Asian Criminology (2008) 3:37–59
DOI 10.1007/s11417-007-9035-y

Criminal Exploitation of Online Systems by Organised Crime Groups

Kim-Kwang Raymond Choo · Russell G. Smith

Received: 24 August 2007 / Accepted: 8 October 2007 /
Published online: 15 November 2007

Abstract This article considers how information and communications technologies (ICT) can be used by organised crime groups to infringe legal and regulatory controls. Three categories of groups are identified: traditional organised criminal groups which make use of ICT to enhance their terrestrial criminal activities; organised cybercriminal groups which operate exclusively online; and organised groups of ideologically and politically motivated individuals who make use of ICT to facilitate their criminal conduct. The activities of each group are then assessed in relation to five areas of risk: the use of online payment systems, online auctions, online gaming, social networking sites and blogs. It is concluded that the distinction between traditional organised crime groups and the other two groups—cybercriminal groups and ideologically/politically motivated cyber groups—is converging, with financially-motivated attacks becoming more targeted. Legislation will need to adapt to deal with new technological developments and threats that organised criminals seek to exploit.

Keywords Organised cybercriminal groups · Online payment · Online auction · Online gaming · Social networking sites · Blogs · Ideologically motivated cyber groups · Politically motivated cyber groups · Cybercriminal groups

Introduction

Digital content (or electronically stored information) can be broadly defined as information or data extracted from a computer or other electronic storage medium. A 2003 study reported that information is increasingly being stored or archived in electronic form—approximately 92% of data were created in electronic-only form, particularly on hard disks (Lyman and Varian 2003). Another report indicated that the amount of digital information created, captured and replicated in 2006 was approximately 161 billion gigabytes (Gantz et al. 2007),

This research paper does not necessarily reflect the policy position of the Australian Government or the Australian Institute of Criminology (AIC).

K.-K. R. Choo (✉) · R. G. Smith
Australian Institute of Criminology, GPO Box 2944, Canberra ACT 2601, Australia
e-mail: Raymond.choo@aic.gov.au

R. G. Smith
e-mail: russell.smith@aic.gov.au

or to put this into perspective, the equivalent of 230 billion standard 700-megabyte CDs or 37 billion standard 4.3-gigabyte DVDs.

Broadband connection, technological innovations and the declining cost of electronic data storage devices continue to lower entry barriers for digitisation of information, which will continue to have a wide-ranging influence on how the banking and finance industry operates. This includes customer service (e.g. electronic payment systems) and business operations (e.g. electronic clearing).

The declining importance of dial-up connections and the expansion of broadband services have also created an environment in which connections are maintained continually. Investment in network expansion by telecommunications companies will see a further expansion in capacity that will result in an increase in bandwidth availability and greater adoption of wireless and mobile technologies. Although Asia represents about 56.5% of the world population, only about 10.7% of its population has access to the internet as of March 2007 (World internet usage and population statistics 2007). This, however, represents just over one-third of the world's current population with access to the internet and is thus a highly significant market. In addition, although English remains the dominant language, Asian languages (i.e. Chinese, Japanese and Korean) constitute least 25% of online use as described in Table 1.

As businesses continue to engage in electronic commerce, they will become increasingly globalised and interconnected. Australia has experienced a considerable increase in electronic banking (APCA 2005). This is perhaps due to the cost of an internet-based transaction being a small fraction of a 'bricks-and-mortar' based transaction. The propensity for consumers to buy online is indicated in a recent report that online spending on retail websites in United States has exceeded US$100 billion (Ames 2007).

Ease in accessing and sharing content electronically offers governments and businesses the opportunity to engage the public online and to bridge the gap between sectors. The

Table 1 Top ten languages used in the web

Top ten languages in the internet	% of all internet users	Number of internet users by language	Internet penetration and by language	Internet growth % for language (2000–2007)	2007 estimate world population for the language
English	30	328,666,386	29	140	1,143,218,916
Chinese	14	159,001,513	12	392	1,351,737,925
Spanish	8	88,920,232	20	260	439,284,783
Japanese	8	86,300,000	67	83	128,646,345
German	5	58,711,687	61	113	96,025,053
French	5	55,521,294	14	355	387,820,873
Portuguese	4	40,216,760	17	431	234,099,347
Korean	3	34,120,000	46	79	74,811,368
Italian	3	30,763,940	52	133	59,546,696
Arabic	3	28,540,700	8	932	340,548,157
Top ten languages	82	910,762,512	21	181	4,255,739,462
Rest of World Languages	18	203,511,914	9	445	2,318,926,955
World total	**100**	1,114,274,426	17	209	6,574,666,417

Internet usage and world population statistics at 10 March 2007. Source: adapted from http://www.internetworldstats.com/stats7.htm

emerging trend of individuals using the internet to access public-domain services in preference to more traditional offline modes will increase the popularity of digital content in e-commerce, e-government and social activities such as e-tendering, e-reporting and e-voting (e.g. the *Parliamentary Elections (Amendment) Act 2001* (Cap. 218) was passed by the Parliament of Singapore on 20 April 2001 to allow e-voting in Singapore).

With the ease of accessing and sharing content electronically, the key issue to consider in this article is whether crime follows opportunity, particularly criminal exploitation of online payments, auctions, gaming, social networking sites and blogs? The next section discusses three categories of organised crime groups. Risks associated with online payments, auctions, gaming, social networking sites and blogs are then examined (e.g. how can these be exploited by organised crime groups to 'develop' new crimes and 'cleverly transform' traditional crimes). Examples of 'cleverly transformed' traditional crimes include abusing online payment systems to facilitate money laundering activities and using the internet as a distributor of computer-based images of child abuse and child pornography. It is also possible to disseminate video coverage of sexual abuse in real time. The last section concludes this article.

Organised Crime Groups

The definition of "organised criminal group" from Article 2 of the UN Convention on Transnational Organized Crime is adopted in this article:

> a group having at least three members, taking some action in concert (i.e. together or in some co-ordinated manner) for the purpose of committing a 'serious crime' and for the purpose of obtaining a financial or other benefit. The group must have some internal organization or structure, and exist for some period of time before or after the actual commission of the offence(s) involved.

Traditional Organised Criminal Groups

Organised crime is not a new phenomenon. It preceded, and then accompanied, the rise of the modern state. Pursuit of financial gain has always been the driving force behind traditional organised crime. This motivation has been explained through the use of a number of theoretical models. One, for example, is Bandura's (1999) social cognitive theory of behaviour. This argues that behaviour, first acquired vicariously through exposure to social models, is dependent on, and shaped by, positive reinforcement arising from different combinations of fundamental human incentives—money, power, status and sensory needs.

Traditional organised criminal groups (e.g. Japanese Yakuza and Asian triads) have recognised the value of leveraging information and communication technologies (ICT) to facilitate or enhance the commission of crimes. Examples include: using ICT to facilitate drug trafficking; trafficking corporate secrets and identity information; committing extortion, frauds and scams online; money laundering using online payment systems; and distributing illegal materials over the internet. The involvement of traditional organised criminal groups in technology-enabled crime now emphasises the importance of large-scale profit-driven incentives.

Examples of traditional organised criminal groups involved in technology-enabled crime include the highly structured and global criminal syndicates such as the Asian triads and Japanese Yakuza, whose criminal activities have been known to include computer software

piracy and credit card forgery and fraud (Canadian Security Intelligence Service 2000; OECD 2007; Inside the Yamaguchi-gumi: Ex-gangster's life a history of Japan's postwar underworld 2006). A more recent incident involves the arrest of 12 members of a piracy syndicate in China for copyright infringement offences (Raid of a major pirate packaging facility in Guangzhou 2007). A recent report noted that:

> Harco Glodok (Jakarta, Indonesia) [is] one of the largest markets for counterfeit and pirated goods, particularly well-known for pirated optical discs. Enforcement officials are reportedly reluctant to conduct regular enforcement actions because of the presence of organized criminal gangs (Office of the United States Trade Representative 2007: p. 8)

Traditional organised criminal groups from Eastern Europe have also been known to carry out extortion from online gambling and pornography websites by threatening to carry out denial-of-service attacks using botnets (Kshetri 2005; Schrank 2007). In January 2007, two Dutch members of a hacking ring were sentenced to imprisonment for their alleged roles in extortion of a company in the United States, stealing identities to purchase cameras and games consoles, and distributing bot malware. Four others facing lesser charges are currently awaiting trial (Libbenga and Leyden 2007). In recent years, organised criminal groups have been reported to recruit 'a new generation of high-flying cybercriminals using tactics which echo those employed by the KGB to recruit operatives at the height of the cold war' (McAfee 2006: p. 2). This should come as no surprise to long-time political observers. In countries such as Russia, the lack of economic and employment opportunities have forced many highly educated individuals with advanced computer and programming skills to work in the cyber underground.

