Organizations and Cybercrime

Title Page

Draft October 11, 2013 ANU Cybercrime Observatory

Roderic Broadhurst, Peter Grabosky, Mamoun Alazab, Brigitte Bouhours, and Steve Chon.

Contact: roderic.broadhurst@anu.edu.au

Australian National University, ANU Cybercrime Observatory
Paper submitted to the International Journal of Cyber Criminology

October 11, 2013

Organizations and Cybercrime

Abstract

This paper explores the nature of groups engaged in cybercrime. It briefly outlines the definition and scope of cybercrime, theoretical and empirical challenges in addressing what is known about cyber offenders, and the likely role of organized crime groups (OCG). We give examples of known cases that illustrate individual and group behaviour, and motivations of typical offenders, including state actors. Different types of cybercrime and different forms of criminal organisation are described drawing on the typology suggested by McGuire (2012). It is apparent that a wide variety of organisational structures are involved in cybercrime. Enterprise or profit-oriented activities, and especially cybercrime committed by state actors, appear to require leadership, structure, and specialisation. By contrast, protest activity tends to be less organized, with weak (if any) chain of command.

Keywords

cybercrime, organized crime, crime groups; Internet crime; cyber offenders; online offenders, state crime

Organizations and Cybercrime

Introduction

Cybercrime exploits cross-national differences in the capacity to prevent, detect, investigate, and prosecute such crime, and is fast becoming a growing global concern (United Nations, 2004). This transnational character provides cybercriminals, whether operating as individuals or as organized crime groups, with the potential to evade counter-measures, even when these are designed and implemented by the most capable actors (Brenner, 2006; Council of Europe, 2005; Broadhurst & Choo, 2011). Cybercrime has evolved in parallel with the opportunities afforded by the rapid increase in the use of the Internet for e-commerce and its take-up in the developing world. In February 2013, 2.7 billion people, nearly 40% of the world population, had access to the Internet. The rate was higher in the developed world (77%) than in the developing world (31%). While Africa had the lowest Internet penetration rate (16%), between 2009 and 2013 Internet penetration has grown fastest in Africa (annual growth of 27%) followed by Asia-Pacific, the former Soviet Union, and the Arab states (15% annual growth rate). Around one-quarter of all Internet users used English (27%) on the web, and another quarter (24%) used Chinese (International Telecommunication Union, 2013). This increasingly diffuse and interdependent market will attract a diverse range of criminal actors.

The growth in scale and scope of cybercrime since 2005 has been attributed to the proliferation of 'botnets'[1] as mass tools for computer misuse aided by 'exploit kits' (e.g., Blackhole Exploit Kit) that compromise systems and 'botnet kits' (e.g., ZeuS) that subsequently provide control of the compromised computers to cybercriminals for nefarious purposes.. Spam and malicious websites are still the usual vectors for deceptive intrusion and widespread distribution of 'malware' such as 'bots'.[2] Various forms of social engineering are also common means of compromising computers. Botnet operators or 'herders' provide such services for fees that reflect the number and likely value of 'zombie' (or infected) computers in the botnet. These activities operate like criminal services in other domains of crime, for example, those of forgers or money launderers. Crimeware toolkit users also adopt the 'software as a service' approach by renting out malicious software from their creators or owners for a specified period of time during which they are then used to commit crime. A more basic service is that of a stolen-data supplier, who allows others to download stolen data, such as credit card details, for a fee (Ben-Itzhak, 2009). In short, cybercrime has gradually evolved from a relatively low volume crime committed by an individual specialist offender to a mainstream or common high volume crime 'organized and industrial like'(see Moore, Clayton, & Anderson, 2009; Anderson et al., 2012).

While many types of cybercrime require a high degree of organization and specialization, there is insufficient empirical evidence to ascertain if cybercrime is now dominated by organized crime groups and what form or structure such groups may take (Lusthaus, 2013). Digital technology has empowered individuals as never before. Teenagers acting alone have succeeded in disabling air traffic control systems, shutting down major e-retailers, and manipulating trades on the NASDAQ stock exchange (US Securities and Exchange Commission, 2000). What individuals can do, organizations can also do, and often better. It is apparent that many if not all types of criminal organization are capable of engaging in cybercrime. The Internet and related technologies lend themselves perfectly to coordination across a dispersed area. Thus, an organized crime group may be a highly structured traditional mafia like group that engages

delinquent IT professionals. Alternatively, it could be a short-lived project driven by a group that undertakes a specific online crime and/or targets a particular victim or group. Rather than groups, it may involve a wider community that is exclusively based online and dealing in digital property (e.g. trading in 'cracked' software or distributing obscene images of children).[3] It may also consist of individuals who operate alone but are linked to a macro-criminal network (Spapens, 2010) as may be found in the 'darknet' and underground Tor[4] sites.

Many cybercrimes begin with unauthorized access to a computer system. Information systems may be targeted for the data they contain, including banking and credit card details, commercial trade secrets, or classified information held by governments. Theft of personal financial details has provided the basis for thriving markets in such data, which enable fraud on a significant scale (Glenny, 2011). The Internet has also been used as a vehicle for fraud. Spurious investment solicitations, marriage proposals, and a variety of other fraudulent overtures are made daily by the hundreds of millions. A recent estimate showed that of approximately 183 billion emails sent every day in the first quarter of 2013 alone, 6 billion contained malicious attachments. Such volume indicates the scale of the problem in this common vector for acquiring unauthorised access to a computer (Kaspersky Lab 2013). In recent years, insurgent and extremist groups have used Internet technology as an instrument of theft in order to enhance their resource base. Imam Samudra, convicted architect of the 2002 Bali bombings, reportedly called upon his followers to commit credit card fraud in order to finance militant activities (Sipress, 2004).

As digital technology pervades modern society, we have become increasingly dependent upon it to manage our lives. Much of our ordinary communications and record keeping rely on the Internet and related technologies. Just as digital technology enhances the efficiency of our ordinary legitimate activities, so too does it enhance the efficiency of criminal activities. Conventional criminals and terrorists use the Internet as a medium of communication in furtherance of criminal conspiracies. And, as is the case with law-abiding citizens, digital technology enhances the capacity for storing records and other information, and for performing financial transactions. In the case of criminals, such transactions may be part of money laundering activities. Manufacturers of illicit drugs advertise and trade recipes over the Internet (Schneider, 2003; See also United States of America v Ross William Ulbricht 2013).

