Chapter 5 – Organised cybercrime and national security

Peter Grabosky, Regulatory Institutions Network, College of Asia and the Pacific, Australian National University

Abstract: While much cybercrime is committed by lone individuals, a significant amount is accomplished by offenders acting collectively. These groups tend to vary significantly in terms of their structure, goals, criminal activities, and organisational life courses. The nature of these collectivities, and whether organised cybercrime constitutes a national security threat, are the subjects of this chapter. The answer will depend on one's definitions of 'national security' and 'organised cybercrime'. Each of these concepts is problematic; the meaning of national security has been stretched significantly in recent years, while conceptions of organised crime (terrestrial or in cyberspace) have been overly narrow. The chapter concludes that some forms of organised cybercrime can indeed threaten national security, both in a more conventional sense and in ways previously overlooked.

Acknowledgement

An earlier version of this chapter appeared in Korean Institute of Criminology Research Report Series 13-B-01 *Information Society and Cybercrime: Challenges for Criminology and Criminal Justice.* Korean Institute of Criminology and International Society of Criminology, Seoul, 2013.

Introduction

While much cybercrime is committed by individuals acting alone, a significant amount is accomplished by offenders acting in concert. These groups have tended to vary significantly in terms of their structures, their goals, the criminal activities in which they engage, and their organisational life courses. The nature of these collectivities, and the question of whether organised cybercrime constitutes a national security threat, are the subjects of this chapter. The answer will depend on one's definitions of 'national security' and 'organised cybercrime.' Each of these concepts is problematic; the meaning of national security has been stretched significantly in recent years, while conceptions of organised crime (terrestrial or in cyberspace) have been overly narrow. The chapter concludes that some forms of organised cybercrime can indeed threaten national security, both in a more conventional sense and in ways previously overlooked.

National Security

National Security is a term used loosely and for many purposes, not all of them legitimate. Traditionally, national security meant the capacity to deter or to resist the invasion of one's territorial borders by foreign military, naval or air forces. Nowadays, the concept has expanded to embrace a range of factors that might support this capacity, including threats to public health, to education, to welfare, to social cohesion, and to the national economy. In recent years, senior US military officials have spoken of the national debt and global warming as significant national security threats.

One should be cautious about uncritically accepting pronouncements relating to security risks. Historically, national security has been invoked as a justification for domestic political repression, to chill democratic political debate, or to distract public and media attention from shortcomings in governance. The Nixon Administration sought to terminate the investigation

of the Watergate break-in and cover-up on national security grounds. Appeals to national security to justify military intervention are sometimes based on fabricated or exaggerated evidence of threat. The 2003 US invasion of Iraq was rationalised by the threat of weapons of mass destruction in the hands of Saddam Hussein (Bamford 2004). This alleged threat proved to have been greatly over-stated. More recently, national security pretexts in the United States have served to obscure the contours of (and thereby inhibit debate on) the massive electronic surveillance program undertaken by the National Security Agency (*New York Times* 2013).

Organised Crime

Organised crime is a term that means many things to many people. Klaus von Lampe's website (http://www.organized-crime.de/organizedcrimedefinitions.htm) contains 150 definitions. Most if not all of these tend to be mired in the 20th century, too narrow in scope, and too constrained by ideology. Most fail to capture the very significant changes in organisational form that have occurred since the beginning of the digital age.

Traditional definitions of organised crime tended to be based on the profit motive. However, even the most insightful observers of 'terrestrial' organised crime note the intrinsic attraction of excitement, comradeship and other non-material values to participants. Similarly, a great deal of organised criminal activity on the internet is driven primarily by non-monetary considerations. These include the quest for intellectual challenge, individual or group notoriety, lust (in the case of organised paedophile activity), ideology, rebellion, and curiosity. Today, there are many criminal organisations active in cyberspace which do not exist to enrich their members; nor do they practice violence or engage in bribery. Moreover, the traditional view of criminal organisations consisting of full or part time professional criminals was also somewhat simplistic. In cyberspace, no less than in terrestrial space, some criminal organisations have explicit or implicit membership, but may also include a variety of

hangers-on, camp followers, consultants and accomplices, some of whom will be well aware of their complicity in criminal enterprise, while others may not.

