. The capital investment is staggering.' In support of this assertion McCafferty[88] cited the example of Kansas based company, Lexitrans. Officials there were indicted in February 2004 after allegedly running a shell-company operation to market adult websites and 900 numbers that advertised for free trials but instead charged the unwary user. The illegal business generated US $750 million and Lexitrans and its shell companies were linked to the Gambino crime family.

Fisher[89] has argued, on the basis of information relayed by Larkin of the Cyber Initiative and Resource Fusion Unit (FBI), that organised crime groups range from '…so-called traditional organized crime groups, such as the Russian and Eastern European mafia, to loosely affiliated crews who pool their resources and skills in online forums.' Neate[90] (the e-crime liaison for the United Kingdom's Serious Organised Crime Agency - SOCA) noted in 2006 that '[organized crime] has changed. [There is] still…traditional organized crime, but now they have learned to compromise employees and contractors. [They are] new-age, maybe have computer degrees and are enterprising themselves. They have a wide circle of associates and new structures.'

Horn[91] argues that '[c]yber crime is rapidly evolving from the domain of misguided pranksters, to elaborate, profit-driven schemes involving organized-crime syndicates that may be based around the block, or halfway around the world.' Hynds[92], formerly of the United Kingdom's National High Tech Crime Unit (recently absorbed into SOCA) argued in 2002 that '[w]e now have reliable intelligence showing major drugs and arms traffickers using sophisticated and disciplined methods of communication using internet relay chat and ICQ (I seek you) protocols as well as encrypted emails.' He suggested[93] that in addition '[w]e are also seeing these groups using hacking skills to access and compromise IT systems, in order to secrete their illicit material on the servers of unsuspecting businesses.'

APACS[94] has argued that '[t]he primary threat to UK e-banking services has come from eastern European crime gangs…[which] have managed to meld their criminal skills along with the technology skills of a ready pool of highly educated IT professionals to find ways of developing many criminal business streams from the internet.' In an indication of increasing mastery over the transition from syntactic (targeting the computer) to semantic (targeting the

computer user) attacks, the use of people to transfer drugs and/or money, a long standing practice of the criminal fraternity, is being replicated in the cybercrime environment. 'Money mules' (ostensibly innocent people unrelated to the criminal activity that creates the illicit funds) transfer relatively small amounts of money lodged in their bank accounts to overseas accounts held by criminals. Money mules are a consequence of the need for criminals to transfer, and disguise the origins of, illicit proceeds of crime. Money mules seem to be recruited largely from the US, UK and Australia and transfer illegal funds to criminals located primarily, in the former Soviet Union[95].

Conclusion

There are undoubtedly criminal elements (known colloquially as 'super-empowered criminals') operating in the online environment as obtainers and disseminators of identity and identity-related information. Operation Firewall[96], for example, in 2004 in the US and Canada culminated in the arrest of 28 people from six countries for offences including the buying and selling of 1.7 million credit card numbers. Such groups may be typified as criminal individuals and/or groups online who are organised rather than traditional organised crime groups who are online. It seems certain, however, that traditional organised crime groups are nevertheless prepared to pay for such information in order to facilitate the commission of physical rather than virtual crimes. However, it remains unclear, and indeed doubtful, whether currently there are traditional organised crime groups operating within the cyber environment. Equally, it seems likely that traditional organised crime groups will not shy away from using the cyber environment to facilitate the operation, and / or to disguise the illicit proceeds, of physical world-based crimes. The use, for example, of denial of service attacks to pursue extortion, of online banking to transfer laundered funds and the use of malware and/or botnet operators to acquire pertinent personal information for use in identity related financial crime is likely to continue to develop. The wholesale or partial mutation of traditional organised crime groups into fully-fledged cybercriminals will ultimately be determined as much by the diminished profitability, or increased risk, of real world criminal activities as it will by the innate attractiveness and relatively low risk of virtual criminality.

References

[1] Research Analyst in Transnational Crime, Australian Institute of Criminology

[2] Question posed at Interpol's Fourth Cybercrime Conference, 2000 cited in Brenner, S (2002), Organized cybercrime? How cyberspace may affect the structure of criminal relationships, North Carolina Journal of Law & Technology (4:1)

[3] Yar, Majid (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory, *European Journal of Criminology* (2:4), 407-427:408

[4] Grabosky, P.N. (2001). Virtual criminality: Old wine in new bottles?, Social and Legal Studies (10:2), 243-249:243

[5] Nisbett, C (2002). New directions in cyber-crime, White Paper, QineticQ, http://www.qinetiq.com/home/security/information_and_network_security/white_paper_index.Par.0012.File.pdf

[6] Wall, D.S.(2004). The internet as a conduit for criminal activity, Chapter 4:77 in A. Pattavina (ed) *Information Technology and the Criminal Justice System*, Sage

[7] IBM (2006). *IBM B2B security survey: Australia/Global Summary Report* (provided to author by IBM)

[8] Article 2 (a) of the UN Convention Against Transnational Organized Crime defines an 'organised criminal group' as 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 [the] Convention, in order to obtain, directly or indirectly, a financial or other material benefit.'