The role of organized crime groups

Governments, law enforcement, academic researchers, and the cyber-security industry speculate that 'conventional' organized crime groups have become increasingly involved in digital crime. The available empirical data suggest that criminals, operating online or on the ground, are more likely to be involved in loosely associated illicit networks rather than formal organizations (Décary-Hétu & Dupont, 2012). McGuire's (2012) review found that up to 80% of cybercrime could be the result of some form of organized activity. This does not mean, however, that these groups take the form of traditional, hierarchical organized crime groups or that these groups commit exclusively digital crime. Rather, the study suggests that traditional organized crime groups are extending their activities to the digital world alongside newer, looser types of crime networks. Crime groups show various levels of organization, depending on whether their activity is purely aimed at online targets, uses online tools to enable crimes in the 'real' world, or combine online and offline targets.

McGuire's review estimated that half the cybercrime groups in his sample comprised six or more people, with one-quarter of groups comprising over 10 individuals. One-quarter of cybercrime groups had operated for less than 6 months. However, the size of the group or the duration of their activities did not predict the scale of offending, as small groups can cause significant damage in a short time.

Cybercriminals may operate as loose networks, but evidence suggests that members are still located in close geographic proximity even when their attacks are cross-national. For example, small local networks, as well as groups centred on relatives and friends, remain significant actors. Cybercrime hot spots with potential links to organized crime groups are found in countries of the former Soviet Union (Kshetri, 2013a; see also *Microsoft Security Blog*, 2010). Hackers from Russia and Ukraine are regarded as skilful innovators. For example, the cybercrime hub in the small town of Rmnicu Vicea in Romania is one of a number of such hubs widely reported in Eastern Europe (Bhattacharjee, 2011). There is also increasing concern about cybercrime in China (*China Daily* 2010; Pauli, 2012). The source and extent of malware attacks (whether of domestic or foreign origin) and the scale of malware/botnet activity remain unclear, but a substantial proportion of Chinese computers are compromised and it is likely that local crime groups play a crucial role (Kshetri, 2013a; Chang, 2012; Kshetri, 2013b; Broadhurst & Chang, 2013). A recent study of spam and phishing sources found that these originated from a small number of ISPs (20 of 42,201 observed), which the author dubbed 'Internet bad neighbourhoods.' One in particular, Spectranet (Nigeria), was host to 62% of IP addresses that were spam related. Phishing hosts were mostly located in the United States, while spam originated from ISPs located in India, Brazil and Vietnam (Moura, 2013).

Given the diversity of the types and sources of cybercrime, it is important to avoid stereotypical images of cybercriminals or spreading an alarmist or 'moral panic' narrative. Popular images include the menacing Russian hacker in pursuit of profit, or more recently the Chinese 'hacker patriot.' Such offender images offer a specific type of 'folk devil;' David Wall (2012) regards them as inherently misleading about the assumptions of offender action and sources of cybercrime. Despite the media image, offenders come from many nations and motivations are diverse, although financial goals appear to dominate.[5]

The standard definition of organized crime contained in the UN Palermo Convention,[6] based on the participation of three or more persons acting in concert, does not extend to certain highly sophisticated forms of organization such as the mobilization of robot networks that may be operated by a single person. So-called botnets involve an offender using malicious software to acquire control over a large number of computers (the largest including more than a million separate machines). Even though the individual and institutional custodians of compromised computers may be unwitting participants in a criminal enterprise, some commentators maintain that botnets mobilized by a sole offender should be considered a form of organized crime (Chang, 2012).

Challenges of Theory and Evidence

The absence of evidence about the extent, role, and nature of organized crime groups in cyberspace impedes the development of sound countermeasures. While a growing number of experts consider that cybercrime has become the domain of organized groups and the days of the

lone hacker are past, little is yet known about the preferred structures and longevity of groups, how trust is assured, and the relationship with other forms of crime. There is an absence of evidence-based research about offender behaviour and recruitment in cyberspace, although learning and imitation play important roles (Broadhurst & Grabosky, 2005). Hence, organized crime groups cannot be understood from their functional (illicit) activities alone, that is – as rational profit-driven networks of criminal actors- since socio-cultural forces also play an important role in the genesis and sustainability of such groups. In some cases obsessive-compulsive behaviour is evident; in others, a sense of impunity (born of over-confidence in anonymity) is apparent. Greed may be only one of many motives: lust, excitement, rebellion, technological challenge, and the desire for notoriety or celebrity status may be present to varying degrees, depending on the types of crime.

Structure

McGuire (2012) has suggested a typology of cybercrime groups, which comprises six types of group structure. He emphasized that 'these basic organizational patterns often cross-cut in highly fluid and confusing ways' and the typology represents a 'best guess,' based on what we currently know about cyber offenders. He notes that the typology is likely to change as the digital environment evolves. McGuire's typology includes three main group types, each divided into two subgroups depending on the strength of association between members:

Type I groups operate essentially online and can be further divided into *swarms* and *hubs*. They are mostly 'virtual' and trust is assessed via reputation in online illicit activities.

- *Swarms* share many of the features of networks and are described as 'disorganized organizations [with] common purpose without leadership.' Typically swarms have minimal chains of command and may operate in viral forms in ways reminiscent of earlier 'hacktivist' groups. Swarms seem to be most active in ideologically driven online activities such as hate crimes and political resistance. The group Anonymous illustrates a typical swarm-type group (Olson, 2012).
    - *Hubs*, like swarms, are essentially active online but are more organized with a clear command structure. They involve a focal point (hub) of core criminals around which peripheral associates gather. Their online activities are diverse, including piracy, phishing attacks, botnets and online sexual offending. McGuire reports that the distribution of scareware often involves hub-like groups. Carders' markets and malware bazaars such as Silk Roadwould also fit this model (United States of America v Ross William Ulbricht 2013).

Type II groups combine online and offline offending and are described as 'hybrids', which in turn are said to be 'clustered' or 'extended.'

- In a *clustered hybrid*, offending is articulated around a small group of individuals and focused around specific activities or methods. They are somewhat similar in structure to *hubs*, but move seamlessly between online and offline offending. A typical group will skim credit cards, then use the data for online purchases or on-sell the data through carding networks (McGuire, 2012, 50; Soudijn & Zegers, 2012).
    - Groups of the *extended hybrid* form operate in similar ways to the clustered hybrids but are a lot less centralized. They typically include many associates and

subgroups and carry out a variety of criminal activities, but still retain a level of coordination sufficient to ensure the success of their operations.

Type III groups operate mainly offline but use online technology to facilitate their offline activities. McGuire argues that this type of group needs to be considered because they are increasingly contributing to digital crime. Like the previous group-types, Type III groups can be subdivided into 'hierarchies' and 'aggregates', according to their degree of cohesion and organization.