Conventional organised crime was characterised as monolithic and hierarchical in nature. The classic 'mafia model' that served as the basis of Cressey's (1972) analysis four decades ago conjured up visions of ethnically-based, pyramidal organisations ruled by 'godfathers' or 'Mr Bigs.' By the 1990s, observers of criminal organisations reported that rather than the work of formal, enduring structures, a significant amount of criminal activity was undertaken by loose coalitions of smaller groups converging temporarily to exchange goods and services (Halstead 1998). The idea of vertically integrated enterprises thus gave way to the metaphor of networks (Williams 2001), which provided a foundation for contemporary thinking about the interrelationships within organised criminal groups and between individual groups (Morselli 2009). Digital technology also facilitates new organisational forms, such as short term opportunistic 'swarms' which can serve criminal ends, and which differ significantly from the traditional hierarchical paradigm of the mid-20th century (Choo and Grabosky 2014).

Today, it requires an exceptionally closed mind to deny that states are also capable of criminal acts. Throughout recorded history, crimes by state actors have occurred in times of peace, as well as during armed conflict. In recent years, there have been allegations of drug manufacture and trafficking, illicit arms transfers, and counterfeiting by agents of the Democratic People's Republic of Korea (Bradsher 2006; Perl 2007). States have also engaged periodically in kidnapping and assassination, at home and abroad. Today, the business of the International Criminal Court is booming, notwithstanding the refusal of some states to submit to its jurisdiction.

Just as the distinctions between public and private sectors have blurred in recent years with regard to legitimate activities such as public-private partnerships, contracting out, and other mechanisms for the co-production of governance (Grabosky 1995), there is a long tradition of public/private collaboration in criminal activity to advance state interests. Administrators of the French Concession in Shanghai during the 1920s and 1930s relied upon the Green Gang to suppress industrial unrest and regulate drug markets (Martin 1996; Wakeman 1995, 123-130). The US Central Intelligence Agency engaged burglars and criminals around the world to conduct break-ins and kidnappings, and enlisted mafia members in an unsuccessful attempt to assassinate Cuban President Fidel Castro (Weiner 2007: 186; 199). Toward the end of the Apartheid era, South African state security engaged criminal groups to assist with 'sanctions busting' and with resisting ANC insurgents (Standing 2003).

Organised cybercrime, whether it is the work of 'conventional' criminal offenders, nation states, or some public/private hybrid, entails a diverse set of organisational forms and motives. The following paragraphs describe a number of organisations whose activities have been reported in recent years. The cases in question are not the product of a representative sample; rather, they have been selected to illustrate the diversity of organised cybercriminal exploits by state and non-state actors alike.

W0nderland was a members-only group that exchanged illicit images of children, until its interdiction by a multi-national police investigation named Operation Cathedral on 2 September 1998. Simultaneous raids in 14 countries revealed a group of 180 individuals from 49 countries around the world who collectively possessed over 750,000 illicit images of children and over 1,800 digitised videos depicting child abuse. The group had been established in the mid-1990s to facilitate file sharing of the images and videos (Russell 2008; Graham 2000). It was a very sophisticated collective that vetted prospective members,

encrypted the information shared amongst them, and periodically rotated the physical location of the servers that supported the group's activities.

