Internet Mafias? The Dis-Organisation of Crime on the Internet

David S. Wall

Introduction

One of Prof. Ernesto Savona's major contributions to the longstanding debate over organised crime has been to encourage students and colleagues to question common assumptions held about organised crime and Mafia and to encourage academics to take a critical approach in their own analyses. Such an approach ensures that myths become supplanted (or displaced) by empirical evidence and encourage more useful operational concepts to be developed. See, for example (out of many examples), his work on mapping out organised crime (Adamoli et al. 1998) or his work on enablers of organised crime, as chair of a high profile committee (Savona 2012). It is critical work such as Prof Savona's which has driven my own investigations into the organisation of cybercrime. Central to my own research has been a challenge to the tacit, and often completely unfounded, assumption that the internet and society have been brought to their knees by organised crime groups. Furthermore, there is an uncritical assumption, also found in many media reports and also police and some academic practice, that these organised crime groups are Mafia driven. Often presented without any evidence or challenge to conventional wisdom, such reductionism not only confuses the public, but can also cause police and researchers looking for 'truth' to look in the wrong direction for their evidence.

Drawing upon existing literature and an analysis of the structure of known cybercrime gangs, this chapter focuses upon deconstructing the 'Mafia' model when understanding the organization of cybercrime. It introduces instead, for want of a better description, a 'disorganised' model for understanding cybercrime. The first part will explore the ways that criminal behaviour has been transformed by new technology. The second part will draw upon a simple analysis of the structures of known/apprehended 'cybercrime gangs' to look at the way that the organization of criminal behaviour has been transformed (described in full in Wall, forthcoming).

D. S. Wall (✉)
School of Applied Social Sciences,
Durham University, 32 Old Elvet, DH1 3HN Durham, UK
e-mail: d.s.wall@durham.ac.uk

S. Caneppele, F. Calderoni (eds.), *Organized Crime, Corruption and Crime Prevention,* DOI 10.1007/978-3-319-01839-3_26,

The third part will compare the organization of known cybercrime gangs with what is known about the way that new threats are organised in order to draw out any similarities or differences. The final part will consider new enterprise and networked methodological approaches to the subject as well as new techniques such as criminal network analysis in order to further understand the organization of new forms of cybercrime.

Two decades on since the birth of the internet, it is clear that the cybersecurity threat landscape has changed as networked technologies have transformed the way that crime (cybercrime) is organised. As policing techniques develop to address the challenges of cybercrime (Wall 2007b) the question being posed today is how is crime organised online and by whom? The (personal, corporate, national) information security debates over the organization of cybercrime are still dominated by a paradigm of traditional thinking about organized crime, namely the tendency by commentators to assume that the organization of cybercrime and cybercriminals naturally follows the hierarchical traditional (Mafia) model of organised crime. There is, therefore, the need to develop a more accurate and 'nuanced' explanation of the organization of cybercrime. Particularly as it also shapes cybercrime policy and the discussions over who is ultimately responsible for policing cybercrime. What the explanations based upon the common assumption fail to acknowledge is that the internet has transformed the organization of crime in substantially different ways to the organization of more traditional crimes. In a nutshell, networked technologies create an environment in which there is no need to commit one large risky crime anymore because one person can now commit many small crimes with lesser risk to themselves. Such crimes fall in one or more of the three generic cybercrime groups found on the internet defined by, firstly, *Modus Operandi*: Crimes against the machine (hacking etc.); Crimes using the machine (frauds etc.) and Crimes in the machine (pornography, hate speech, but also social networking originated offences). Secondly, there is *mediation by technology*: crimes that use the internet to crimes; crimes that are the spawn of the internet and a range of hybrid crimes (e.g. frauds) that fall in between. Thirdly, cybercrimes can be differentiated by *security concern* (victim group)—personal, corporate and national security (see Wall 2005/10). Each has different implications for understanding the organisation of cybercrime.