- *Hierarchies* are best described as traditional criminal groups (e.g. crime families), which export some of their activities online. For example, the traditional interest of some mafia groups in prostitution now extends to pornography websites; other examples include online gambling, extortion, and blackmail through threats of shutting down systems or accessing private records via malware attacks or hacking. (US v Fiore et al (2009); United States Attorney, Eastern District of New York, 2003)
- *Aggregate* groups are loosely organized, temporary, and often without clear purpose. They make use of digital technologies in an *ad hoc* manner, which nevertheless can inflict harm. Examples include the use of Blackberry or mobile phones to coordinate gang activity or public disorder, as occurred during the 2011 UK riots or the Sydney riots in September 2012 (Cubby & McNeilage, 2012).

The most sophisticated cybercrime organizations are characterized by substantial functional specialization and division of labor. The following roles, outlined in a speech by a representative of the US Federal Bureau of Investigation's Cyber Division, illustrate the kind of roles that a major fraud conspiracy may entail (Chabinsky, 2010):

1. **Coders** or programmers write the malware, exploits, and other tools necessary to commit the crime.
2. **Distributors** or vendors trade and sell stolen data, and vouch for the goods provided by the other specialties.
3. **Technicians** maintain the criminal infrastructure and supporting technologies, such as servers, ISPs, and encryption.
4. **Hackers** search for and exploit vulnerabilities in applications, systems, and networks in order to gain administrator or payroll access.
5. **Fraud specialists** develop and employ social engineering schemes, including phishing, spamming, and domain squatting.
6. **Hosts** provide "safe" facilities of illicit content servers and sites, often through elaborate botnet and proxy networks.
7. **Cashers** control drop accounts and provide those names and accounts to other criminals for a fee; they also typically manage individual cash couriers, or "money mules."
8. **Money mules** transfer the proceeds of frauds which they have committed to a third party for further transfer to a secure location.

9. **Tellers** assist in transferring and laundering illicit proceeds through digital currency services and between different national currencies.
10. **Executives** of the organization select the targets, and recruit and assign members to the above tasks, in addition to managing the distribution of criminal proceeds.

This ideal type is not necessarily limited to a formal, fixed organization. Some functions may be outsourced, as was the case with the Koobface group discussed below. The organization of cybercrime may also occur at a wider level involving networks of individuals that meet and interact within online discussion forums and chat rooms. Some discussion forums function as 'virtual' black markets that advertise, for example, stolen credit card numbers (Holt and Lampke, 2010). Among Chinese cybercriminals, QQ is a popular instant messaging and chat service, as well as the preferred choice for private contact linked to 'carding' – the market in stolen credit cards and their acquisition (Yip, 2011). Given the ephemeral nature of many of the interactions, such networks operate as criminal macro-networks rather than closely knit groups.

Examples of cybercrimes and offenders

The first set of illustrative cases involves individual offenders. All these offenders were male; four were under 30 when they committed their offences, the other two were in their mid-30s. Only one of these cases had a financial motive, although Pearson, the offender, denied this. Cleary and Auernheimer claimed that the reason for their offending was, at least in part, altruistic. They wanted to demonstrate that despite claims to the contrary, the data repository of large corporations and organizations, which kept important confidential information on their clients, was not secure. It is likely that the desire for fame and recognition of their skills also played a part in their actions. Swartz was also motivated by ideology and believed that information should be freely accessible. The two other hackers were pushed by emotional reasons: Chaney by his obsession with celebrities, and Yin, by his desire for revenge after losing his job. Pearson benefited financially from hacking, but he could potentially have stolen much more. The final case illustrates the potential harm that just one cybercriminal might cause. All faced the risk of long prison sentences.

Ryan Cleary: DDoS on SOCA

Police in the UK arrested 19-year-old Ryan Cleary for allegedly orchestrating a distributed denial-of-service (DDoS) attack against the website of the British Serious Organised Crime Agency (SOCA) website in 2011, and the websites of the International Federation of the Phonographic Industry and the British Phonographic Industry during the previous year. Cleary allegedly rented and sublet a large botnet to conduct the attack. He was associated with the hacking group LulzSec, although the group itself denied that he was a member, claiming that he was merely a loose associate. Cleary's arrest followed his exposure by *Anonymous* who published his name, address, and phone number as retaliation for his hacking into the group *AnonOps*' website and exposing over 600 nicknames and IP addresses. Cleary was reported as stating that AnonOps was 'publicity hungry.' He pleaded guilty to most of the charges, and in May 2013 was sentenced to imprisonment for 32 months (*The Guardian* 2013; see also Olson, 2012).

Andrew Auernheimer: Apple iPad Snoop

In June 2010, 25-year-old Andrew Auernheimer managed to obtain the email addresses of 114,000 iPad users including celebrities and politicians, by hacking the website of the telecommunication company AT&T. Auernheimer was a member of the group Goatse Security, that specializes in uncovering security flaws. The attack was carried out when Auernheimer and other hackers realized they could trick the AT&T site into offering up the email address of iPad users if they sent an HTTP request that included the SIM card serial number for the corresponding device. Simply guessing serial numbers, a task made easy by the fact that they were generated sequentially during manufacturing, allowed access to a large number of addresses. Auernheimer and Goatse released details about the attacks to Gawker Media. Shortly after, the FBI arrested Auernheimer in connection with the breach. In March 2013, he was sentenced to 3 ½ years in prison for exploiting an AT&T security flaw (Chickowski, 2011; "Goatse Security," 2013; Thomas, 2013).

Aaron Swartz: Content Downloader

A programmer and fellow at Harvard University's Safra Center for Ethics, 24-year-old Aaron Swartz was indicted in 2011 after he downloaded more than 4 million academic articles through the Massachusetts Institute of Technology (MIT) network connection to JSTOR, an online academic repository. Swartz used anonymous log-ins on the network in September 2010 and actively worked to mask his log-ins when MIT and JSTOR tried to stop the massive drain of copyrighted material. After JSTOR shut down the access to its database from the entire MIT network, Swartz went on campus, directly plugged his laptop in the information infrastructure of a MIT networking room, and left it hidden as it downloaded more content. However, an IT administrator reported the laptop to the authorities. A hidden webcam was installed and when Swartz came and picked up his laptop, he was identified and arrested. Swartz did not steal any confidential data and, once the content of the site had been secured, JSTOR did not wish to initiate legal action; however, federal prosecutors went ahead and charged Swartz with 13 felony counts (*United States of America v Aaron Swartz,* 2012). Swartz was known as 'a freedom-of-information activist' who called for civil disobedience against copyright laws, particularly in relation to the dissemination of publicly funded research. Swartz said he was protesting how JSTOR stifled academic research and that he had planned to make the articles he downloaded publicly and freely available. Swartz committed suicide in early 2013, before his court case was finalised. His family accused the government of having some responsibility for his death because of the overzealous prosecution of what they described as a non-violent victimless crime. In March 2013 he was posthumously awarded the James Madison Award by the American Library Association, a prize to acknowledge those who champion public access to information (Bort, 2013; Cohen, 2013).