Anonymous is a loose group of anarchists based largely on a shared ethos of mischief and resentment of authority, who engage in what Denning (2001) referred to as 'hactivism.' The participants' prevailing ethos of iconoclasm, if not nihilism, began to focus on prominent symbols. The chosen methods were website defacements and distributed denial of service attacks, complemented by online verbal abuse (Olson 2012). Not surprisingly, the website of the US Central Intelligence Agency represented an attractive target. Imbued with the hacker ethos that information should be free, the group also targeted the Church of Scientology because of its secrecy, the Motion Picture Association of America for its proprietary commercialism, and became a supporter of Wikileaks. When the US Government prevailed upon various electronic payment service providers to discontinue processing of contributions to Wikileaks after its publication in 2010 of secret US State Department messages, *Anonymous* orchestrated denial of service attacks against the complying sites (Coleman 2011).

'Drink or Die' was an international group of copyright pirates who illegally reproduced and distributed software, games and movies over the Internet. They were motivated less by profit than by their desire for recognition as the first group to distribute a perfect copy of a newly pirated product. Founded in Moscow in 1993, the group expanded internationally within three years, with members in more than 12 countries including Britain, Australia, Finland, Norway, Sweden, and the United States. Its approximately 65 members were technologically sophisticated, and included IT professionals skilled in security, programming and internet communications, each performing specialised roles (US Department of Justice 2002; Lee 2002; McIllwain 2005; Urbas 2006).

The Ukranian ZeuS Group. Software engineers in Eastern Europe had refined malware known as the ZeuS virus. This malicious code was used by one group of Ukranian hackers to gain access to the computers of individuals employed in variety of small businesses, municipalities, and non-government organisations in the United States. Target computers were compromised when the victim opened an apparently benign email message. With access to the victim's bank account numbers and password details, principals in the Ukraine were able to log on to the target organisations' bank accounts. Accomplices of the Ukranian principals placed notices on Russian language websites inviting students resident in the United States to assist in transferring funds out of the country. These so-called 'mules' were provided with counterfeit passports, and were directed to open accounts in false names in various US financial institutions. When principals in the Ukraine transferred funds from legitimate account holders to the mules' accounts, the mules were instructed to move the funds to accounts offshore, or in some cases, to smuggle the funds physically out of the United States (FBI 2012).

Dark Market was a forum for the exchange of stolen credit card and banking details, malicious software, and related technology. Its website provided the infrastructure for an electronic bazaar-- a meeting place for buyers and sellers of the illicit material. The forum was founded in May, 2005 in order to take advantage of the criminal opportunities presented by the advent of electronic banking and the increasing use of credit and debit cards. Banking and card details were illicitly obtained by various means, including surreptitious recording with 'skimming' devices, unauthorised access to personal or business information systems, or techniques of 'social engineering' where victims were persuaded to part with the details at the request of an ostensibly legitimate source. 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 United Kingdom, Canada, the United States, Russia, Turkey,

Germany and France. Shortly thereafter, having been infiltrated by an undercover FBI agent, the market ceased operation (Glenny 2011).

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 are inclined to discuss the operation (Sanger 2012; Zetter 2014).

Ghost Net was the name given by a group of Canadian researchers in 2010 to a cyber-espionage operation apparently operating from commercial internet accounts in China. The hackers compromised government computers in over 100 countries on several continents; prominent among them was India. They also targeted emails from the server of the Dalai Lama (Markoff and Barboza 2010). The Chinese Government denied involvement, and there was no conclusive evidence to the contrary. There was, however, some evidence of government complicity. Chinese officials have confronted expatriate dissidents returning to China with transcripts of internet chats in which they were involved during their absence. Whether the activity in question was the work of patriotic hackers acting unilaterally, or skilled individuals with guidance from state authorities who were otherwise acting at arm's length, remains unclear. Canadian investigators claim to have found evidence of links to two

individuals in the underground hacking community of the PRC (Information Warfare Monitor 2010).