Organised Cybercriminal Groups

Another category of organised criminal group comprises like-minded individuals, who usually know each other only online but are involved in an organisational structure working collectively towards a common goal, as the internet makes it far easier to meet and plan activities. Although the objective is usually pursuit of financial gain, it can include other criminal goals such as producing and disseminating child exploitation materials (e.g. online paedophile rings). For example, a recent case involved three men in the United Kingdom who had never met in person and knew each other only online. All three were convicted at London's Southwark Crown Court of a conspiracy to rape a girl under 16, based on a discussion in an internet chat room (GB CPS 2006). In a separate incident, more than 700 suspects associated with the online paedophile ring operating the UK-based Internet chatroom, "Kids, the Light of Our Lives", were arrested worldwide (UK CEOP 2007).

Despite the synergy between traditional organised criminal groups and cyberspace, such groups should not be confused with organised cybercriminal groups. As Eugene Kaspersky, the founder and head of research and development of the Russian anti-virus Kaspersky Lab, observed:

> IT criminals are just IT people who change their mind, or have a broken mind. It seems that traditional criminals are quite far away from that. IT criminals don't see their victims, so it's easier for them to do it, because they don't feel their hand in someone else's pocket (Interview: Eugene Kaspersky 2007)

Moreover, the organisational structure of the organised cybercriminal group differs significantly from a traditional organised criminal group, as the former is more likely to entail circumstances in which individual members coalesce for a limited period of time to

conduct a specifically defined task or set of tasks and, having succeeded, go their separate ways. Organised cybercriminal groups are also more loosely structured and flexible, transnational and tend to have smaller membership sizes. Brenner explains this as follow:

> physical strength is insignificant [in the cyberworld]; a hacker surmounts a victim's defenses, not by summoning combined efforts of ten or twenty hackers, but by using technology, automated techniques that enable one to bypass electronic defenses. In the cyberworld, strength is in software, not in numbers of individuals (Brenner 2002: p. 27)

Individuals in organised cybercriminal groups are likely to be more technically sophisticated. For example, the leader of the five-member computer hacker group arrested in 2001 was a former computer programmer at a Moscow institute (Russia arrests 'grandfather of cybercrime' 2001). In a more recent case involving the arrest of a credit card skimming syndicate in Singapore, two of the six-member syndicate were University undergraduates (Singapore Commercial Affairs Department 2007). Moreover, to circumvent access control technological protection measures in today's commercial software, one would need advanced technical knowledge and the ability to manufacture circumvention devices for such technological protection measures. Individual members of organised hacker groups such as cnxhacker and milw0rm have and will continue to publicise vulnerabilities they discover, to write exploit code, and to develop sophisticated hacking techniques. Studies by Kshetri (2006) and Jen, Chang and Chou (2006) indicated that a sizeable percentage of cybercriminals in Russia and Taiwan belong to the educated generation Y group.

Organised criminal groups have been reportedly building their own encrypted instant-message (IM) program, CarderIM, designed to sell stolen financial and personal information including credit card numbers and e-mail addresses (Kirk 2007b). Several cases of organised hacking groups stealing credit card information have also been reported (e.g. FBI warns of Eastern European hacker groups 2001). In a more recent incident, a hacker group allegedly involved in stealing credit card data from TJX were "selling it on the Internet on password-protected sites used by gangs who then run up charges using fake cards printed with the numbers" (Pereira 2007). Such stolen credit card data can then be used to make fraudulent purchases (e.g. PP VS Kelvin Leong Jia Wen and Lim Xiang Rui as cited in Singapore Commercial Affairs Department 2006a: p. 24). In May 2007, a Calgary man was arrested for allegedly using the internet to sell concealed devices designed to illegally capture data from bank ATM users (van Rassel 2007)[1]. Although there are no known published statistics involving monthly subscription-based services for malware updates being offered at such underground sites, it is likely that such services will become increasingly popular.

Symantec (2007a) highlighted the emerging trend of underground markets for a wide variety of commodities. The report indicated the main locations of servers hosting such underground markets, with 58% located in North America and 39% in Western Europe, as might be expected in countries with extensive computer infrastructure (see Fig. 1). Asia is conspicuous by its absence.

Other examples of known organised cybercriminal groups include

- 'Shadowcrew': an underground criminal group that trafficked more than 1.7 million credit cards online (USSS 2004; US DoJ 2004)

[1] Such incidents can be perpetrated by both groups (as defined under Article 2 of the UN Convention on Transnational Organized Crime) or by one or more individuals as illustrated in this example.

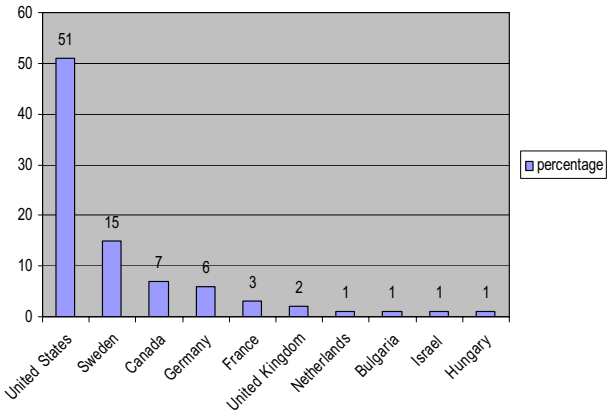

Fig. 1 Location of underground market servers (%). Source: Adapted from (Symantec 2007c): Fig. 2

- 'DrinkOrDie': an underground software piracy group (US DoJ 2007d; US DoJ 2007e)
- The 'Rock-Phish' gang: an underground phishing group identified in a recent research by researchers from the University of Cambridge (Moore and Clayton 2007)
- The 'M00P virus-writing gang': three suspected members of the gang were arrested by the Metropolitan Police Computer Crime Unit, the Finnish National Bureau of Investigation and the Finnish Pori Police Department, in connection with a conspiracy to infect computers with malware to create a botnet (Jaques 2006)
- The 'botmaster underground': a member of the group, pleaded guilty to computer fraud and spam offences connected to his dealings in botnets. The offender created new variants of the 'rxbot' robot family.11 and distributed these variants to establish several botnets. The botnets were then hired out to others for the purposes of sending spam and launching DDoS attacks, thus generating thousands of dollars of income. It was also alleged that the botnets were used to generate income from the surreptitious installation of adware on the zombies. In May 2006, the offender was sentenced to 57 months in federal prison (US DoJ 2006b)
- The 'Mpack' gang that was allegedly behind the cyberattack that had successfully compromised the homepages of hundreds of legitimate Italian websites (Symantec 2007b). The MPack toolkit is allegedly being sold for US$700 (PandaLabs 2007).

Organised Ideologically and Politically Motivated Cyber Groups

Prior to 11 September 2001, terrorism and organised crime were usually considered separate entities because they did not share the same motivating factor (e.g. making a political statement vs profit). In recent years, there has been a noted convergence between terrorism and organised crime (McCusker 2006), According to Warren (as cited in Charlton 2005) "Al Qaeda has turned to organi[s]ed crime groups for their money laundering expertise". Crimes commonly associated with organised criminal groups (e.g. scam and fraud schemes, identity and immigration crimes, the counterfeit of goods, and illegal weapons procurement) are also precursor crimes used by terrorist groups to raise funds (e.g. Tigers have joined jihadi drug trade, says official 2007). Moreover,

> [c]riminal organizations can become ideological over time. In South Asia, they seem to have acquired ideological or religious predispositions that motivate, not merely cover, their actions. And they have increasingly become involved in supporting

> terrorist activities. Terrorist groups rely upon organized crime for the weaponry and munitions they require for terrorist attacks and insurgencies. To transport these goods, they use routes that have been carefully constructed by the criminal gangs, who in return seek from the terrorist groups training in the use of guns and explosives and safe passage (for a price) through militant territory. The two groups are further connected by the drug trade: both are financially dependent on narcotrafficking (Lal 2005: p. 294)

Terrorist groups have been known to obtain information on and acquire chemical, biological and radiological materials via the internet, which increases the risk of terrorist groups possessing sufficient fissile material to develop their own nuclear weapon. The use of global telecommunications technologies can also be used to mount attacks against key critical infrastructures. The diffusion of information on the internet regarding dual-use research of concern has compounded this challenge. In July 2006, Faheem Khalid Lodhi was convicted of offences including plotting in October 2003 to bomb Australia's national electricity grid in the cause of violent jihad. It was alleged that Lodhi had downloaded information, including electricity grid maps, from the internet. Lodhi was sentenced to 20 years in prison on 23 August 2006 (Regina v Lodhi [2006] NSWSC 691 23 August 2006). In 2007, it was reported that terrorists might have used information obtained from Google Earth™ to facilitate their planning of (physical) attacks against British troops in Iraq.