Christopher Chaney: Celebrity Hackerazzi

In what amounted to 'cyberstalking', celebrity-obsessed Christopher Chaney, 35 years, used publicly available information from celebrity blog sites to guess the passwords to Google and Yahoo email accounts owned by over 50 stars, including Scarlett Johansson, Mila Kunis, and Christina Aguilera. He successfully managed to hack into the accounts and set up an email-forwarding system to send himself a copy of all emails received by the stars. From November

2010 to October 2011, Chaney had access to emails, photos, and confidential documents. He was responsible for the release of nude photos of Scarlett Johansson that subsequently circulated on the Internet. He was also accused of circulating nude photos of two (non-celebrity) women but he denied this. FBI investigators did not give details of how they tracked Chaney, who was sentenced to 10 years jail in December 2012. Chaney apologized for his actions; he said that he empathized with the victims but could not stop what he was doing (Eimiller, 2011; Chickowski, 2011).

Sam Yin: Gucci Hacker

Fired after being accused of selling stolen Gucci shoes and bags on the Asian grey market, a former Gucci IT employee, Sam Yin, 34 years, managed to hack into the company's system using a secret account he had created while working, and a bogus employee's name. He shut down the whole operation's computers, cutting off employee access to files and emails for nearly an entire business day. During that day he deleted servers, destroyed storage set-ups and wiped out mailboxes. Gucci estimated the cost of the intrusion at $200,000. Yin was sentenced to prison for a minimum of 2 years and a maximum of 6 years in September 2012 (Italiano, 2012).

Edward Pearson: Identity Theft

Originally from York, Northern England, 23-year old Edward Pearson stole 8 million identities, 200,000 PayPal account details, and 2,700 bank card numbers between January 2010 and August 2011. Using the malware ZeuS and SpyEye, which he rewrote to suit his purpose, he managed to not only hack into the PayPal website but also into the networks of AOL and Nokia, which remained down for two weeks. Pearson finally got caught after his girlfriend tried to use forged credit cards to pay hotel bills. He was described as 'incredibly talented' and a clever computer coder, who had been active in cybercrime forums for several years prior to his hacking spree. His lawyer, however, argued that Pearson was not so interested in making money but that hacking was 'an intellectual challenge'. A prosecutor estimated that based on the information he had stolen, he could potentially have stolen $13 million; yet, before his arrest, he had only stolen around $3,700, which he had spent on takeaway meals and mobile phone bills. Pearson was sentenced to 26 months jail in April 2012 (Liebowitz, 2012).

The next set of cases involves small groups or networks of offenders, and illustrates the diversity of criminal organizations operating across crime types. LulzSec was a loose network of like-minded hackers responsible for infiltrating the systems of high profile organizations, supposedly to draw attention to potential security failures. Dreamboard was a members-only group that exchanged illicit images of children. DrinkOrDie was an organization devoted to piracy and the dissemination of pirated content. The four other organizations were motivated by financial profit. Each organization was the target of successful law enforcement action, and, as such, they may not be representative of other organisations whose members managed to avoid prosecution. One common characteristic of these groups was their trans-national reach. Each was comprised of members from different countries and was active across borders. Some members of these groups have been convicted for their cybercrimes.

LulzSec and Sony Hackers

Cody Kretsinger (nicknamed Recursion) was arrested for allegedly carrying out an attack against Sony Pictures on behalf of LulzSec in September 2011. Kretsinger, aged 25, was arrested when the UK-based proxy server HideMyAss, a service that disguises the online identity of its customers, provided logs to police. These allowed them to match time-stamps with IP addresses and identify Kretsinger (Chickowski, 2011; Olson, 2012). In April 2012, Kretsinger pleaded guilty to unauthorised access, conspiracy and attempting to break into computers, and he was later sentenced to one year in jail and 1,000 hours community service. Kretsinger, along with other members of LulzSec, obtained confidential information from the computer systems of Sony Pictures by using an SQL injection attack against the website. They disseminated the stolen data on the Internet. The stolen data contained confidential information such as names, addresses, phone numbers, and e-mail addresses for thousands of Sony customers. The hackers did not use the data illegally but wanted to demonstrate that Sony's website was not secure. Hector Xavier Monsegur, 28, the former alleged leader of LulzSec, was arrested in June 2011 and agreed to act as an informant for the FBI. He provided information on his fellow hackers and is believed to have played an important role in their identification and arrest. Other members of LulzSec included Ryan Cleary (19), Ryan Ackroyd (27), Mustafa al-Bassam (18), Jake Davis (18). All pleaded guilty and were sentenced in May 2013 (Italiano, 2012). On 24 April 2013, the Australian Federal Police (AFP) arrested a Sydney man, Matthew Flannery, known online as Aush0k, alleged to have been the leader of the LulzSec hacking group.

Dreamboard was a members-only group that exchanged illicit images of children under the age of twelve, until its interdiction by a multi-national police investigation begun in 2009. The operation resulted in charges against 72 people in 14 countries across five continents. Servers were situated in the United States, and the group's top administrators were located in France and Canada. Rules of conduct on the site's bulletin board were printed in English, Russian, Japanese and Spanish. It was a very sophisticated operation that vetted prospective members, required continuing contributions of illicit material as a condition of membership, and rewarded those who produced and shared their own content. Members achieved status levels reflecting the quantity and quality of their contributions. The group used aliases rather than their actual names. Links to illicit content were encrypted and password-protected. Access to the group's bulletin board was through proxy servers. These routed traffic through other computers in order to mask a member's true location, thereby impeding investigators from tracing the member's online activity (US Department of Homeland Security, 2011).

DrinkOrDie

DrinkOrDie, founded in Moscow in 1993, was a group of copyright pirates who illegally reproduced and distributed software, games, and movies over the Internet. Within three years the group expanded internationally and counted around 65 members in 12 countries including Britain, Australia, Finland, Norway, Sweden, and the US. The membership included a relatively large proportion of undergraduate university students who were technologically sophisticated and skilled in security, programming, and internet communication. The group was highly organized, hierarchical in form, and entailed a division of labour. A new program was often obtained through employees of software companies; 'crackers' stripped the content of its electronic protection; 'testers' made sure the unprotected version worked; and 'packers' distributed the pirated version to around 10,000 publicly accessible sites around the Internet. The

content was available to casual users and to other criminal enterprises for commercial distribution. Members were not motivated by profit but by their desire to compete with other pirates and to achieve recognition as the first group to distribute a perfect copy of a newly pirated product. DrinkOrDie's most prominent achievement was its illegal distribution of Windows 95 two weeks prior to the official release by Microsoft. The group was dismantled by authorities in 2001 and 20 members were convicted worldwide. Eleven people were prosecuted in the US in 2002 including one woman. They were between 20 and 34 years. Two of the leaders were sentenced to 46 and 33 months jail respectively (US Department of Justice, 2001, 2002).