PLA Unit 61398

In February 2013, the information security company Mandiant reported that a large scale program of industrial espionage had been undertaken since 2006 by Unit 61398 of the People's Liberation Army (Mandiant Intelligence Center 2013; Sanger, Barboza and Perlroth 2013). Based in Shanghai, this organisation is alleged to have acquired a massive volume of data from a wide variety of industries in English-speaking 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 it was 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. The US Government filed criminal charges against Five PLA officers were charged in absentia by the US Department of Justice in 2014 (Schmidt and Sanger 2014).

The Prism Program

The Prism program entails systematic harvesting of digital information by the US National Security Agency (NSA). Outlined five years earlier by Bamford (2008), further classified details of the scheme were disclosed in 2013 by whistleblower Edward Snowden (Gidda 2013). Part of a larger NSA program of data capture, storage and analysis, Prism was assisted by some of the world's more prominent IT companies, including Microsoft, Google,

Yahoo!, Facebook, Pal Talk, You Tube, Skype AOL and Apple. The program reportedly captured and stored a wide range of data, including email, chatroom exchanges, voice-over internet protocol (VOIP), photos, stored data, file transfers, video conferencing, and other social network content (Greenwald 2014). The precise nature of the engagement between the agency and the IT companies remains unclear. In some instances, industry cooperation was required by secret court order; some degree of voluntary cooperation may also have occurred. The legality of such data collection under US law has been challenged; it seems likely that the activity has breached the law of a number of nations whose citizens' communications were intercepted (Donohue 2013).

Public-Private partnerships in Cybercrime

One characteristic of state or state-sponsored cybercrime appears to be its hybrid organisational form. One might envisage a continuum of state-private interaction, from state ignorance of private criminal activity at one extreme, to state monopoly of criminal activity at the other. In between these polar extremes, one might find state incapacity to control private illegality; the state turning a 'blind eye' to the activity in question; tacit encouragement of non-state crime; active sponsorship by the state; loose cooperation between state authorities and private criminal actors; then formal collaboration between state and non-state entities.

One notes that Russian 'patriotic hackers' were allegedly involved in cyber attacks on government servers in Estonia. It has also been suggested that Chinese civilian IT specialists working in one or more universities are linked with the People's Liberation Army. It has been reported that the North Korean Army has trained hackers to commit fraud for the purpose of raising revenue. The North Korean state was allegedly involved with a hacking ring that exploited online gaming sites and generated US$6 million in cash (Greitens 2012). The US National Security Agency spends millions of dollars engaging private consultants

to assist it in collecting and analysing communications intelligence (Bamford 2008; Priest and Arkin 2011, 189-90). Whistleblower Edward Snowden was one of them, having been previously employed by a major government contractor, Booz Allen. In most cases of state or state-sponsored cybercrime, the degree of explicit state involvement remains obscure; this should come as no surprise, as plausible deniability is a valued condition for all criminals, state or private, terrestrial or cyber.

Most types of cybercrime can be committed by individuals or by organisations, although the latter can be capable of activities on a grander scale. At the extreme, operations as complex and sophisticated as *Olympic Games*, the cyber espionage activities of the People's Liberation Army, and the Prism project of the US National Security Agency, require very many hands.

State cybercrime activity tends to involve espionage, surveillance, and destruction or degradation of an adversary's systems. It tends to be motivated by the need to identify and to neutralise perceived national security threats, or to give one's nation a strategic advantage. Conventional organised cybercrime activity is more diverse, and depending on crime type, tends to involve a wider variety of objectives, from financial gain, to sexual gratification, to political protest, to notoriety. Both state and private cybercrime may produce adverse unintended consequences for the perpetrator; state and state-sponsored cybercrime may ironically cause harm to national security.

Iatrogenic security threats

Organisations sometimes inflict damage upon themselves, most commonly through strategic misjudgement. Commonly, they fail to adapt to a changing environment. In the commercial world, businesses may fail to be attuned to market signals. Paoli (2003) describes the lack of adaptability on the part of some traditional Mafia groups: Among the factors she identifies are

the inward focus on family, village and neighbourhood, the inability or unwillingness to broaden the pool of new recruits, and the consequent failure to exploit emerging market opportunities such as the growing illicit arms trade.