> Documents seized during raids on the homes of insurgents last week uncovered printouts from photographs taken from Google™. The satellite photographs show in detail the buildings inside the bases and vulnerable areas such as tented accommodation, lavatory blocks and where lightly armoured Land Rovers are parked (Harding 2007).

Members of terrorist groups include engineers and computer scientists (US NSTC 2006: p. 7) and they have been known to use the internet as a medium for propaganda (e.g. publishing doctrines such as "The Global Islamic Resistance Call" on the internet), recruitment and training of potential terrorists, and transferring information.

In March 2007, Singapore's Deputy Prime Minister and Minister of Home Affairs told Parliament that the Internal Security Department of Singapore investigated internet-driven radicalisation cases involving "Singaporeans who had become attracted to terrorist and radical ideas purveyed in the mass media, particularly the Internet" (Ahmad 2007). Internet-driven radicalisation includes cases of radical youths and other individuals linking up with like-minded people and making contact with extremists from overseas involved in terrorist recruitment and financing over the internet in chat rooms, blogs and social networking sites (see also Wee 2007). A recent article reported that there are about 6,000 websites espousing radical ideologies, such as hosting heavy philosophical and religious discussions and combining religious songs and war images to drum up support for militant jihad (Bahrawi 2007a).

A recent example of how the internet has been used in terrorist planning activities includes the following case that has been brought before the district court of Connecticut in the United States. The indictment alleged that:

> from approximately 1997 through at least August 2004, British nationals Babar Ahmad, Syed Talha Ahsan, and others, through an organization based in London called Azzam Publications, are alleged to have conspired to provide material support and resources to persons engaged in acts of terrorism through the creation and use of various internet Web sites, e-mail communications, and other means. One of the means Ahmad and his co-conspirators are alleged to have used in this effort was the

> management of various Azzam Publications websites, principally www.azzam.com, which, along with associated administrative email accounts, were hosted for a period of time on the servers of a Web hosting company located in the state of Connecticut (US DoJ 2007f).

Politically-motivated hacker groups (hacktivists) have also carried out hacktivism activities such as bringing down government agencies' websites and engaging in information warfare.

> A well-known cyberwar between Chinese and American hackers erupted in April 2001 following the collision of a U.S. military spy plane and Chinese fighter. U.S. government Web sites were hacked and defaced with slogans such as "Beat down imperialism of American," courtesy of a group calling itself the Honker Union of China (Kirk 2007c)

> A recent series of cyberattacks directed against targets in Taiwan and the United States may confirm that "those fears now appear justified," says a Taiwanese intelligence officer. Taiwan and China regularly engage in low-level information-warfare attacks. But the past few months have seen a noticeable spike in activity. "'Blitz' is an accurate description" of the recent attacks, says the Taiwanese security source. "It's almost like . . . a major cyberwar exercise." (Curry and McGrane 2006: p. 93)

Other recent hacktivism activities include the 2006 defacing of Danish websites by Islamic hackers protesting controversial cartoons mocking the Prophet Muhammad (Ward 2006) and the denial-of-service attacks on several Estonian government websites in April 2007 (Kirk 2007a; Rodriguez 2007). Known politically-motivated hacker groups include 'Hacker Union for China' and 'ChinaHonker.com'.

In the sections that follow, the activities of each group are assessed in relation to the risk areas identified.

Online Payments

Online payment systems can be broadly categorised as follows (AIC 2007):

- *Software-based or hardware-based*: The former, implemented in software-only form includes virtual currency used in massively multiplayer online games. Hardware-based money (or card money) includes bank-driven and bank-backed key stored value systems such as Mondex, NETS cashcard and NTT's NCash.
- *Online-based or offline-based schemes* (based on the type of payment validation): In the former (e.g. BPay), issuing banks have to be contacted at the point of purchase to provide authorisation when payments are made. Offline-based schemes provide offline authorisation capability where validation is made based on information contained on the card (e.g. pre-paid cards including Mondex, NETS cashcard and NTT's NCash).
- *Picopayment systems, micropayment systems or macropayment systems* (depending on the dollar amount of transactions): Requirements for these systems differ. Picopayment and micropayment systems typically require efficiency, low-cost and security. Due to the larger amount of transactions involved, macropayment systems typically require higher levels of security and non-repudiation of transactions.

An increased dependence on global electronic payment systems and the ability to move large amounts of money expeditiously across different jurisdictions expose both payment processing companies (payment bureaus) and consumers to an evolving spectrum of threats

such as fraud and money laundering. In June 2007, Omar Zieba, an alleged member of an organised cybercriminal group, was charged with conspiracy to defraud by hacking into 30 ATMs in Sydney and Melbourne so that AUD$20 or AUD$50 notes would be dispensed for every dollar withdrawn (Frith 2007).

In money laundering cases, the proceeds of crime can be placed into financial systems by purchasing electronic currency or digital precious metals. To disguise the origins of the illicit proceeds, criminals can perform a series of business transactions (e.g. transferring electronic currency through a series of offshore companies and the purchase of goods for resale) prior to integrating the 'cleaned' proceeds. For example, in the recent case involving the arrest of four Russians, it was noted that:

> [they] then transfer the fraudulently-obtained money and goods back to Russia. ... Using stolen identity and credit information, defendant CHUGAEV made on-line purchases of PayPal cards, gift cards, computers, and other merchandise, and requested that the items be shipped to United States addresses under the control of his associates. Those associates quickly withdrew cash from the credit cards, then deposited the cash into bank accounts, and allowed CHUGAEV to withdraw the stolen money in Russia using ATM cards associated with the bank accounts. The computers and other merchandise were repackaged by CHUGAEV's associates in the United States and mailed on to Russia, where the stolen goods were resold (US DoJ 2007b).

Organised criminal groups (including traditional organised criminal groups) have also been known to hire money mules in the money laundering process. For example, a criminal syndicate allegedly set up a website (www.fias.sg) that resembles the Foreign Investment Advisory Service website (www.fias.net). Money mules were recruited to launder money originating from frauds committed in Australia using remittance companies and telegraphic transfer. Thirteen Singaporeans were arrested for allegedly wiring a total amount of S $278,270.80 to Russia or Latvia and collecting a commission based on the amount of money laundered. These money mules reportedly earned a total of S$42,378 in commission (Singapore Commercial Affairs Department 2006b). Fig. 2 describes the basic three-stage money laundering process[2].

The following are examples of common online payment systems.

Smartcards and Prepaid Cards

Smartcards and prepaid cards, which have been adopted in countries worldwide, are typically used for micropayments in view of their limited storage capacity. In October 2006, a trial of the contactless Europay, MasterCard and Visa standards consortium (EMV) debit cards was conducted by the Royal Bank of Scotland. The NETS cashcard is also currently used in Singapore. The cashcard can be used to pay any amount up to a limit of S$500, such as paying for small-value consumer items. The cashcard can be topped up at various places including automated teller machines and designated convenience stores.

The anonymity offered by prepaid cards could be abused by organised crime groups and terrorist groups for illicit financial transactions, money laundering and bulk cash smuggling particularly as value limits increase. In March 2007, a six-member syndicate was arrested by the

[2] In Australia, money laundering transactions are estimated to be between AUD$2 billion (Institute of Chartered Accountants 2006) and AUD$4.5 billion per year (AGD n/a). The IMF has further suggested that money laundering transactions are equal to approximately two to five percent of the global gross domestic product (GDP).

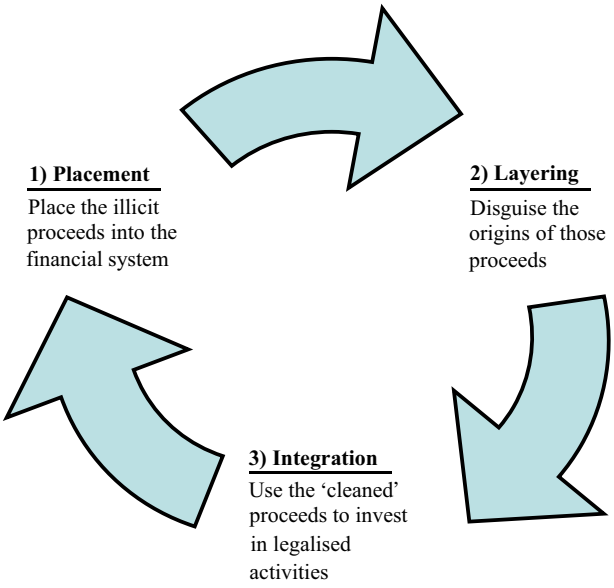

Fig. 2 Basic three-stage money laundering process)

Gainesville Police Department for allegedly using stolen credit cards to purchase large quantities of WAL-MART and Sam's Club gift cards. The purchased cards were then redeemed for merchandise such as computers (US FDLE 2007). In a separate incident, individuals were allegedly recruited by organised crime groups to purchase gift cards using counterfeit credit cards. These credit cards were manufactured using stolen credit card data obtained from the hacking of TJX's database by organised cybercriminal groups (Swartz and Acohid 2007).