The Internet and Criminal Activity in a Nutshell

Generally speaking, the internet and its networked technologies have transformed criminal behaviour in six major ways. Firstly, they not only *globalise* the communication of information, ideas and desires, but they also impact locally by creating a *glocalising* effect—the global impact upon the local. Secondly, they create the potential for *asymmetric* as well as *symmetric relationships*—one person can address many others at the same time (and also allow the many to also talk to the few). Thirdly, the surveillant aspects of the technology not only allow *panopticism*—where the many do not know when the few are watching them and so mediates their behaviour, but

they also allow for *synopticism* where 'the many' can also watch 'the few' with a simultaneous mediation of behaviour. Fourthly, and relevant to the previous point, every transaction on the internet leaves a *data trail* (data doubling, data trails, and the disappearance of disappearance) that, with the right resources, can be traced. Or it can be used to mediate our general internet experience (e.g. tracking cookies) and preferences. Fifthly, network technologies and associated media are creating *new forms of networked social relationships* (social media networks) that can be very beneficial, but are also the source of new criminal opportunities (Wall 2007). The upshot is that crime can now be global, asymmetric, synoptic and panoptic, and data trails can be captured to entrap victims. Which leads on to the sixth impact, namely, networked technologies and new social media and the five impacts described above also providing new forms of criminal opportunity that are *changing the way that crime is taking place*. Indeed criminal labour itself is becoming rapidly becoming deskilled and reskilled simultaneously (Wall 2007). The level entry skills of cybercrime have dropped as the technological developments of network technology (malware and delivery mechanisms) that help criminals have become automated to the point that malware can now be rented or bought off the self. Another significant development is that the cost of technologies is now relatively low, thus reducing start up costs.

The impact of these transformations upon crime is that offenders can now commit offences that were previously beyond their financial and organizational means, and on a global scale. Significantly, one person (or a few) can now control a whole criminal process or part thereof, which has profound implications for our understanding of the organization of cybercrime. In a rather cynical way the internet has effectively democratized crimes such as fraud that were once seen as the domain of the powerful and the privileged, however, there is a debate afoot that a new internet mafia is forming. We therefore need to deconstruct the organised crime debate as it applies to the internet.

Deconstructing the Organised Cyber-Crime Debate

Debates about organised cybercrime and the internet are likely to run and run because the topic is so highly emotive and newsworthy, especially when media and academic commentators continue to resort to dramatic convenient stereotypes of traditional-hierarchical organised crime groups or 'Mafias' when there is a dearth of facts. This simplification of the relationship between organised crime and the internet is based upon a powerful cultural logic, especially as the various statistics clearly show that the internet is increasingly being by used by fraudsters to steal large amounts of money from innocent victims, or by hackers to obtain information and disrupt business or governmental processes. The main challenge, however, for policy makers and practitioners is to identify exactly who the fraudsters and hackers are and how they are organised because, despite the hyperbole, comparatively little is known about them or how they are organised. Until more research is undertaken to understand the

nature of organised crime online then the existing assumptions will carry the day. Whilst the mythology of organised crime remains intact, then so does the potential for misshapen public demands for security, distortions in the formation of policy and ultimately the mis-allocation of resources.

It will be argued here that the debate over organised crime online can only be advanced by looking at the ways that crime is organised online. The discussion will therefore begin by briefly describing the current debate over organised crime online and drawing upon known examples of the organization of cybercrime. In order to illustrate how 'true' cybercrimes—those which are wholly mediated by the internet are being organised, an analysis of new cybercrimes and cybercrime gangs (groups) will follow. The new cybercrimes are Stuxnet, a professional form of malware; Scareware (fake antivirus), a relatively new form of malicious software, and the whistleblowing and hacking associated with Wikileaks. It will be shown that the organization of crime online, when it involves 'true' cybercrimes (Wall 2007a, 47), does not lend itself to traditional 'Mafia-type' command and control analogies; furthermore, it is arguable that the networked technologies that facilitate cybercrime could, would likely, oppose attempts to impose control over them. Instead, it will be argued that the organization of crime online follows a different logic, an observation which has implications both for law enforcement as well as cybercrime prevention because it is a logic that lends itself to a relativist rather than absolutist conceptualisation of cybercrime. In other words, we have to accept that, by its very nature; cybercrime (along with the internet) characteristically evolves in order to evade attempts to control it and therefore can never be eradicated; only managed.