Organisations may also suffer from over-extending themselves. Business history is littered with the remains of companies whose directors, blinded by hubris or emboldened by previous successes, sought to expand too rapidly. The overreach of organised crime may also backfire. The assassinations of Sicilian investigating judges Giovanni Falcone and Paolo Borsellino in 1992 were more than just Mafia 'hits.' The massive explosions themselves constituted a political statement, and were obviously intended to discourage further investigative activity. Ironically, these killings had the effect of provoking widespread revulsion to organised crime and of fostering public support for increased law enforcement powers (Cowell 1992; Paoli 2003, p. 204).

The decisions of governments to go to war may be similarly flawed. Far from enhancing their own national security, Napoleon's invasion of Russia and Japan's attack on Pearl Harbor each led to disastrous consequences for the aggressors. The second Iraq war cost the United States one trillion dollars, over 4000 military personnel killed in action, and considerable reputational capital. It incited further Al Qaida activism, and also left Iran unrestrained by what had been a formidable adversary.

Some of the more significant cyber-threats to national security are also self-inflicted. States that commit cybercrime may themselves be weakened as a result, especially when their activities come to public attention. States that present themselves as paragons of virtue, only to be found to have been engaged in criminal activities, may see their moral authority eroded. Hypocrisy tends to be inconsistent with leadership. The state that does not practice what it preaches may lose legitimacy, both domestically and internationally. This appears to have

been the case recently with the United States. In 2013, the US Government became increasingly strident in voicing its displeasure with the Government of the People's Republic of China regarding their programs of economic espionage. President Obama was to raise the issue during his June 2013 summit meeting with President Xi Jianping. However, Obama was upstaged by whistleblower Edward Snowden, who disclosed the Prism program and thereby revealed that the United States was itself engaged in a massive program of telecommunications interception.

Once it becomes public knowledge, the modus operandi of state cybercrime may well enhance the capacity of ordinary cybercriminals and other states. The escaped 'Stuxnet' virus, reportedly used in the operation against Iranian nuclear enrichment facilities, is now available for use or further refinement by rogue states and cybercriminals, organised or acting alone.

The potential for 'conventional' organised cybercrime to threaten national security is real. Its likely impact, however, is by no means constant across all nations. All else equal, states with weak economies and those lacking in social cohesion face a greater security risk than robust developed nations. Relatively disadvantaged nations may be less able to afford the IT security infrastructure to protect state and private information systems (such as they are), particularly those supporting financial services. They may also lack the regulatory and enforcement resources to prevent and control cybercrime. But the more fortunate nations themselves may be attractive targets to cybercriminals. They contain a larger number of targets, both symbolic and material.

In addition, state or state-sponsored cybercrime may inspire imitative criminal behaviour by other states and individuals alike. Leadership can function in a wholly unsuitable manner. Moreover, states can also provide imitators with a vocabulary of extenuation, a means of

rationalising or neutralising criminal acts. The appeal to a higher purpose, the argument that the end justifies the means, will be particularly resonant with other states. History has shown that many states have pursued objectives which they at the time regarded as honourable, but which turned out to be terribly perverse.

The full consequences of Operation Olympic Games are uncertain, as neither the victims nor the perpetrators are inclined to discuss it. With knowledge of the operation now widespread, and some of the software elements in the public domain, there are individuals and organisations who may follow the example of perpetrators and engage in cyber attacks for their own purposes. The ultimate consequences of this potential turn of events are unpredictable. Recent electronic attacks against US financial institutions and Saudi oil facilities may represent two examples (Perlroth 2012; Perlroth and Hardy 2013).