A recent case involving Tammy Black, a former employee of the deputy registrar for the Ohio Bureau of Motor Vehicles, demonstrated how prepaid cards can also be used as a means of payment by organised crime groups. Black was charged for her role in selling fraudulent Ohio drivers' licences in 2005. She was reportedly paid using US$10 phone cards (US ICE 2005). A recent report also identified pre-paid cards as a potential tool for organised crime groups to launder drug proceeds (US NDIC 2006).

The future will see organised cybercriminal groups continue to design hardware devices and software programs to compromise the quality of data-protection mechanisms used in electronic purses, electronic wallets, smartcards and prepaid cards. For example, a recent study which examined 20 different RFID-enabled credit cards issued in the United States by Visa, Master Card and American Express observed that:

> ... (1) the cardholder's name and often credit card number and expiration are leaked in plaintext to unauthenticated readers, (2) our homemade device costing around [US] $150 effectively clones one type of skimmed cards-providing a proof-of-concept of the RF replay attack for cards, (3) information revealed by the RFID transmission cross contaminates the security of non-RFID payment media, and (4) RFID-enabled credit cards are susceptible in various degrees to a range of other traditional RFID attacks such as skimming and relaying (Heydt-Benjamin et al. 2007: p. 1).

The feasibility of RFID devices being abused and exploited in attacks against RFID-enabled credit cards offers opportunities for organised crime groups to commit economic crimes with larger payoffs and fewer risks.

Digital Precious Metals

Digital precious metals, a relatively new way of transferring value online, enable users to secure cash deposits against precious metals held offshore. Prior to trading online, users establish online accounts by providing their name, email address and physical address. The required identification, however, can be easily fabricated and some digital precious metals allow users to establish anonymous accounts. Recent examples of e-gold being abused include the arrest of the members of the organised cybercriminal group, Shadowcrew. In October 2004, the United States Secret Service closed an illicit online website that trafficked in at least 1.5 million stolen credit and bank card numbers that resulted in losses in excess of US$4 million. Six Shadowcrew members were eventually charged with conspiracy to commit credit and bank card fraud, as well as identification document fraud. One of the six defendants was also charged with unlawful transfer of identification to facilitate criminal conduct. Several others were also indicted on conspiracy charges (US DoJ 2005).

It was also noted that:

> [p]ersons seeking to use the E Gold payment system were only required to provide a valid email address to open an E Gold account and no other contact information was verified. Once an individual opened an E Gold account, he/she could fund the account using any number of exchangers, which converted national currency into E Gold. Once open and funded, account holders could access their accounts through the Internet and conduct anonymous transactions with other parties anywhere in the world (US DoJ 2007c).

As a result it is likely that such systems will be used to facilitate money laundering and terrorist financing, perhaps with the assistance of an exchange agent such as a shell corporation. On 24 April 2007, two companies operating e-Gold, a digital currency business, and their owners were indicted on charges of money laundering, conspiracy, and operating an unlicensed money transmitting business. It was alleged that the owners of e-Gold allowed e-Gold to conduct fund transfers despite knowing that the money being moved was the result of illegal activity such as credit card and investment fraud and child exploitation (US DoJ 2007c).

Online Auctions

Online auction sites provide buyers and sellers with a global virtual market and storefront to buy and sell a wide range of merchandise through competitive bidding. They constitute one of the most successful internet-based business models. Online auction sites can, however, be abused by organised crime groups to facilitate the traditional ‘transfer-pricing’ money laundering technique—manipulating the purchase or sale price (significantly below and above the actual market price, respectively). For example, a seller inflates the selling price of the merchandise listed on auction sites (e.g. a shipment of computer motherboards worth AUD$1 selling for AUD$10,000 each). *Placement* concludes once the colluding buyer pays the seller with illicit proceeds. *Layering* in this case is performed by the seller as the buyer does not have to worry about disguising the origins of the illicit proceeds. Once the sale has been finalised, the cleaned proceeds can then be invested in legalised activities (*integration*).

Crimes associated with online auctions, particularly online auction frauds, are increasingly becoming more sophisticated. Recent statistics released by NW3C/FBI (2007) indicated that in 2006, 207,492 high tech crime complaints were reported to the Internet Crime Complaint Center. Online auction fraud, the most prevalent offence type, accounted for 44.9% of the 86,279 referred cases to US law enforcement agencies and 33% of the total reported dollar loss.

Examples of criminal exploitation of online auctions include the case involving the arrest of 21 people on December 2006. They were arrested for participating in an international fraud scheme and illegally obtaining more than US$5 million from more than 2,000 victims. The victims who bid unsuccessfully on items were led to believe that they were being given a second chance to purchase items and were instructed over the internet to send money via Western Union to be picked up by the seller or the seller's agent (US DoJ 2006a). In a separate incident, four suspects in Atlanta, United States were indicted on charges of internet fraud charges related to the posting of non-existent items for sale on eBay in 2007. Funds amounting to half a million dollars were then collected from the successful bidders (US DoJ 2007a).

Mariyana Feliksova Lozanova, a Bulgarian member of a transnational criminal group, was arrested on United States charges by law enforcement authorities in Budapest, Hungary. It is alleged that

> Lozanova and others allegedly participated in a scheme to advertise merchandise for sale on the eBay Web site, including expensive motor vehicles and boats. When the U.S. victims expressed interest in the merchandise, they were contacted directly by an email from a purported seller. The victims were then instructed to wire transfer payments through "eBay Secure Traders"–an entity which has no actual affiliation to eBay but was used as a ruse to persuade the victims that they were sending money into a secure escrow account pending delivery and inspection of their purchases. Instead, the victims' funds were allegedly wired directly into one of several bank accounts in Hungary or Slovakia controlled by Lozanova and her co-conspirators (US DoJ 2007h).

Another similar incident involves the arrest of Dov Tenenboim, the leader of an AUD $20,000 internet fraud ring. Tenenboim allegedly 'hacked in to over 90 eBay accounts to sell imaginary goods'. He was ordered to serve eight months home detention and pay AUD $19,116 in compensation to the online shopping network after eBay reimbursed clients tricked into buying one of Tenenboim's bogus Apple iPods over four months (Rao 2007).

Online Gaming

The increasing popularity of the second generation of internet-based services—emphasising online collaboration and sharing among users (i.e. Web 2.0) and supporting virtual communities—results in new ways of assessing and sharing information electronically, such as online gaming. Online gaming, typically played via the internet and local area network, is a growing industry. Major online gaming vendors include Microsoft (Xbox).

Games, particularly MMOG (massively multiplayer online games) and MMORPG (massively multiplayer online role-playing games) allow players to compete with and against each other on a grand scale in real-time. MMOG and MMORPG are increasingly gaining popularity with the digital generation. The virtual worlds in MMOG and MMORPG provide an environment where people communicate with each other using a

virtual persona—avatar—and allow strangers who do not necessarily speak the same language to establish relationships (in the virtual worlds).

To participate in the games, players exchange real cash for virtual currency from the gaming sites (e.g. LindeX, the official Second Life currency exchange) or from third-party trading websites (e.g. http://www.ige.com/). Using these virtual currencies, players can purchase virtual properties, virtual accommodation and virtual merchandise (e.g. weapons to use in the "World of Warcraft" games), and to inflate their virtual status in the virtual worlds. A study by Chen et al. (2004) suggested that, as at March 2003, a virtual exchange rate was estimated to be 10,000 virtual cash units to US$1. It was also reported on LindeX that a virtual exchange rate was estimated to be L$266 (Linden Dollars) to US$1 as at 28 March 2007.