Dark Market

Dark Market, founded in 2005, was a website providing the infrastructure for an online bazaar where buyers and sellers of credit card and banking details could meet, and illicit material such as malicious software could be purchased. Banking and card details were illicitly obtained by various means, including surreptitious recording at ATMs using 'skimming' devices, unauthorized access to personal or business information systems, or techniques of 'social engineering' where victims were persuaded to part with the details. Initially trading in stolen information occurred on a one-to-one basis, but given the sheer volume of such material, using a forum where prospective parties could interact collectively was much more efficient. At its peak, Dark Market was the world's pre-eminent English language 'carding' site, with over 2500 members from a number of countries around the world, including the UK, Canada, the US, Russia, Turkey, Germany and France. The group was highly organized. Prospective vendors had to prove that they were able to provide useable credit card information, which was assessed for its validity. Members were nominated and vetted. A maximum of four administrators ran the site at any time. They ensured the security of the site, provided an escrow service, and patrolled the site for 'illicit' activity such as dealing in drugs or child pornography. It seemed that reputation and status was more important for these VIP members than was self-enrichment. Ordinary members, who traded in information and used the information they bought to make money, generally sought to keep a low profile. The forum was infiltrated by an FBI agent and the investigation resulted in 60 arrests worldwide. One of the most prominent members, a 33-year-old Sri-Lankan born British man, was sentenced to 5years imprisonment in March 2010 (Glenny, 2011; Davies, 2010).

DNSChanger

Six Estonian men, posing as the legitimate company Rove Digital, were arrested in November 2011 for creating and operating the DNSChanger malware, which allowed them to control Domain Name System (DNS) servers. DNS is an Internet service that converts domain names into numerical data that computers understand. Without DNS and DNS servers, Internet browsing, access to websites, and emails would be impossible. The group was running an Internet fraud operation that enabled them to manipulate Internet advertising. The malware was propagated using social engineering techniques; in one instance, the malware was offered as a video code that was supposedly required to watch adult movies. At its peak, an estimated four million computers worldwide were infected with the malware. DNSChanger worked by substituting advertising on websites with advertising sold by Rove Digital and by redirecting users of infected computers to rogue servers controlled by affiliates of the group. When users clicked on the links to a licit official website, they were in fact taken to a fake website that resembled the legitimate website but promoted counterfeit, and sometimes dangerous, products.

The group allegedly netted $14 million in stolen advertising views. Operation Ghost Click, a five-year collaboration between the FBI and private corporations, began after Trend Micro researchers identified the gang's botnet. The six offenders were aged between 26 and 31 years. It is likely they will all be extradited to the US for trial. A seventh member of the group, a 31-year-old Russian man, has not yet been arrested (US Federal Bureau of Investigation 2011; *Krebs on Security* 2011).

Carberp

Carberp is malicious software designed to steal banking information. When it first appeared in 2009, Carberp was used exclusively by a small, closed group operating only in Russian-speaking countries. In 2011 the malware's creators started selling it to a few customers in the former Soviet Union. In March 2012, following a joint investigation with Group-IB, a Russian cyber security firm, Russian authorities arrested eight Carberp operators. The group was led by two brothers in their late 20s. One of them was already a known criminal with a record related to real estate fraud. The group demonstrated a high level of collaboration. Carberp's group members were working remotely from different cities in Ukraine. Using stolen banking data, they illegally transferred large sums of money into accounts controlled by the group. The money was then withdrawn from a variety of ATM machines in the Moscow area. It is estimated the group had stolen around $2 million from over 90 victims (Warner, 2012).

Despite the arrests, Carberp continued to evolve with added functionality. It has worked with three different cybercrime groups (Matrosov, 2012). The first group had a direct association with the creator of the malware. In 2010 Carberp source code was sold to the organizer of the second group and they worked in parallel to develop a second version. The third group was already engaged in online bank fraud with the botnet Origami Hodprot but switched to using Carberp in 2011. As the botnet grew, the group's operations became increasingly organised and members of the group were highly coordinated. They had command-and-control servers in several European countries and the US, and attacked Russian as well as foreign banks. In December 2012, members from the Carberp team posted messages on underground Russian cybercrime forums, offering a new version of Carberp for rent. At US$40,000 per month, this was one of the most expensive kits thus far advertised. Carberp is said to be more effective and more dangerous than ZeuS and SpyEye, and might soon be able to target US and Australian banks (Constantin, 2012). With various reports of the Carberp source code being available online in mid-2013, there are fears that improved 'copycat' variants may be developed and released in the near future.

'Unlimited Operation'

On 9 May 2013 eight men were charged in New York with stealing US$2.8 million in cash from a number of ATM machines. These men formed the New York cell of an international cybercrime ring running 'unlimited operations'. The headquarters of the cyber gang is located outside of the US, but there may be other cells in the US. The masterminds of the group had hacked the network of global financial institutions to steal prepaid debit card data. They managed to eliminate the withdrawing limit on these cards. Using fake cards manufactured from the stolen data, 'casher crews' were able to withdraw virtually unlimited funds from ATMs around the world. The individuals charged in New York comprised one of these 'casher crews.' It was later found that the leader of the gang had been murdered in April. Six of the seven suspects were under 25 years, and all were US citizens. Two worked as bus drivers for a private

company.[7] The New York gang conducted two successful operations. During the first one, in December 2012, a total of US$5 million was withdrawn in 20 countries. In New York City, the group scoured 140 ATMs, and stole US$400,000 in just 2 hours and 25 minutes. The second operation went for just over 10 hours on 19-20 February 2013. Worldwide, over US$40 million was taken; in New York City, the defendants withdrew US$2.4 million from around 3,000 ATMs. The success of such attacks was attributed to the speed and meticulous planning of these 'unlimited operations'. The New York prosecutor remarked:

> 'Unlimited operations' are marked by three characteristics: 1) the surgical precision of the hackers carrying out the cyber-attacks, 2) the global nature of the cybercrime organization, and 3) the speed and coordination with which the organization executes its operations on the ground. These attacks rely upon both highly sophisticated hackers and organized criminal cells whole role is to withdraw the cash as quickly as possible.' (US Attorney's Office, 2013)

Koobface

Koobface is a worm-based malware that targets Web 2.0 social networks such as Facebook (the name of the malware is an anagram of Facebook). Koobface spread by sending messages to 'friends' of an infected Facebook account user. The message directed the recipient to a fake website where they were prompted to download what was presented as an update to Adobe Flash Player. Once the fake program was installed, Koobface controlled the computer's search engine and directed the user toaffiliated illicit websites offering various scams such as false investments, fake AV programs, fake dating services, etc. The Koobface botnet made money through pay-per-install and pay-per-click fees from these other websites. Sophos identified five potential members of the Koobface gang, also referred to as 'Ali Baba & 4' who operated from Russian and Czech locations. One member was older than the others and possibly the leader, but the structure of the group was not fully understood. Members of the group had previously worked in online pornography, spyware, and also attempted to conduct a legitimate mobile software and services business, MobSoft Ltd (Richmond 2012). The Koobface crime group was able to regularly upgrade and adapt the botnet, which included an effective Traffic Direction System that managed the activity on affiliate sites and boosted the Internet traffic to the botnet (e.g. targeting showbiz fans, online daters, casual porn surfers, and car enthusiasts). The overall structure of the botnet was resilient; it survived takedown attempts and countermeasures by targets such as *Facebook, Google,* and other social networks. Data found in the botnet's command-and-control system suggested the group has earned around $2 million a year.