Conclusions

Not all organisations acting illegally in cyberspace may be regarded as threats to national or international security. Some of their activity is unquestionably annoying, offensive in the extreme, and/or harmful. There are online activities which, if writ large, might conceivably weaken the integrity and economy of states and thus come to be regarded as security threats. Online paedophilia, no matter how heinous or distasteful one might regard it, does not occur on a scale at which a nation's economy or social fabric is damaged. Nor is it likely ever to do so. The software and entertainment industries in the United States have sought to make the case that information piracy costs the domestic economy millions of dollars in lost profits, and has a chilling effect on entrepreneurialism and creativity world-wide. However, the US economy is sufficiently diverse and vigorous that its future strength will depend on other factors. Indeed, one could argue that piracy allows citizens of less developed countries to benefit from access to products that they would otherwise be unable to afford. By contrast,

major, persistent industrial or political espionage on a wider scale may well threaten the security of the target state. Industrial espionage can weaken the international competitiveness of a company or of an industry sector. When the information in question relates to weapons systems, the security implications are obvious. Theft of credit card and banking details, were it to occur on a larger scale, would certainly impede commercial activity, with corresponding harm to a state's economy. For the time being, however, online fraud appears manageable. Technologies of information security continue to be refined, and tech savvy members of the public, at least in developing countries, are able to protect themselves. On-line banking and e-commerce continue to thrive.

In less developed countries, however, where users are just entering the digital age, lack of awareness of cybersecurity may enhance the vulnerability of individuals and of organisations in both the public and private sectors. To the extent that the threat of cybercrime impedes the development of electronic commerce, it could contribute to the weakening of a nation's economy, and by extension, its security.

As far as organisations are concerned, it appears that the greatest threats to national security are posed by states themselves, either singlehandedly or in collaboration with skilled non-state actors. Resources available to the strongest states are indeed formidable, and we have seen them used with considerable effect. The activity reported to have led to the destruction of Iranian centrifuges would certainly be defined by authorities of that country (or those of any other nation on the receiving end of a similar attack) as a security threat. So too would denial of service attacks that degrade government information systems or those servers that support critical infrastructure. Indeed, nations on the receiving end of such attacks might be inclined to regard them as acts of cyber-war (Turns 2012).

The activities of *Anonymous*, for example, eavesdropping on a conference call between law enforcement agents and attempts to shut down the website of the Central Intelligence Agency, have certainly been found annoying by authorities in the United States. On the scale at which they were conducted, activities of this kind were certainly embarrassing, but would not constitute harm to national security. However, if undertaken persistently or on a larger scale, they might convey the impression of state nonchalance at best, and incompetence at worst, and thereby invite imitation from many quarters. The potential for significant harm is therefore real, if perhaps somewhat distant. The threshold of objective threat would appear to be a function of the scope and intensity of criminal activity on the one hand, and the resilience of the state and its infrastructure on the other.

Other security threats may be self-inflicted by states, as the result of their own cybercriminal activity. The threat intensifies when the illegality in question reaches public attention. This is not to suggest that the only crime is 'getting caught.' Any illicit activity on the part of the state runs the risk of detection and exposure, whether by insiders or external adversaries.

If organised cybercrime were to occur on a greater scale, it could lead to a weakening of trust in major public or private institutions. The fundamental question for our purposes is at what point does the nature and scale of online criminal activity (organised or otherwise) begin to constitute a security threat. National security is not a binary variable. The question is not 'are you, or are you not, secure?' but rather 'might a specific circumstance contribute to an enhancement or diminution of security?'

Bibliography

Bamford, James (2004) *A Pretext for War* New York: Doubleday.

Bamford, James (2008) *The Shadow Factory: The NSA from 9/11 to the Eavesdropping on America* New York: Random House.

Bradsher, Keith (2006) 'North Korean Ploy Masks Ships Under Other Flags' *New York Times*, October 20 http://www.nytimes.com/2006/10/20/world/asia/20shipping.html?pagewanted=print (accessed 25 July 2014).