The availability of a market for virtual currency exchange has attracted the interest of individuals and multinational corporations. In November 2006, Anshe Chung—the first self proclaimed virtual world millionaire—announced that she had accumulated virtual assets worth more than US$1 million in physical currency. Multinational corporations such as IBM have established or intend to establish a presence in these virtual worlds. Sweden and Duran Duran (a music band) also announced recently the establishment of a diplomatic representation in Second Life and purchase of a luxury island in Second Life, respectively. The recent article of "Kristie Lu Stout (picture) [being] the first CNN correspondent to report from within Second Life, and will host a new programme looking at how technological developments in the virtual world will shape our future" (Supian 2007) signals the trend of online gaming within the near future. Although there has been speculation that profits generated from economic activities taking place in the virtual worlds might be taxable in the near future (Terdiman 2006), the likelihood of this happening in most countries in the near future is rather low.

Risks of money laundering will increase as MMOG and MMORPG sites emerge as a vehicle for money laundering online. For example, organised crime groups can purchase virtual properties in the virtual worlds worth 1,000 Linden dollars, but actually pay AUD$2 million in cash (Palmers 2007). Colluding avatars (controlled by criminals) can also launder illicit proceeds in the form of gifts or mutually beneficial economic exchanges in the virtual worlds. Although online gaming site operators in Australia are required to monitor and report any suspicious transactions under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth), such privately-conducted transactions are unlikely to be regulated by Financial Intelligence Units.

Software piracy has also been associated with games that adopt the 'charge for software licence' revenue model rather than the 'charge for network connection' model (i.e. players are charged a network connection fee for playing). For example, organised cybercriminal groups can host online game sites using pirated gaming source codes. In November 2006, the United States FBI closed the website www.l2extreme.com that hosted the "Lineage" online game using pirated source code. A Californian man was arrested for criminal copyright infringement and faces up to five years in prison and a US$250,000 fine (US FBI 2007).

Moreover, the availability of a market for virtual goods trading (e.g. http://www.itembay.com.tw/) provides criminals with financial incentives to offend. On December 2006, 44 suspects were arrested in China for stealing more than 700,000 yuan (approximately AUD $112,220) worth of virtual items by selling properties belonging to compromised Tecent QQ users' accounts (Zhu 2006).

Organised cybercriminal groups are targeting MMOG sites to steal gamers' usernames, passwords, credit card numbers, and virtual game pieces and accessories. In September 2006, the database of Second Life was reportedly hacked into and information about 650,000 game users, including addresses, passwords and encrypted credit card details,

stolen (Sophos 2006). Such stolen information can then be used to facilitate other crimes including identity theft or extortion. Stolen merchandise can also be 'sold' to the original owners and other players, or traded on online auction sites. In June 2002, virtual currency with an estimated value of S$15,000 was reportedly stolen from four compromised players' accounts in Singapore (IMCYC 2005). Another example includes the case of J.B. Weasel who, in 2003, was arrested and charged in the United States District court under the federal *Computer Fraud and Abuse Act* for allegedly hacking into another player's GettaLife game account and stealing the player's virtual assets (BlackHat 2003).

In the same way that legitimate businesses look at market forces and new opportunities, organised crime groups will also explore new areas that can be exploited to maximise their profits and to evade the scrutiny of law enforcement agencies. Examples include:

- Selling non-existent merchandise to other players.
- Creating special programs to gain unfair advantages by modifying game software and data, by exploiting bugs and design flaws and reverse engineering the gaming program. The perpetrators then have a better chance of winning in competitions and tournaments that award winners with prizes (e.g. unlocking new car components or car models). These acquired virtual assets can subsequently be traded or sold.
- Designing cloned websites with the aim of gaining login credentials of legitimate players and committing other crimes including identity theft.
- Disseminating spyware or malicious code via disguised email. For example, the 'MultiDropper-RL' Trojan disguises itself as an installer for the "Omerta" game, and installs information stealing malware onto the infected machine once the victim executes the installer. Cases involving the use of Trojan by organised cybercriminal groups include the arrest of 23 members in Spain on September 2006. It was alleged that the group used the "Trojan to steal personal banking data from unsuspecting users in Spain and then to move the money outside the country to Eastern Europe" (Kornakov 2006).
- Continuing to employ social engineering to gain access to networks and gaming accounts. It was recently reported that identity thefts hijacked gaming accounts by making pretext calls to Microsoft Xbox Live's gaming service support centre (Keizer 2007).
- Online paedophile rings offering sexual activities with virtual children (child avatars) and other virtual child exploitation activities. In May 2007, police in the German city of Halle has reportedly commenced an investigation into "virtual" child pornography cases (Fell 2007; Johnston 2007). In May–June 2007, 300 websites allegedly hosting links to pornographic websites and 10,000 online porn games were shut down by Chinese authorities (Online porn merchants dodge internet dragnet 2007).
- Designing games to facilitate terrorist training such as the "Quest for Bush" game allegedly produced by the Global Islamic Media Front (Web video game aim: 'Kill' Bush characters 2006). For example, images found in seized Iraqi cartoon how-to-torture guides "teach terrorists what to do with their victims to force them to talk. Some images showed how to drill hands, sever limbs, drag victims behind cars, remove eyes, and put a blowtorch or iron to someone's skin, according to the Fox News Channel" (Iraqi cartoon manuals show how to torture 2007). Games based on such twisted ideology can be designed to radicalise and desensitise the young and naïve digital generation (with a shallow understanding of any religion).

The future will see the continued development of malicious code by organised cybercriminal groups (e.g. hackers and information thieves groups) targeting the online gaming community, such as:

- 'CopyBot'-type code that allows gamers to replicate virtual goods without paying the original designers;
- 'Grey goo'-type code designed to self-replicate objects within the virtual world that might eventually cause a denial of service-type attack;
- 'Waigua'-type code (especially popular in Chinese online games) designed to automatically carry out activities on behalf of the players with the aim of 'assisting' other players to increase the levels of their characters; and
- Other gaming Trojans (e.g. Trojan.PSW) designed to steal user account details for popular online games.

Social Networking Sites

Popular social networking sites such as Friendster, MySpace and Facebook allow users to post their personal details and photographs and also interact with other users in real-time. Such information could, however, be used to identify or profile a particular user, and it has been shown that such sites could be exploited by organised cybercriminal groups, particularly malware authors. Pieces of personal information obtained from social networking sites could also be used to facilitate other crimes such as identity theft and context-aware phishing.

Context-aware Phishing

Phishing attacks can be facilitated by publicly available personal information such as name, email address, schools attended and names of acquaintances. A recent phishing experiment conducted by researchers at Indiana University in April 2005 (Jagatic et al. 2007) suggested that phishers can easily exploit social network data found on the internet to increase the yield of a phishing attack as internet users may be over four times as likely to become victims if they are solicited by someone appearing to be an acquaintance. Phishers have also been known to

> target the users in question with phishing emails that - by means of context - appear plausible to their respective recipients. For example, phishers can infer online banking relationships, and later send out emails appearing to come from the appropriate financial institutions. Similarly, phishers can detect possible online purchases and then send notifications stating that the payment did not go through, requesting that the recipient follow the included link to correct the credit card information and the billing address. The victims would be taken to a site looking just like the site they recently did perform a purchase at, and may have to start by entering their login information used with the real site (Jakobsson and Stamm 2006).

Organised cybercriminal groups such as the 'Rock-Phish' gang are likely to exploit such information to identify or profile a particular user and increase the yield of future phishing attacks.

Distributing Propaganda

Organised ideologically-motivated cyber groups (including terrorist groups) could, potentially, use online chat rooms and social networking sites, particularly jihad-oriented forums, as vehicles to reach an international audience, solicit funding, recruit new members, and to distribute propaganda. A recent report (IDSS 2006) highlighted the proliferation of jihad-oriented sites in Southeast Asia, which facilitate radicalisation among the Muslim community in the region. Such sites target the digital generation—the young and the internet-aware—particularly among the Muslim community. The latter, with a shallow understanding of Islam, could be easily misled by the propaganda posted on such sites and forums. For example, Jason Walters, a member of the Dutch-based 'Hofstad group', allegedly visited radical websites, posted messages glorifying jihad and talked about killing those he deemed enemies of Islam. Walters and several other members of the group were arrested in November 2004 for their alleged involvement in terrorist activities and the attempted murder of film director Theo Van Gogh (Vidino 2007). Examples of propaganda material include religious rulings (fatwa) declaring suicide terrorism to be legitimate within Islam:

> He who commits suicide kills himself for his own benefit, while he who commits martyrdom sacrifices himself for the sake of his religion and his nation. While someone who commits suicide has lost hope with himself and with the spirit of Allah, the Mujahid struggler is full of hope with regard to Allah's spirit and mercy. He fights his enemy and the enemy of Allah with this new weapon, which destiny has put in the hands of the weak, so that they would fight against the evil of the strong and arrogant (Weimann 2006: p. 634).