State and State-sponsored cybercrime

One of the more significant developments in cybercrime over the past decade has been an apparent increase in the volume of illegal activity committed by governments or their proxies. Because of the sensitive nature of such activities, their nature and extent tend to be obscured from public view. Nevertheless, recent disclosures, some noted below, have been informative. One might envisage a continuum of state-private interaction, from state monopoly of criminal activity at one extreme, to state ignorance of private criminal activity at the other. In between these polar extremes, one might find formal collaboration between state and non-state entities; loose cooperation between state authorities and private criminal actors; active sponsorship by the

state; tacit encouragement of non-state crime; the state turning a "blind eye" to the activity in question; and state incapacity to control private illegality. (Stohl, 2014)

PLA Unit 61398

In February 2013, the information security company Mandiant reported that a large scale program of industrial espionage had been undertaken in 2006 by Unit 61398 of the People's Liberation Army. Based in Shanghai, this organization is alleged to have acquired a massive volume of data from a wide variety of industries in Englishspeaking countries. Information alleged to have been taken includes technical specifications, negotiation strategies, pricing documents and other proprietary data. One of the alleged targets, a major US beverage manufacturer, was planning in 2009 what was to have been the largest foreign purchase of a Chinese company to date. It was reported that an apparently innocuous email to an executive of the US company contained a link, which when opened, allowed the attackers access to the company network. Sensitive information on pending negotiations was reportedly accessed by Chinese intruders on a regular basis; the purchase did not eventuate. It is unclear whether the unit is staffed exclusively by military personnel or includes civilian contractors (Mandiant, 2013; Sanger, Barboza, & Perlroth, 2013).

Operation Olympic Games is reportedly a collaboration between the US National Security Agency and its Israeli counterpart, Unit 8200, intended to disrupt the Iranian nuclear enrichment program. It allegedly involved the clandestine insertion of an extremely complex and sophisticated set of software into communications and control systems at the Natanz nuclear facility. The software reportedly includes a capacity to monitor communications and processing activity, as well as the ability to corrupt control systems at the facility. The operation succeeded in delaying the progress of uranium enrichment through remote controlled destruction of a number of centrifuges used in the process. The secrecy surrounding the operation was compromised in part when the malicious software escaped because of a programming error. Neither the United States nor the Israeli governments have yet to acknowledge the existence of the operation (Sanger, 2012).

Conclusion

The above discussion raises two basic questions. The first is whether organizations and individual offenders pursue similar goals. The second is the degree to which the McGuire and Chabinsky typologies fit with the cases we have summarized, and the relationship, if any, between crime type and organizational form. Since the cases in question were not randomly chosen, our conclusions cannot be regarded as definitive. Rather, they are tentative judgments that may serve as the basis for further inquiry.

Although they may not be representative of cybercriminals generally, the individual offenders discussed above appeared less preoccupied with financial gain than with libertarian ideology, technological challenge, celebrity obsession, and revenge against a former employer. This is not to suggest that money doesn't matter to solo cybercriminals. Rather, the observed variation enhances our appreciation of the range and diversity of individual motivations.

Organizations, too, reflected a variety of goals, including defiance of authority, freedom of information, sexual gratification of members, and technological challenge. The profit motive was

more apparent in the organization cases than with individual offenders. One notes the activities undertaken by organizations operating under state auspices, specifically those involving espionage and offensive cyber operations. These have explicit economic and political goals, which most certainly do not include the desire for publicity and notoriety.

A comparison of individual offenders and criminal organizations reveals that both possessed impressive skills. Despite the formidable capacities of some individual offenders, the skills and resources of some organizations were truly extraordinary. This was particularly evident in the cases of state cyber activity, although the work of Drink or Die, Dreamboard and 'Unlimited Operation' all showed considerable complexity and sophistication.

As discussed above, the organizational structure depicted in Chabinsky's model appears more characteristic of a sophisticated, enterprise-like fraud than of other crime types. The "Unlimited Operation" and Koobface cases would appear to provide the best fit. To a lesser extent, the "Drink or Die" group had a division of labor, involving at least six of the ten roles specified in Chabinsky's model. The group's lack of a significant financial motive precluded the need for "cashers" "tellers" and "money mules."

McGuire's typology would also appear reliable in light of the cases we have discussed. The state crime cases appeared to consistent with hierarchy, or, to the extent that non-state actors are involved, with the extended hybrid form. Complex frauds, such as 'Unlimited Operation' are also the work of hierarchies.

As we have noted, "annoyance crime" and relatively complex protest activity such as that involving denial of service, seem most suited to swarm; the work of Anonymous is illustrative. Protest activity of a more *ad hoc*, short term nature, is done by aggregate groups. Illicit markets and organized paedophile activity resemble hubs. To the extent that pedophile activity entails offline offending, it will take the clustered hybrid form.

The study of organized cybercriminal activity is in its infancy. Every new technology and every new application will create an opportunity that criminals will soon seek to exploit. In order to keep abreast of cybercrime it will be important to track the evolution of the organizational forms that these criminal activities will take. This essay has taken a small step in this direction.

References

Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M., Levi, M., & Moore, T. (2012). Measuring the Cost of Cybercrime. Presented at the Workshop on the Economics of Information Security (WEIS), Berlin, Germany. Retrieved from http//weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

Baltazar, J. Costoya, J. & R Flores, R (2009) The Real Face of Koobface: the Largest Web 2.0 Botnet Explained and Show me the Money: The Monetization of Koobface (Trend Micro).<http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_real_face_of_KOOBFACE_jul2009.pdf>.

Ben-Itzhak, Y. (2009). Organized Cybercrime and Payment Cards. Card Technology Today, 21(2), 10–11.

Bhattacharjee, Y. (2011, February). Why Does A Remote Town In Romania Have So Many Cybercriminals. Wired, 19(2).