In her study of organised criminal activity on the internet, Susan Brenner predicted that organised cybercrime would most likely manifest itself in 'transient, lateral and fluid' forms, as networks of criminals (Brenner 2002, p. 1) rather than replicate the 'gang' and hierarchical American 'Mafia' models of organised criminal activity found offline in the terrestrial world. This is mainly because offline or kinetic/ physical crime organizations have evolved largely in response to real world opportunities and constraints that are largely absent in cyberspace. In support of Brenner's 2002 prediction, there have since been a number of examples of the emergence of new forms of online criminal organization, but they differ greatly from the command and control mafia model. The finding in 2004 by a German Magazine *C'T*, for example, that virus writers had been selling the IP addresses of computers infected with their remote administration Trojans to spammers (C'T 2004; Wall 2007) was significant because it was some of the first published evidence of botnets (following the botnet explosion in 2003/04). Another example arose in June 2005 when the NISCC (National Infrastructure Security Coordination Centre) warned users about 'a highly sophisticated high-tech gang' reputed to be located in the far-East using various distributed means, including botnets, to infect sensitive computer systems to steal government and business secrets (NISCC 2005; Warren 2005).

A further example arose from 'Operation Firewall' in 2004 and 2005 which led to the investigation and prosecution of 'shadowcrew', an international identity theft network which hosted online forums that shared information about stealing, trading and selling personal information that could be used to commit frauds. The various reports

of the investigation and prosecution illustrate how different the groups/ cells were in terms of their networked organization. The, then, head of e-crime at the Serious Organised Crime Agency (SOCA) observed that the Shadowcrew worked 'remotely, without ever needing to meet', which is 'typical of how the new e-crime networks operate compared to the old-style "top down" organised crime groups' (Rodgers 2007). These groups have a very detailed division of labour with specific skill sets rather than the 'usual pyramid structure'. One person would provide the documents, 'another would buy credit card details, and another would create identities while another would provide the drop address' (Rodgers 2007). Together these examples, and also those of other known cybercrime gangs operating between 2000–2010 illustrate the relatively new forms of networked criminal organization that depart from traditional thinking about hierarchically organised crime. Although these gangs specialised in a range of different offences, they displayed similar forms of organization. Word length does not allow for in-depth analysis of each, but briefly, they display common characteristics in that they are fairly ephemeral and amorphous in terms of organization and flex according to demands and opportunities of the day. They also seem to be mostly self-contained and almost akin to small cottage-industries in structure. For further details, see for example, Wall (2010c; forthcoming); Yip et al. (2013). They can be driven by an individual or by a very small group, but not always, because the organising principle is often a central common idea or even ethic. Just because they are Russian or Eastern European in origin, or are based upon servers in those countries, is not prima facie evidence of a link to traditional organised crime. Indeed, the new networked technologies used are relatively cheap, so there are comparatively few start-up costs and little upfront investment, plus they are online and do not need street protection—thus evading two well known hooks of traditional organised crime organizations.

The key difference between cybercrime and traditional crime is its informational nature, networked structure and global reach (see BBC 2007; Goodin 2007a, b). True cybercrimes, those solely the product of the internet, but also those hybrid traditional crimes which have globalised opportunities are very different from traditional crimes that use the internet (Wall 2007, 44–46). They are best understood as reflections of the new forms of social behaviours that are being fostered by networked technologies. So we find that cybercrime is increasingly taking on a 'Wikicrime' form of peer-production, for want of a better description (after Tapscott and Williams 2007), as its organization follows a Wiki model of organization characterised by online collaborations rather than the 'command and control' Mafia model that is assumed by many. A useful example of such a collaboration is the account in Wall 2007, 66–68) of an online group instructing a 'newbie' how to commit a hack. In this example, the group, because I resist using the term 'gang', in question is ordered only by a respect hierarchy and it is organised around the common interest in hacking chip security (for satellite receivers) and driven by a reputational economy. It is a model that persists and is common to later cybercrime types. In many ways cybercrimes, by their very informational, networked and global nature, go against the very grain of the traditional model of organised crime. As observed earlier, cybercriminals evade control by traditional organised crime groups in much the same way as they evade control by, say, government.

Three Paradigm Shifts in Cybercrime

Before exploring the gangs, there have recently been three major shifts in cybercrime and their organization. Stuxnet is a crime against the machine, scareware fraud is a crime using the machine and Whistleblowing is (potentially) crime in the machine because of the appropriation of data. Each of the three show, and especially Scareware, how the organization of a true cybercrime mostly imitates a flat (e-commerce business type) organizational models rather than the hierarchical command and control model invoked in debates about organised crime.