In fact, the digital generation has been identified by Rohan Gunaratna, a Singapore-based counter-terrorism expert, as the new face of extremism (Bahrawi 2007b). In March 2007, the Deputy Prime Minister and Minister of Home Affairs of Singapore told Parliament that the Internal Security Department of Singapore has investigated cases involving "Singaporeans who had become attracted to terrorist and radical ideas purveyed in the mass media, particularly the Internet" (Ahmad 2007) such as the recent case involving Abdul Basheer Abdul Kader—a former legally-trained academic.

Disseminating Malicious Code

Such sites can also be exploited as a vehicle to distribute malware—malicious code. For example, the codec program is sometimes required to play video clips posted on the internet and online video sharing websites. Malware including potentially unwanted programs can be embedded in the codec, which will infect end-users' computers when installed. Recent incidents include the installer for 'Zango Cash Toolbar' being embedded in video clips hosted on several MySpace users' profile pages (Websense Security Labs 2006).

The popularity of online video sharing websites is likely to increase the possibility of being exploited by organised cybercriminal groups to disseminate malware.

Intellectual Property and Copyright Infringement

In today's knowledge-based economy, managing and protecting intellectual property , the principal economic asset and sustainable corporate competitive advantage, has become the cornerstone of corporate strategy. Social networking sites, including online video sharing websites, can be abused by criminals to facilitate the dissemination of copyright materials,

such as MP3 blogs and video clips featuring copyright protected tracks and movies, without the consent of the copyright owner, or creating hyperlinks to third-party websites carrying infringing sound recordings.

A related incident is Universal Music Australia Pty Ltd v Cooper [2005] FCA 972 (14 July 2005). The Federal Court found that there had been an infringement of copyright by Stephen Cooper (MP3s4free.net), internet service provider E-Talk Communications (trading as ComCen Internet Services), Liam Francis Bal (director of E-Talk/Com-Cen), and Chris Takoushis (employee of E-Talk/Com-Cen) by creating hyperlinks to third-party websites that had infringing sound recordings.

Weblogs (Blogs)

Blogs, an emerging form of communication, allow internet users to disseminate and share information and ideas. Various communities have emerged in the blogosphere (the world of blogs) ranging from technical support communities such as Google blogs http://googleblog.blogspot.com/) to groups of bloggers who are known to each other, to hate blog groups formed by bloggers who are racists or extremists (Chau and Xu 2007). It has been estimated that the number of bloggers in China is 20.8 million (China tops 20m bloggers 2007). Several multinational corporations have also established company-based blogs (e.g. Symantec Security Response Weblog).

Distributing Propaganda, and Racial Vilification and Offensive Material

Similar to online chat rooms and social networking sites, blogs can also be used to distribute propaganda and host offensive content, including racial vilification material and insensitive statements about a particular ethnic group.

> Radical websites masquerading as innocuous blogs are also sprouting on the Internet. One such blog is maintained by a man who described himself as a Muslim living in Britain with his family. Writing in English, the blogger offers his own interpretations of passages from the Quran. His most recent post derides Muslims who live happily in the West and who are unsympathetic to the sufferings of those in Afghanistan and Iraq. Because of the youths' lack of knowledge of the religion and their own grievances and feelings, they can be susceptible to radical ideologies (New worry: homemade extremists 2007)

In October 2005, two Singaporeans were convicted under s4(1)(a) of the *Sedition Act*, Chapter 290, for posting invective and pejorative remarks on their blogs and a general discussion forum on the internet; see Public Prosecutor v Koh (2005) DAC 39442 and Public Prosecutor v Lim (2005) DAC 39444. Such insensitive remarks targeting a particular religion, ethnic group or segment of the community could have "a seditious tendency to promote feelings of ill-will and hostility between different classes of the population" (Public Prosecutor v Koh (2005) DAC 39442 and Public Prosecutor v Lim (2005) DAC 39444: 2).

Phishing and Hosting Malware and Child Pornography

Blogs such as the Google-owned Blogger.com have recently been used as vehicles to direct unsuspecting users to phishing sites (Fortinet 2007). Blogs can also be compromised by criminals and malware authors by exploiting vulnerabilities of web servers or operating systems to host malware (e.g. ransomware and self-mutating Trojan malware). Unsuspecting

users' computers can be infected by malware when they visit these compromised blogs that host malware (e.g. ransomware and self-mutating Trojan malware). The recent Global Threat Report by ScanSafe (2007) indicated that up to 6% of blogs host malware. The same techniques used by organised cybercriminal groups to host malware can be used to host child pornography material and distribute links and drive traffic to other sites of similar natures.

Blogs can also be abused by organised crime groups as a vehicle to disseminate massive amounts of spam. Given the potential financial gain in sending massive amounts of spam, it should come as no surprise when organised cyber groups are involved in spam-related cases. In November 2006, a six-member group was arrested by the Cyber Terror Response Center of the Seoul Metropolitan Police Agency for various offences including sending spam via mobile phone short messaging services (SMS) (Police break phone sex hacking ring 2006). In a more recent incident, 34 people were arrested in Malaysia during a two-day Operation Mynah in May 2007 for sending spam email. In those emails, the unwary recipients were either asked to help transfer an inheritance sum stuck in Nigeria for a cut of the money or were being congratulated recipients for winning a lottery that they did not take part in ('Nigerian scam' conmen caught in KL 2007). In a separate incident in June 2007, Adam Vitale and his co-conspirators were charged with sending spam over the internet to the e-mail addresses of approximately 1.2 million subscribers of America Online, Inc., and of hiding the true origin of those e-mails, in the Southern District of New York, United States (US DoJ 2007g).

Ways in which blogs can be abused to disseminate massive amounts of spam include:

- *Spam blogs (splogs)*: Including pornographic-oriented splogs, typically containing gibberish or hijacked content (e.g. information from academic papers) from other blogs and news sources. They are designed to increase the probability of being indexed by search engines (e.g. raise the PageRank index in Google search engines).
- *Trackback spam*: Spammers leverage the trackback feature—automatic cross-linking between websites and blogs that increases—to direct bloggers to spam portals. The trackback feature can also increase the probability of being indexed by search engines.
- *Hjacking blog accounts*: Spammers have also been known to host spam content including links to spam portals, on hijacked blog accounts or hacked blog accounts (particularly inactive accounts).

Conclusion

The strength of the internet in terms of its ease of accessing and sharing content electronically has become one of its weaknesses. A key observation that can be drawn from the preceding discussion is that the internet has influenced the world of organised crime and the criminal marketplace. The internet has resulted in new avenues for traditional crime and has also opened up a whole new area of criminal activities. Technology-enabled crime has also become more sophisticated and organised as the distinction between traditional organised crime and cybercriminal and ideologically / politically motivated cyber groups converges (e.g. traditional organised crime groups recruiting computer specialists and becoming more ideological over time). As Choo, Smith and McCusker (2007: p. xxi) noted:

> [i]t is unlikely that traditional organised crime groups will shy away from using the technology-enabled crime environment to facilitate and/or to disguise illicit proceeds of real world based crimes. The use, for example, of denial-of-service attacks to pursue

> extortion and the use of online banking to transfer laundered funds are both likely to continue. The development of traditional transnational organised crime groups into fully-fledged technology-enabled criminals will 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 technology-enabled crimes. Organised operations that make use of conventional technology-enabled crime methodologies, such as financial scams or piracy, will also increase as the use of networked computers for criminal purposes develops.

Financially-motivated cyber-attacks will continue to be more targeted, focusing their attention particularly on financial institutions. The AusCERT (2006) survey and the DTI Information Security Breaches survey (PwC 2006) found an increase in the views held by the businesses surveyed that electronic attacks are more often motivated by illicit financial gain than in the past, both in Australia and around the world. The United States Federal Bureau of Investigation has estimated the financial loss due to cybercrime in 2004 as being approximately US$400 billion (McAfee 2005), while a United Kingdom survey (PwC 2006) found that information security breaches cost British companies across several industry sectors £10 billion per annum.

The threats of organised cybercriminal groups and organised ideologically / politically motivated cyber groups that aim to incite hatred, violence, and intimidation through the internet present a real danger to the economic and social stability of society. These threats will be exacerbated by the increasing reliance which businesses and individuals place upon online systems for the functioning of their daily lives. Extraterritoriality, the notion that the internet has no geographic boundaries has driven the e-commerce revolution. Unfortunately, the criminal fraternity operates online under the same free market principles, while legislative and law enforcement endeavours launched against them suffer from geographical and cultural restrictions.

These threats have given rise to a growing demand for new strategies of response. These include the need to reduce the opportunities for technology-enabled crime to occur, to make technology-enabled crime more difficult to commit, to increase the risks of detection and punishment associated with committing technology-enabled crime, and to show that there are fewer benefits to be gained from committing such crimes.