Bort, J. (2013, March 16). The American Library Association Has Given Aaron Swartz Its First Ever Posthumous Award. Business Insider. Retrieved from http://www.businessinsider.com.au/aaron-swartz-granted-posthumous-award-2013-3

Brenner, S. W. (2006). Cybercrime jurisdiction. Crime, Law and Social Change, 46(4-5), 189–206. doi:10.1007/s10611-007-9063-7

Broadhurst, R., & Chang, Y. C. (2013). Cybercrime in Asia: Trends and Challenges. In Asian Handbook of Criminology (pp. 49–64). Springer.

Broadhurst, R., & Choo, K. K. R. (2011). Cybercrime and Online Safety in Cyberspace. In C. Smith, S. Zhang, & R. Barbaret (Eds.), International Handbook of Criminology (pp. 153–165). Routledge.

Broadhurst, R., & Grabosky, P. (2005). Computer-Related Crime in Asia: Emergent Issues. In R. Broadhurst & P. Grabosky (Eds.), Cyber-crime: The Challenge in Asia (pp. 347–360). Hong Kong University Press.

Chabinsky, S. R. (2010, March 23). The Cyber Threat: Who's Doing What to Whom? FBI. Retrieved from http://www.fbi.gov/news/speeches/the-cyber-threat-whos-doing-what-to-whom

Chang, Y.-C. (2012). Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention Across the Taiwan Strait. Edward Elgar Publishing.

Chickowski, E. (2011, December 7). The Most Notorious Cybercrooks Of 2011 - And How They Got Caught. Dark Reading. Retrieved from http://www.darkreading.com/security/attacks-breaches/232300124/the-most-notorious-cybercrooks-of-2011-and-how-they-got-caught.html

China Daily (2010) Internet Policing Hinges on Transnational Cybercrime. (November 10). Retrieved from http://www.china.org.cn/business/2010-11/10/content_21310523.htm

Cohen, A. (2013, January 18). Was Aaron Swartz Really "Killed by the Government"? Time Ideas. Retrieved from http://ideas.time.com/2013/01/18/was-aaron-swartz-really-killed-by-the-government/

Constantin, L. (2012, December 17). Improved Carberp Banking Malware will Target North American Banks, Group-IB Says. IDG News Service. Retrieved from http://www.computerworld.com.au/article/print/444820/improved_carberp_banking_malware_will_target_north_american_banks_group-ib_says

Council of Europe. (2005). Summary of the Organized Crime Situation Report: Focus on Cybercrime. Presented at the Octopus Interface Conference: Challenge of Cybercrime, September 15-17, Strasbourg.
Cubby, B., & McNeilage, A. (2012, September 17). Police investigate rioters' text messages. Sydney Morning Herald. Retrieved from http://www.smh.com.au/nsw/police-investigate-rioters-text-messages-20120916-260mk.html
Davies, C. (2010, January 14). Welcome to DarkMarket – global one-stop shop for cybercrime and banking fraud. The Guardian. Retrieved from http://www.theguardian.com/technology/2010/jan/14/darkmarket-online-fraud-trial-wembley
Décary-Hétu, D., & Dupont, B. (2012). The social network of hackers. Global Crime, 13(3), 160–175. doi:10.1080/17440572.2012.702523
Eimiller, L. (2011, October 12). Florida Man Arrested in "Operation Hackerazzi" for Targeting Celebrities with Computer Intrusion, Wiretapping, and Identity Theft. FBI. Retrieved October 5, 2013, from http://www.fbi.gov/losangeles/press-releases/2011/florida-man-arrested-in-operation-hackerazzi-for-targeting-celebrities-with-computer-intrusion-wiretapping-and-identity-theft
Glenny, M. (2011). DarkMarket: Cyberthieves, Cybercops and You. New York: Alfred A. Knopf.
Goatse Security (2013) September 22). In Wikipedia. Retrieved from https://en.wikipedia.org/w/index.php?title=Goatse_Security&oldid=570984627
Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets online: products and market forces. Criminal Justice Studies, 23(1), 33-50.International Telecommunication Union. (2013). ICT Facts and Figures. Geneva: ITU. Retrieved from http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf
Italiano, L. (2012, September 10). Ex-staffer sentenced to 2-6 years for hacking into Gucci's system. New York Post. Retrieved from http://nypost.com/2012/09/10/ex-staffer-sentenced-to-2-6-years-for-hacking-into-guccis-system/
Kaspersky Lab Secure list article: "Spam in Q1 2013." (8 May 2013) http://www.securelist.com/en/analysis/204792291/Spam _in_Q1_2013
Krebs on Security (2011) 'Biggest Cybercriminal Takedown in History' (November 11). http://krebsonsecurity.com/2011/11/malware-click-fraud-kingpins-arrested-in-estonia/
Kshetri, N. (2013a). Cybercrime and Cybersecurity in the Global South. Palgrave Macmillan.
Kshetri, N. (2013b). Cyber-Victimization and Cyber-Security in China. Communications of the ACM, (forthcoming).
Liebowitz, M. (2012, April 4). UK hacker sentenced for stealing 8 million identities. NBC News. Retrieved from http://www.nbcnews.com/id/46955000/ns/technology_and_science-security/t/uk-hacker-sentenced-stealing-million-identities/
Lusthaus, J. (2013). How organised is organised cybercrime? Global Crime, 14(1), 52–60. doi:10.1080/17440572.2012.759508
Mandiant. (2013). Mandiant Intelligence Center Report. Mandiant. Retrieved from http://intelreport.mandiant.com/
Marzulli, J (2013) 'Global Cyber, ATM Heist Nets Thieves $45 Million from 26 Countries', NY Daily News, 9 May. <http://www.nydailynews.com/new-york/cyber-thieves-busted-45-million-heist-article-1.1339051>.