Choo, Kim-Kwang Raymond and Grabosky, Peter (2014) 'Cyber Crime' in Paoli, L. (ed.) *The Oxford Handbook of Organized Crime* New York: Oxford University Press.

Coleman, Gabriella (2011) Anonymous: From the Lulz to Collective Action *The New Everyday*, 6 April. http://mediacommons.futureofthebook.org/tne/pieces/anonymous-lulz-collective-action (accessed 25 July 2014).

Cowell, A. (1992) Sicilians Jeer Italian Leaders at a Funeral Protest, 22 July, *The New York Times*, http://www.nytimes.com/1992/07/22/world/sicilians-jeer-italian-leaders-at-a-funeral-protest.html (accessed 25 July 2014).

Cressey, Donald R (1972) *Criminal Organization: Its Elementary Forms* London: Heinemann Educational Books.

Denning, Dorothy (2001) 'Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy' in Arquilla, John and Ronfeldt, David F (eds) *Networks and Netwars: The Future of Terror, Crime, and Militancy* Santa Monica: RAND Corporation.

Donohue, Laura (2013) 'NSA Surveillance May be Legal — But it's Unconstitutional' *The Washington Post*, 21 June http://articles.washingtonpost.com/2013-06-

21/opinions/40110321_1_electronic-surveillance-fisa-nsa-surveillance (accessed 25 July 2014).

Federal Bureau of Investigation (FBI) (2012) 'Press Release: Another Cyber Fraud Defendant Charged in Operation Aching Mules Sentenced in Manhattan Federal Court'. 23 March. http://www.fbi.gov/newyork/press-releases/2012/another-cyber-fraud-defendant-charged-in-operation-aching-mules-sentenced-in-manhattan-federal-court (accessed 25 July 2014).

Gidda, Miren (2013) 'Edward Snowden and the NSA Files – Timeline' *The Guardian*, Friday 26 July http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline?INTCMP=SRCH (accessed 25 July 2014).

Glenny, Misha (2011) *Dark Market* New York: Knopf.

Grabosky, Peter (1995) 'Using Non-governmental Resources to Foster Regulatory Compliance', *Governance: An International Journal of Policy and Administration*, 8, 4, 527-50.

Graham, William R, Jr (2000) 'Uncovering and Eliminating Child Pornography Rings on the Internet: Issues Regarding and Avenues Facilitating Law Enforcement's Access to "Wonderland"' *Law Review of Michigan State University- Detroit College of Law*, 2000, 457-84.

Greenwald, Glenn (2014) *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State* New York: Metropolitan Books.

Greitens, Sheena (2012) ‘A North Korean Corleone’ *New York Times*, March 12 http://www.nytimes.com/2012/03/04/opinion/sunday/a-north-korean-corleone.html?pagewanted=all (accessed 25 July 2014).

Halstead, Boronia (1998) ‘The Use of Models in the Analysis of Organized Crime and Development of Policy’ *Transnational Organized Crime* 4, 1. 1–24.

Information Warfare Monitor (2010) ‘Shadows in the Cloud: Investigating Cyber Espionage 2.0’ http://www.nartv.org/mirror/shadows-in-the-cloud.pdf (accessed 25 July 2014).

Lee, Jennifer (2002) ‘Pirates on the Web, Spoils on the Street’. *New York Times*, 11 July, 2002 http://www.nytimes.com/2002/07/11/technology/pirates-on-the-web-spoils-on-the-street.html?pagewanted=all&src=pm (accessed 25 July 2014).

McIllwain, Jeffrey (2005) ‘Intellectual Property Theft and Organized Crime: The Case of Film Piracy’ *Trends in Organized Crime*, 8, 4, 15-39.

Mandiant Intelligence Center (2013) *APT1: Exposing One of China's Cyber Espionage Units* http://intelreport.mandiant.com/ (accessed 25 July 2014).