There is no single all-encompassing solution to responding to the risks posed by the digitisation of information. The ability of organised crime groups, particularly cybercriminal groups, to leverage advances in ICT to operate in cyberspace, alters the nature of the criminals encountered by law enforcement and continues to be a major challenge for law enforcement. For example, the internet increases the potential for cybercriminal groups to establish highly coordinated and geographically widespread internet-based criminal networks making use of cryptography and security tools to evade the scrutiny of law enforcement. In addition to making use of these technological developments, cyber groups have also increasingly adopted networked strategies and organisational structures that span across different countries. This, in turn, requires changes in the training of law enforcement officers and in the ways in which law enforcement agencies operate.

Legislation relating to the activities of organised cybercriminal groups, computer technology, anti-money laundering, counter-terrorism and national security will need to be continually monitored over the next two years to deal with new technological developments. As Duffy noted,

> [i]t is clear that government regulations that are supposed to protect the environment are rendered ineffective in the face of local networks that are inter-linked with

> globalised networks, such as the offshore finance sector and drug trafficking. The expansion of organised and global level criminal networks has resulted in locally based facilitators and protectors of criminality. These interest groups are able to effectively challenge governments for control of key state institutions, thereby ensuring that the enforcement of legislation is impossible and domestic accountability is non-existent (Duffy 2006: p. 42).

The capacity of international law enforcement agencies to maintain and extend the delivery of criminal information and intelligence on which individual national agencies can draw to inform the national and international criminal intelligence picture will be another key element of countering future threats by organised cybercriminal and ideologically / politically motivated cyber groups.

The community can also play an important role in crime prevention and reduction. For example, in countering the use of the internet as a basis for radicalisation and recruitment to terrorism (internet-driven counter-radicalisation) is more than putting in place legislation that criminalises activities that encourage acts of terrorism or the dissemination of terrorist publications. Religious leaders and scholars can counter terrorist or extremist ideologies by setting up counter-terrorism websites 'that debunk the dangerous views and misinformation that characterise these rogue sites' (How to fight hate websites? 2007).

Acknowledgements The authors wish to thank Rob McCusker (AIC), Janet Smith (AIC), Professor Peter Grabosky (ANU) and the anonymous referees for their feedback on earlier drafts of this article. Despite their invaluable assistance, any errors remaining are solely attributed to the authors.

References

Ahmad, R. (2007). Slashing through the Web of terror. *Todayonline* 3 March.

Ames, B. (2007). *Online spending tops US$100 billion*. *Computerworld.com.au* 05 January.

AusCERT (2006). *Computer crime and security survey*. http://www.auscert.org.au/images/ACCSS2006.pdf.

Australia Attorney-General's Department (AGD) n/a. Why are anti-money laundering and counter-terrorism financing reforms required?. *Fact sheet*. http://www.ag.gov.au/www/agd/agd.nsf/Page/Anti-moneylaundering_Factsheets.

Australian Institute of Criminology (AIC) (2007). New methods of transferring value electronically. *High tech crime brief* 14. http://www.aic.gov.au/publications/htcb/htcb014.html.

Australian Payments Clearing Association (APCA) (2005). *Annual report 2005*. http://www.apca.com.au/Public/apca01_live.nsf/WebPageDisplay/PUB_AnnualReport.

Bahrawi, N. (2007a). One abdul basheer is one too many. *Todayonline* 11 June.

Bahrawi, N. (2007b). The new face of extremism: Young, Internet-savvy and easily duped. *Todayonline* 26 March.

Bandura, A. (1999). Social cognitive theory of personality. *Asian Journal of Social Psychology, 2*(1), 21–41.

BlackHat (2003). *BlackHat briefings*. http://www.blackhat.com/presentations/bh-usa-03/bh-us-03-hackercourt.pdf.

Brenner, S. W. (2002). Organized cybercrime? How cyberspace may affect the structure of criminal relationships. *North Carolina Journal of Law & Technology, 4*(1), 1–50.

Canadian Security Intelligence Service (2000). *Transnational criminal activity: A global context*. http://www.csis-scrs.gc.ca/en/publications/perspectives/200007.asp?print_view=1.

Charlton, J. (2005). Al Qaeda buys cyber criminal expertise. *Computer Fraud & Security, 2005*(3), 2.

Chau, M., & Xu, J. (2007). Mining communities and their relationships in blogs: A study of online hate groups. *International Journal of Human-computer Studies, 65*(1), 57–70.

Chen, Y. -C., Chen, P., Song, R., & Korba, L. (2004). Online gaming crime and security issue: Cases and countermeasures from Taiwan. Paper to Second Annual Conference on Privacy, Security and Trust, University of New Brunswick, October 2004.

China tops 20m bloggers (2007). *Australian IT* 12 January.

Choo, K. K. R., Smith, R. G., & McCusker, R. (2007). Future directions in technology-enabled crime: 2007–09. *Research and public policy series* no 77. Australian Institute of Criminology.

Curry, A., & McGrane, S. (2006). China's cyberwarriors. *Foreign policy* September/October issue: 93.
Duffy, R. (2006). Global governance, criminalisation and environmental change. *Global crime, 7*(1), 25–42.
Fell, M. (2007). Crime in the virtual world 2007. ABC.net.au 11 May.
FBI warns of Eastern European hacker groups (2001). OUT-Law.com 9 March.
Fortinet (2007). *Malicious code appears on Blogger.com*. http://www.fortiguardcenter.com/advisory/FGA-2007-04.html.
Frith, M. (2007). Student 'in bank fraud plot'. *The sun-herald* 17 June.
Gantz, J. F., Reinsel, D., Chute, C., Schlichting, W., McArthur, J., Minton, S., et al. (2007). The expanding digital universe. *IDC white paper* March.
Great Britain. Crown Prosecution Service (GB CPS) (2006). Convictions for internet rape plan. *Media release* 1 December.
Harding, T. (2007). Terrorists 'use Google maps to hit UK troops'. Telegraph.co.uk 13 January.
Heydt-Benjamin, T. S., Bailey, D., Fu, K., Juels, A., & O'Hare, T. (2007). Vulnerabilities in first-generation RFID-enabled credit cards, in Proceedings of Financial Cryptography and Data Security 2007 *Lecture notes in computer science* (forthcoming). http://www.cs.umass.edu/~tshb/FC07-heydt-benjamin.pdf.
How to fight hate websites? (2007). *The electric new paper* 21 June.
Inside the Yamaguchi-gumi: Ex-gangster's life a history of Japan's postwar underworld (2006). *MSN-Mainichi daily news* 24 May.
Institute of Chartered Accountants (2006). Money laundering worth up to 5% of global GDP. *News release* 26 May.
Institute of Defence and Strategic Studies (IDSS) 2006. *Proceedings of the International conference on Terrorism in Southeast Asia: The threat and response*. http://www.rsis.edu.sg/.
Interview: Eugene Kaspersky (2007). *Infosecurity* May/June issue.
Iraqi cartoon manuals show how to torture (2007). *The electric new paper* 29 May.
Jagatic, T., Johnson, N., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM* (forthcoming). http://www.indiana.edu/~phishing/social-network-experiment/phishing-preprint.pdf.
Jakobsson, M., & Stamm, S. (2006). Invasive browser sniffing and countermeasures, in *Proceedings of the 15th international Conference on World Wide Web, Edinburgh, 2006*: http://www2006.org/programme/item.php?id=3527.
Jaques, R. (2006). European police nab zombie hackers. Vnunet.com 27 Jun.
Jen, W. Y., Chang, W., & Chou, S. (2006). Cybercrime in Taiwan: An analysis of suspect records. Paper to Workshop on Intelligence and Security.
Johnston, C. (2007). Brave new world or virtual pedophile paradise? Second Life falls foul of law. The.age.com.au 10 May.
Keizer, G. (2007). Microsoft owns up to Xbox Live pretexting. Computerworld.com 25 March.
Kirk, J. (2007a). Estonia recovers from massive denial-of-service attack. *InfoWorld* 17 May.
Kirk, J. (2007b). Hackers build private IM to keep out the law. Computerworld.com 28 March.
Kirk, J. (2007c). Symantec: Chinese hackers grow in number, skills. Infoworld.com 18 May.
Kornakov, K. (2006). Cyberfraudsters detained in Spain. Viruslist.com 18 September.
Kshetri, N. (2005). Hacking the odds. *Foreign Policy, 148*, 93.
Kshetri, N. (2006). The simple economics of cybercrimes. *IEEE Security & Privacy, 4*(1), 33–39.
Lal, R. (2005). South Asian organized crime and terrorist networks. *Orbis, 49*(2), 293–304.
Libbenga, J. & Leyden, J. (2007). Dutch botnet duo sentenced. *The register* 1 February.
Lyman, P., & Varian, H. R. (2003). *How much information 2003?*. http://www.sims.berkeley.edu/how-much-info-2003.
McAfee (2005). *McAfee virtual criminology report 2005*. Santa Clara CA: McAfee.
McAfee (2006). *Virtual criminology report: Organised crime and the internet*. Santa Clara CA: McAfee.
McCusker, R. (2006). Organised crime and terrorism: Convergence or separation? *Standing group organised crime eNewsletter* 12 May.
Moore, T. & Clayton, R. (2007). An empirical analysis of the current state of phishing attack and defence, in *Proceedings of the Sixth Workshop on the Economics of Information Security,* Pittsburgh, 2007.
National White Collar Crime Center and Federal Bureau of Investigation (NW3C/FBI) (2007). *2006 Internet Fraud Crime Report*. http://www.ic3.gov/media/annualreport/2005_IC3Report.pdf.
New worry: Homemade extremists (2007). *Todayonline* 2 June. http://www.todayonline.com/articles/191998.asp.
'Nigerian scam' conmen caught in KL (2007). *The electric new paper* 2 June.
Office of the United States Trade Representative (2007). *2007 Special 301 report*. http://www.ustr.gov/assets/Document_Library/Reports_Publications/2007/2007_Special_301_Review/asset_upload_file980_11122.pdf.
Online porn merchants dodge internet dragnet (2007). *AsiaOne* 5 June.
Organisation for Economic Co-operation and Development (OECD) (2007). *The economic impact of counterfeiting and piracy*. http://www.oecd.org/dataoecd/11/38/38704571.pdf.