Matrosov, A. (2012, July 2). All Carberp botnet organizers arrested. We Live Security. Retrieved from http://www.welivesecurity.com/2012/07/02/all-carberp-botnet-organizers-arrested/
McGuire, M. (2012). Organised Crime in the Digital Age. London: John Grieve Centre for Policing and Security.
Microsoft Security Blog (2010, March 25). Retrieved from http://blogs.technet.com/b/security/archive/2010/03/25/profile-of-a-global-cybercrime-business-innovative-marketing.aspx
Moore, T., Clayton, R., & Anderson, R. (2009). The Economics of Online Crime. The Journal of Economic Perspectives, 23(3), 3–20. doi:10.1257/089533009789176825
Moura, G. C. (2013). Internet Bad Neighbourhoods. Enschede, The Netherlands: Centre for Telematics and Information Technology.
Olson, P. (2012). We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency. Little, Brown.
Pauli, D. (2012, March 22). China is the "World's Biggest Cybercrime Victim. SC Magazine. Retrieved from http://www.scmagazine.com.au/News/294653china-is-the-worlds-biggest-cybercrime-victim.aspx
Richmond, R. 'Web Gang Operating in the Open', New York Times (16 January 2012), <http://www.nytimes.com/2012/01/17/technology/koobface-gang-that-used-facebook-to-spread-worm-operates-in-the-open.html?pagewanted=all&_r=0
Sanger, D. E. (2012). Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power. New York: Crown Publishers.
Sanger, D. E., Barboza, D., & Perlroth, N. (2013, February 18). China's Army Is Seen as Tied to Hacking Against U.S. The New York Times. Retrieved from http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html
Schneider, J. L. (2003). Hiding in Plain Sight: An Exploration of the Illegal(?) Activities of a Drugs Newsgroup. The Howard Journal of Criminal Justice, 42(4), 374–389. doi:10.1111/1468-2311.00293
Sipress, A. (2004, December 14). An Indonesian's Prison Memoir Takes Holy War Into Cyberspace: In Sign of New Threat, Militant Offers Tips on Credit Card Fraud. Washington Post. Retrieved from http://msl1.mit.edu/furdlog/docs/washpost/2004-12-14_washpost_jihadis_online.pdf.
Soudijn, M. R. J., & Zegers, B. C. H. T. (2012). Cybercrime and virtual offender convergence settings. Trends in Organized Crime, 15(2-3), 111–129. doi:10.1007/s12117-012-9159-z
Spapens, T. (2010). Macro Networks, Collectives, and Business Processes: An Integrated Approach to Organized Crime. European Journal of Crime, Criminal Law and Criminal Justice, 18(2), 185–215.
Stohl, M. (2014). Dr. Strangeweb: Or How They Stopped Worrying and Learned to Love Cyber War. In Cyberterrorism: A Multidisciplinary Approach. New York: Springer.
The Guardian (2013) LulzSec "hacktivists" handed long jail sentences for hacking. (May 17). Retrieved from http://www.theguardian.com/technology/2013/may/16/lulzsec-hacktivists-longest-jail-sentences-hacking.
Thomas, O. (2013, March 18). Infamous iPad Hacker Makes No Apologies As He Faces Jail Time. Business Insider. Retrieved from http://www.businessinsider.com.au/andrew-weev-auernheimer-att-ipad-hacker-sentencing-2013-3

United Nations. (2004). A More Secure World, Our Shared Responsibility: Report of the High-Level Panel on Threats, Challenges, and Change (Online Report). Retrieved from http://www.un.org/secureworld/report2.pdf

United States of America v Aaron Swartz, Superseding Indictment (US District Court, District of Massachusetts September 12, 2012). Retrieved from https://www.docketalarm.com/cases/Massachusetts_District_Court/1--11-cr-10260/USA_v._Swartz/53/

United States of America v Fiore et al (2009) http://www.justice.gov/usao/fls/PressReleases/090521-02.html (accessed 29 November 2010).

United States of America v Ross William Ulbricht (2013) Sealed complaint Southern District of New York 27 September http://www1.icsi.berkeley.edu/~nweaver/UlbrichtCriminalComplaint.pdf

United States Attorney, Eastern District of New York (2003) "Press Release: Massive Internet and Credit Card Fraud Bilks Consumers out of $230 Million in Bogus "Free Tours" of Adult Entertainment Websites- Gambino Soldier, Two Executives and 5 Companies Indicted" http://ebookbrowsee.net/cr-03-304-pressrelease-us-v-salvatore-locascio-pdf-d19910473

US Attorney's Office. (2013, May 9). Eight Members of New York Cell of Cybercrime Organization Indicted in $45 Million Cybercrime Campaign. Retrieved from http://www.justice.gov/usao/nye/pr/2013/2013may09.html

US Department of Justice. (2001, December 11). Federal Law Enforcement Targets International Internet Piracy Syndicates.

US Department of Justice. (2002, May 17). Warez Leader Sentenced to 46 Months.

US Federal Bureau of Investigation (2011) Malware click fraud kingpins arrested in Estonia. (2011, November). FBI. Retrieved from http://www.fbi.gov/news/stories/2011/november/malware_110911>;

US Securities and Exchange Commission. In the Matter of Jonathan G. Lebed (2000). Retrieved from http://www.sec.gov/litigation/admin/33-7891.htm; http://www.usdoj.gov/criminal/cybercrime/juvenilepld.htm; http://cbc.ca/cgi-bin/templates/view.cgi?/news/2001/01/18/mafiaboy010118

Wall, D. S. (2012). The Devil Drives a Lada: The Social Construction of Hackers as Cybercriminals. In C. Gregoriou (Ed.), The Construction of Crime (pp. 4–18). Palgrave Macmillan.

Warner, G. (2012, March 20). Russian MVD announces arrest of CARBERP gang. CyberCrime & Doing Time. Retrieved from http://garwarner.blogspot.com.au/2012/03/russian-mvd-announces-arrest-of-carberp.html.

Yip, M. (2011). An investigation into Chinese cybercrime and the applicability of social network analysis. University of Southampton EPrint, 1-4. Retrieved from (http://scholar.google.com.au/scholar?hl=en&q=yip+cybercrime+china&btnG=&as_sdt=1%2C5&as_sdtp=#).

[1] A botnet is a network of individual computers, which have been compromised by malicious software and are controlled by a third-party, usually for the purpose of criminal activities (e.g. sending spam).

[2] Malware stands for 'malicious software' such as worms, viruses, and trojans. Bots or web robots allow a malicious user to control remotely computers infected by malware.

[3] The Internet has been used to communicate a wide variety of content deemed offensive to the point of criminal prohibition in one or more jurisdictions. Such material includes child pornography, neo Nazi propaganda, and advocacy of Tibetan independence, to list but a few. Jihadist propaganda and incitement messages also abound in cyberspace.

[4] Tor is an encrypted re-routing service designed to obscure the original source of an email or website on the Internet, sometimes known as The Onion Router. Law enforcement concerns about the widespread misuse of Tor recently led Japanese police to recommended blocking access to the service to those that misuse it (BBC Technology, 'Japanese police target users of Tor anonymous network', 22 April 2013, <http://www.bbc.co.uk/news/technology-22248692>.

[5] The 2012 Verizon Data Breach Investigation Report identified that 75% of 621 confirmed breaches of data were financially motivated, <http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf>.

[6] Article 2(a) of the United Nations Convention against Transnational Organized Crime defines an 'organized 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 this Convention, in order to obtain, directly or indirectly, a financial or other material benefit'. Article 2(c) clarifies that 'a structured group shall mean a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure'.