[9] Council of Europe (2004). *Organised crime situation report: Focus on the threat of cybercrime*, http://www.coe.int/T/E/Legal_Affairs/Legal_co-operation/Combating_economic_crime/8_Organised_crime/Documents/Organised%20Crime%20Situation%20Report%202004.pdf

[10] Cited in Naylor, R.T. (2000). *Expert panel on emerging crimes*:4, Research and Statistics Division, Department of Justice, http://www.justice.gc.ca/en/ps/rs/rep/2002/expertpanel.pdf

[11] Cited in McMillan, R (2006). *FBI: Cybercriminals taking clues from Mafia*, www.pcworld.com/article/id, 126664-c,cybercrime/article.html

[12] Ibid

[13] Cited in Wired News (2006), *Cybercrime is getting organized*, http://www.wired.com/news/technology/internet/0,71793-0.html?tw=rss.index

[14] Cited in Thomson, I (2003). *NHTCU issues stark cyber-crime warning*, http://www.managementconsultancy.co.uk/vnunet/news/2122171/nhtcu-issues-stark-c

[15] Nisbett, op. cit

[16] U.S. Congress (1951). Special Committee on Organized Crime in Interstate Commerce

[17] U.S. Congress (1963). Senate Permanent Subcommittee on Investigations of the Committee on Government Operations

[18] A meeting of crime Bosses at the home of Joseph Barbara in Appalachian, New York, in 1957

[19] UN Commission on Crime Prevention and Criminal Justice (2001). *Conclusions of the study on effective measures to prevent and control high-technology and computer-related crime*, 10th Session, 8-17 May, http://www.unodc.org/pdf/crime/10_commission/4e.pdf

[20] Davis, R and Pease, K (2001). Crime, technology and the future, *Security Journal*, 59-61, Perpetuity Press Ltd.

[21] Naylor, op.cit

[22] Ibid: 4

[23] Zittrain, J.L. (2006). The generative internet, Harvard Law Review (119:7), http://www.harvardlawreview.org/issues/119/may06/may06.shtml

[24] Sussman, M.A. (1999). The critical challenges from international high-tech and computer-related crime at the millennium, *Duke Journal of Comparative and International Law* (9:451-489):451

[25] Miller, R, Michalski, W and Stevens, B (1998). The promises and perils of 21st century technology: An overview of the issues, in, 21st century technologies: Promises and perils of a dynamic future, OECD

[26] Symantec (2006). Symantec internet security threat report: Trends for January 06 – June 06, http://www.symantec.com/specprog/threatreport/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf

[27] Symantec (2006). *Cybercrime: A disturbing trend* http://www.symantec.com/home_homeoffice/library/article.jsp?aid=cybercrime_a_disturbing_trend

[28] CipherTrust (2005). Phishing: Organized crime for the 21st century, www.ciphertust.com

[29] UN Commission on Crime Prevention and Criminal Justice (2001), op.cit

[30] Morris, S (2004). The future of netcrime now: Part 1 – threats and challenges, Home Office

[31] Millman, R (2005). *IT managers fail to protect mobile devices*, SC Magazine, 11 November, http://www.scmagazine.com/asia/news/article/527520/it-managers-fail-protect-mobile-devices/

[32] Brenner, op.cit:

[33] Ibid: 24

[34] Nisbett, op.cit

[35] Brenner, op.cit

[36] Ibid: 24

[37] Nisbett, op. cit

[38] Ibid

[39] Cressey, D.R. (1969). *Theft of a nation: The structure and operations of organized crime in America,* New York: Harper & Row

[40] Joseph Valachi, a mafia member, testified before the McClellan Committee (n.17 supra). Details of his life may be found in Maas, P (1968), *The Valachi papers*, New York: G.P. Putnam

[41] United Nations Office on Drugs and Crime (2002). *Results of a pilot study of forty selected organized crime groups in sixteen countries*, www.unodc.org/pdf/crime/publications/Pilot_survey.pdf

[42] Nisbett, op.cit

[43] Olson, J.L. (2004). *The threat of systematic and organized cybercrime and information warfare*: 17 http://www.american.edu/traccc/resources/publications/students/olson01.pdf

[44] Europol (2006). *Organised Crime Threat Assessment 2006*: 18 http://www.europol.europa.eu/publications/OCTA/OCTA2006.pdf

[45] McAfee (2006). *McAfee virtual criminology report: Organised crime and the internet*, http://www.softmart.com/mcafee/docs/McAfee%20NA%20Virtual%20Criminology%20Report.pdf

[46] William, P (2001). Organized crime and cybercrime: Synergies, trends and responses, *Global Issues* (6:2):25, US Department of State, http://usinfo.state.gov/journals/itgic/0801/ijge/ijge0801.pdf