Palmers, C. (2007). Policing a virtual world. *Anti-money laundering magazine, 7*, 25–27.
PandaLabs (2007). *Cybercrime... for sale (II)*. http://blogs.pandasoftware.com/blogs/pandalabs/archive/2007/05/03/Cybercrime_2E002E002E00_-for-sale-_2800_II_2900_.aspx.
Pereira, J. (2007). How credit-card data went out wireless door. *The wall street journal* 4 May.
Police break phone sex hacking ring (2006). Donga.com 10 November.
PricewaterhouseCoopers (PwC) (2006). *DTI information security breaches survey 2006.* http://www.pwc.com/extweb/pwcpublications.nsf/docid/7FA80D2B30A116D7802570B9005C3D16.
Raid of a major pirate packaging facility in Guangzhou (2007). *Enforcement bulletin issue* 33, 5.
Rao, S. (2007). Net hacker avoids jail. *Daily telegraph* 8 June.
Rodriguez, A. (2007). Attacks on Estonia move to new front. *Chicago tribune* 29 May.
Russia arrests 'grandfather of cybercrime' (2001). *BBC news* 26 May.
ScanSafe (2007). *Global threat report*. 18 April.
Schrank, P. (2007). Newly nasty. *The economist* 24 May.
Singapore Inter-Ministry Committee on Youth Crime (IMCYC) (2005). Game over. *The Straits Times article* 11 February.
Singapore Commercial Affairs Department (2006a). *Annual report: Beyond excellence service with assurance*. http://www.cad.gov.sg/topNav/pub/Annual+Reports.htm.
Singapore Commercial Affairs Department (2006b). *Money mules*. http://www.cad.gov.sg/topNav/hom/.
Singapore Commercial Affairs Department (2007). Case of 6-members credit card skimming syndicate. *Media release* 21 May.
Sophos (2006). Hackers may get second chance to benefit from Second Life security breach. *Press release* 11 September.
Supian, H. (2007). Minding the virtual buzz. *Todayonline* 29 May.
Swartz, J., & Acohid, B. (2007). Data theft arrests show how tens of millions are at risk. *USA today* 12 June.
Symantec (2007a). *Symantec internet security threat report vol. XI*. www.symantec.com/threatreport.
Symantec (2007b). *Italy under attack: Mpack gang strikes again!*. 15 June. http://www.symantec.com/enterprise/security_response/weblog/2007/06/italy_under_attack_mpack_gang.html.
Symantec (2007c). *Symantec internet security threat report vol. XI* March. http://www.symantec.com/threatreport.
Terdiman, D. (2006). IRS taxation of online game virtual assets inevitable. CNet.com 3 December.
Tigers have joined jihadi drug trade, says official (2007). *Todayonline* 11 June. http://www.todayonline.com/articles/193618.asp.
United Kingdom Child Exploitation and Online Protection (UK CEOP) (2007). Global online child abuse network smashed - CEOP lead international operation into UK based paedophile ring. *Media release* 18 June.
United States Department of Justice (US DoJ) (2004). Nineteen individuals indicted in internet carding conspiracy. *Media release* 28 August. http://www.usdoj.gov/opa/pr/2004/October/04_crm_726.htm.
United States Department of Justice (US DoJ) (2005). Six defendants plead guilty in internet identity theft and credit card fraud conspiracy. *Media release* 17 November. http://www.cybercrime.gov/mantovaniPlea.htm.
United States Department of Justice (US DoJ) (2006a). 21 charged with participating locally in alleged international internet-based fraud scheme. *Media release* 12 December.
United States Department of Justice (US DoJ) (2006b). 'Botherder' dealt record prison sentence for selling and spreading malicious computer code. *Media release* 8 May.
United States Department of Justice (US DoJ) (2007a). Four defendants arraigned in half-million dollar eBay fraud scheme. *Media release* 16 February.
United States. Department of Justice (US DoJ) (2007b). Four Russians indicted in identity theft and fraud ring. *Media release* 1 March.
United States Department of Justice (US DoJ) (2007c). Digital currency business e-gold indicted for money laundering and illegal money transmitting. *Media release* 27 April.
United States Department of Justice (US DoJ) (2007d). Software piracy ringleader extradited from Australia. *Media release* 20 February.
United States Department of Justice (US DoJ) (2007e). Extradited software piracy ringleader pleads guilty. *Media release* 20 April.
United States. Department of Justice (US DoJ) (2007f). Former member of the US navy indicted on terrorism and espionage charges. *Media release* 31 March.
United States. Department of Justice (US DoJ) (2007g). Brooklyn man pleads guilty to participating in massive AOL spam scheme. *Media release* 11 June.
United States. Department of Justice (US DoJ) (2007h). Bulgarian woman arrested and charged with conspiracy and money laundering. *Media release* 26 March.
United States Federal Bureau of Investigation (US FBI) (2007).Cracking the code: Online IP theft is not a game. *Media release* 1 February.

United States Florida Department of Law Enforcement (US FDLE) (2007). Arrests made in gift card fraud case totaling more than $8 million in losses. *News release* 19 March.
United States Immigration and Customs Enforcement (US ICE) (2005). ICE arrests 9 in Ohio fraud driver's license scheme. *News release* 24 February.
United States National Drug Intelligence Center (US NDIC) (2006). *National drug threat assessment 2007: Drug money laundering.* http://www.usdoj.gov/ndic/pubs21/21137/index.htm.
United States National Science and Technology Council (US NSTC) 2006. *Federal plan for cyber security and information assurance research and development: Report by the Inter-agency Working Group on Cyber-security and Information Assurance.* http://www.ostp.gov/nstc/html/Cyber%20Security%20and%20Information%20Assurance%20Report%20April%202006.pdf.
United States Secret Service (USSS) (2004). U.S. secret service's operation firewall nets 28 arrests. *Press release* 28 October.
van Rassel, J. (2007). ATM skimmers seized in raid. *Calgary herald* 31 May.
Vidino, L. (2007). The hofstad group: The new face of terrorist networks in Europe. *Studies in Conflict & Terrorism, 30*, 579–592.
Ward, M. (2006). Anti-cartoon protests go online. BBC.co.uk 8 February.
Web video game aim: 'Kill' Bush characters (2006). CNN.com 18 September.
Websense Security Labs (2006). Malicious website / malicious code: Fradulent You Tube video on MySpace installing Zango Cash. *Media release* 06 November.
Wee, E. (2007). Global diy terror: No cell, no hardship. *The electric new paper* 10 June.
Weimann, G. (2006). Virtual disputes: The use of the internet for terrorist debates. *Studies in conflict & terrorism, 29*(7), 623–639.
World internet vusage and population statistics (2007). http://www.internetworldstats.com/stats.htm.
Zhu, L. (2006). China nabs 44 suspects in biggest internet virtual property swindle. Xinhuanet.com 15 December.