Recent Example of New Crimes Against the Machine—Stuxnet

The Stuxnet worm is a form of malware that can be used to sabotage industrial control systems (SCADA). It is significant because of its complexity. What is known, or deduced, about its organization is that it was created by a hacker group commissioned by, or with links to government (Halliday 2010). The organization of Stuxnet's creation suggests that there is a small core group (e.g. possibly as small as four or five people), with a broader group from whom specific expert help would be provided (Halliday 2010). It is also believed that the constructors also obtained key information about the targets from insiders within the organization who made the machines the software was being designed to attack (Falliere et al. 2010). Although Stuxnet is not unique in requiring insider complicity, see, for example, the Hydraq Trojan (Symantec 2010; Wall 2013), it has, however, raised the risk stakes and has highlighted the insider threat issue. The discovery of custom-built variants will likely continue this practice (Zetter 2011). The example suggests a small organizational group that draws in assistance and information from outsiders. What is not known is whether the assistance was complicit or obtained illegally.

Recent Example of New Crimes Using the Machine—Scareware

'Scareware', or fake antivirus software, is a type of malicious software that defrauds its victims by scaring them into paying for software that offers to fix their computer. Sometimes referred to 'rogueware', which is a less precise descriptor, it signifies an important trend in the evolution of cybercrime. Not only is it a good example of a 'true' cybercrime being spawned purely by the internet (see further Wall 2007), but possibly for the first time, it provides evidence of a complete crime being committed entirely by malicious software (Malware) in large numbers. The malware not only infects the victim's computer and conducts the scam, but it also takes the victim's money and deposits it into the offender's bank account. It represents the complete automation of the crime. Other prevalent forms of 'true' cybercrime such as Phishing (ID Theft), by comparison, may also be automated by software, but only

to the extent that they scam, or socially engineer, personal financial information from victims and send it directly to the offenders. Offenders then need to employ a third party, typically a 'money mule', to use the stolen ID information to remove money from victim's accounts and pass it onto them (Leyden 2010b).

The organization of a typical scareware operation is effectively a 'criminal' reflection of the structure of the 'Affiliate Marketing' business model; the popular internet based e-retailing practice (see Duffy 2005). The 'Affiliate' model is not just found in cybercrimes that use computers, such as fraud, but also in the organization of crimes against the machine (crimes against computer systems such as hacking etc.) and crimes in the machine (those crimes relating to the content of computers such as extreme pornography etc). A successful scareware project will require the establishment of a financial partnership between the 'Merchant' (or 'Kingpin') whose ideas initiate the project and who has access to the malware to be used. An 'Affiliate' will introduce the Merchant to the Consumer ('victims') by infecting their computers with the Kingpin's malware to encouraged victims to part with their money. The Affiliates tend to be employed on a pay-per-install basis and employ highly specialist computing techniques that use complex attack chains to infect mass numbers of victim's computers with the malware. As found with legitimate mainstream Affiliate Marketing practices, a secondary tier of players, the 'brokers', has subsequently emerged to provide websites that bring together Kingpins and Affiliates and broker their relationship on a commission basis (see further the work of Carlo Moreselli).

The relationship between the various actors involved is not the often assumed 'command and control' Mafia-type relationship, quite the opposite because the participants are distributed. In fact, it is probable that they will never meet, so their relationships tend to be ephemeral and project based. Today, Kingpins seek to conduct their business as quietly and 'professionally' as possible so as not to arouse their victims' suspicions. This is a marked change from the past when they used shock tactics to distress victims into paying up.

The implications of the scareware scam, its feasibility, its relative technical simplicity and the potential size of the yield are three fold for our understanding of the organisation of cybercrime. Firstly, it is highly likely that the overall number of offenders trying to emulate the financial success of the 'pioneer Kingpins' will quickly increase in number to dilute the market and diminish the individual yield and attractiveness of this sort of crime. Secondly, although the growth in size of the offender pool will increase the numbers of different scareware programmes circulating, many of these will be 're-skinned' (given a new appearance) or reverse engineered to create copies or variations of the originals. This means that the security industry, using its CAPTCHA software (or alternative) to discern between real and computer inputs and detect scareware and associated malware such as the spams which infect computers, can quickly close down the scammer's window of opportunity. It is also the case that press coverage of the threat reports which identified the initial scams informs computer users of the threat and makes them more suspicious of scareware, further reducing the likelihood of victims falling for the scam. Thirdly, since there is now so much to gain financially, then the Kingpin's already accumulated criminal wealth and its associated power may be used to protect their own interests by 'policing' new