[47] Clarberg, B (2003). *Cyber crime*, Paper presented at the conference on international cooperation on transnational crime, The Hague, 9-10 October (unpublished)

[48] See, for example, McCusker, R (2006) Organised crime and terrorism: Convergence or separation?, ECPR Standing group on organised crime newsletter (5:2) 2-5 http://www.essex.ac.uk/ecpr/standinggroups/crime/documents/SGOC_Vol5_2.pdf

[49] Olson, op.cit: 15

[50] Ibid:16

[51] Nisbett, op.cit

[52] Brenner, op.cit: 39

[53] Council of Europe (2005). *Organised crime situation report: Focus on the threat of economic crime,* http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/8_Organised_crime/Documents/Report2005E.pdf

[54] Brenner, op. cit: 45

[55] Ibid

[56] Ibid: 47

[57] Clarberg: op.cit

[58] Williams, op.cit: 23

[59] Grabosky, op.cit

[60] See 'Introduction' at p.1 supra

[61] Williams, op.cit: 22

[62] Ibid

[63] Council of Europe (2004), op.cit: 169

[64] Cited in Williams (2001), op.cit: 23

[65] Morris, op.cit: 28

[66] Parizo, E.B. (2005). *Busted: The inside story of 'Operation Firewall'*, Security.com, http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1146949,00.html

[67] Cited in Parizo, op.cit

[68] Council of Europe, op.cit: 118

[69] Ibid: 119

[70] Ibid: 121

[71] Europol, op.cit: 18

[72] Criminal Intelligence Service of Canada (2005). http://www.cisc.gc.ca/annual_reports/annual_report2005/document/annual_report_2005_e.pdf :15

[73] Drug Enforcement Administration, Federal Bureau of Investigation and Royal Canadian Mounted Police (2006). *2006 Canada/US organized crime threat assessment*, http://www.psepc.gc.ca/prg/le/_fl/2006_Canada-US_OC-TA_en.pdf

[74] Ibid: 13

[75] Ibid: 5

[76] Criminal Intelligence Service of Canada (2005). 2005 Annual report on organized crime in Canada: 13, http://www.cisc.gc.ca/annual_reports/annual_report2005/document/annual_report_2005_e.pdf

[77] Criminal Intelligence Service of Canada (2006), op.cit: 9

[78] Europol, op.cit: 18

[79] Serious Organised Crime Agency (2006). The United Kingdom threat assessment of serious organised crime 2006/7: 23 http://www.soca.gov.uk/assessPublications/downloads/threat_assess_unclass_250706.pdf

[80] Hynds, L (2005). *Organized crime offers rent-a-zombie deals*, http://www.spamdailynews.com/publish/Organized_crime_offers_rent-a-zombie_deals.asp

[81] Financial Action Task Force (2006). *Report on new payment methods*, http://www.fatf-gafi.org/dataoecd/30/47/37627240.pdf

[82] Kubic, T.T. (2001). *The FBI's perspective on the cyber crime problem*, Testimony before the House Committee on the Judiciary, Subcommittee on Crime, www.fbi.gov/congress/congress01/kubic061201.htm

[83] Griffiths, P (2006). *Internet gangs hiring students for cybercrime*, www.nzherald.co.nz/section/3/story.cfm?c_id=3&objectid=10414819

[84] McAfee (2006) op.cit

[85] Stone, G (2005). *Microsoft partners with Australian law enforcement agencies to combat cyber crime*, Microsoft press release, http://www.ahtcc.gov.au/__data/assets/pdf_file/13952/MR050330_ForensicWorkshop.pdf ,

[86] CNN (2001). *FBI warns companies about Russian hacker attacks*, http://archives.cnn.com/2001/TECH/internet/03/08/hacker.attacks/index.html

[87] McCafferty, D (2004). *Organized cyber crime*, www.thewhir.com/features/organized-cybercrime.cfm

[88] ibid

[89] Fisher, D (2006). *Feds court infosec pros in fight against cybercrime*, http://searchsecurity.techtarget.com.au/topics/article.asp?DocID=1207228

[90] Cited in Ilett, D (2006). *Mafia insiders infiltrating firms, U.K. cops warn*, http://news.com.com/Mafia+insiders+infiltrating+firms%2C+U.K.+cops+warn/2100-7348_3-6064954.html?tag=mainstry

[91] Horn, P (2006). *It's time to arrest cyber crime*,

[92] Cited in Thomson, I (2002). *Organised crime goes digital*, http://www.crime-research.org/news/2002/12/Mess1201.htm

[93] Ibid

[94] Association for Payment Clearing Services (2006). *A vulnerability and threat assessment of authentication mechanisms for internet based financial services: 2006 review*, London

[95] McCusker, R (2007). The ultimate work at home scam, *Money Laundering Intelligence (14)*

[96] McAfee (2005). *McAfee virtual criminology report: North American study into organized crime and the internet*, http://www.mcafee.com/us/local_content/misc/mcafee_na_virtual_criminology_report.pdf