Markoff, John (2009) ‘Vast Spy System Loots Computers in 103 Countries’ *New York Times* 28 March http://www.theglobeandmail.com/technology/meet-the-canadians-who-busted-ghostnet/article1214210/?page=all (accessed 25 July 2014).

Markoff, John and Barboza, David (2010) ‘Researchers Trace Data Theft to Intruders in China’ *New York Times*, 5 April http://www.nytimes.com/2010/04/06/science/06cyber.html?pagewanted=all (accessed 25 July 2014).

Martin, Brian G (1996) *The Shanghai Green Gang: Politics and Organized Crime 1919-1937* Berkeley: University of California Press.

Morselli, Carlo (2009) *Inside Criminal Networks* New York: Springer.

New York Times (2013) 'More Fog from the Spy Agencies' *New York Times*, 31 July http://www.nytimes.com/2013/08/01/opinion/more-fog-from-the-spy-agencies.html?emc=edit_tnt_20130731&tntemail0=y (accessed 25 July 2014).

Olson, Parmy (2012) *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency*. New York: Little, Brown.

Paoli, L. (2003) *Mafia Brotherhoods: Organized Crime Italian Style*. New York: Oxford University Press.

Perl, Raphael (2007) Drug Trafficking and North Korea: Issues for US Policy Washington DC: Congressional Research Service.http://fas.org/sgp/crs/row/RL32167.pdf (accessed 20 May 2013).

Perlroth, N. (2012) 'In Cyberattack on Saudi Firm, US Sees Iran Firing Back' *New York Times*, October 23 http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all (accessed 25 July 2014).

Perlroth, N. and Hardy, Q. (2013) 'Bank Hacking Was the Work of Iranians, Officials Say' *New York Times*, 8 January http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html (accessed 25 July 2014).

Priest, Dana and Arkin, William (2011) *Top Secret America: The Rise of the New American Security State* New York: Little Brown.

Russell, Gabrielle (2008) ‘Pedophiles in Wonderland: Censoring the Sinful in Cyberspace’ *Journal of Criminal Law and Criminology*, 98, 4, 1467-500.

Schmidt, M. S. and Sanger, D. E. (2014) ‘5 in China Army Face US Charges of Cyberattacks’ *New York Times* 19 May http://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html# (accessed 25 July 2014).

Sanger, David (2012) *Confront and Conceal: Obama’s Secret Wars and Surprising Use of American Power* New York: Crown Publishers.

Sanger, D., Barboza, D. and Perlroth, N (2013) ‘Chinese Army Unit Is Seen as Tied to Hacking Against US’ *New York Times* 18 February. http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all (accessed 25 July 2014).

Turns, David (2012) ‘Cyber Warfare and the Notion of Direct Participation in Hostilities’. *Journal of Conflict Security Law*, 17, 2, 279-297.

Standing, Andre (2003) *The Social Contradictions of Organized Crime on the Cape Flats.* Institute for Security Studies Occasional paper 74. Pretoria: Institute for Security Studies.

US Department of Justice (2002) Warez Leader Sentenced to 46 Months (17 May 2002) http://www.justice.gov/criminal/cybercrime/press-releases/2002/sankusSent.htm (accessed 25 July 2014).

Urbas, Gregor (2006) ‘Cross-national Investigation and Prosecution of Intellectual Property Crimes: The Example of “Operation Buccaneer”’ *Crime, Law and Social Change*, 46, 207-21;

Wakeman, Frederick Jr (1995) *Policing Shanghai, 1927-1937* Berkeley: University of California Press.

Weiner, Tim (2007) *Legacy of Ashes: The history of the CIA* New York: Doubleday.

Williams, Phil (2001) ‘Transnational Criminal Networks’ in Arquilla, John and Ronfeldt, David (eds.) *Networks and Netwars* Santa Monica: Rand Corporation.

Zetter, Kim (2014*) Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon* New York: Crown.