offenders who enter the crime market. A trend found in 2009 and later with some of the more scurrilous scareware has been to encourage victims to buy the scareware solution bundled with branded (but often counterfeit) proprietary security software (e.g. Norton or McAfee etc.) at discounted rates to offset the victim's costs, but also to increase the victims trust because of the associated brand linkage. Of course the additional package rarely arrives or is counterfeit. Such activity threaten the business of both the stealthy Kingpin and also the legitimate security industry who will effectively act alongside (though not with) the former to protect their own interests by seeking to close down the offender.

It may even be the case that some of the original scareware Kingpins have already begun to abandon, re-skin or redeveloped their scareware in favour of more quasi-legitimate versions. The advent of this type of wholly automated crime means that we are entering the era of "the long tail" of crime, mimicking Chris Anderson's 2006 analysis of business in the information age. Anderson describes a globalised world where large numbers of different products can be sold from different sources but in less quantity. The future holds not just multiple victimisations from one scam, but multiple victimisations from multiple scams circulating at the same time. One criminal can now carry out many different automated crimes at the same time (Wall 2007, 39). That is what is different about scareware.

Recent Example of New Crimes in the Machine—Social Networking Media (Trolling), Whistleblowing and Hacktivists

The recent example of Wikileaks (which itself is not a criminal organization, though it is treated as such in some of the security debates and discussions) nevertheless illustrates the potential for the malicious distribution of data. Wikileaks is primarily an organization dedicated to the leaking of information and whistleblowing. In many ways it maintains the old hacker ethic of freeing information to expose the truth. For the purpose of this discussion, it also autonomously exploits the crowd-sourcing potential of the internet in order to garner information and also disseminate it. Wikileaks is made all the more powerful by social networking media, especially Facebook and Twitter. Whilst Wikileaks, Facebook and Twitter are not criminal organizations and indeed bring great benefits to modern society they do provide new opportunities for criminal activity.

In support of the Wikileaks cause has emerged powerful hacker groups such as Anonymous and to a lesser extent LulzSec who seek to disrupt the activities of the detractors of Wikileaks in order to punish them and also highlight the political issues exposed by Wikileaks. Technically, these hacking offences fall under the crimes against the machine category listed earlier, however they are discussed here as crimes in the machine because of their informational link to Wikileaks. But they also illustrate the symbiotic relationship between different criminal missions and also the complexity of the organization of cybercrime. Prior to taking up the Wikileaks cause, Anonymous, a group encouraging civil disobedience of its members, had

launched attacks on Habbo Hotel, but became most well known for their attacks on the Church of Scientology. Their Project Chanology is an ongoing electronic protest against the Church of scientology (VFC 2009, 45).

Since taking up the Wikileaks cause in 2010, Anonymous have successfully attacked a number of different organizations who have tried to prevent Wikileaks from carrying out their mission. Firstly, they have hacked into and exposed the weaknesses of the organizations in order to humiliate them, such as taking client data though not using it. Secondly, they have prevented access by using DDOS Attacks (Distributed Denial of Service). Not only have these attacks achieved their goal of disrupting the target organizations, but they also seem to have caused some reputational damage in the process through the negative publicity attracted by the cases. LulzSec (derived from Laugh out loud) have either grown out of Anonymous or have taken up the Anonymous mission under a separate identity. LulzSec, apparently, has a fairly small core of about six members (Weisenthal 2011) supported by a group of about 56 others. This information was obtained in 2011 from other hacking groups who released personal information about LulzSec members on the internet. The internet relay chat (IRC) logs were leaked to *The Guardian,* but the membership was independently confirmed.

Whether Anonymous and LulzSec are true hacktivists or just rebels looking for a cause is unclear because of the varied and responsive nature of their activites, but what can be observed from their examples is that their organization, like that of the Stuxnet builders and Scareware peddlers is flat. In addition to being effective hackers/ hacktivists in terms of their ability to disrupt, both Anonymous and LulzSec are also experts in media manipulation to the point that a so-called leaked FBI report on the profiles of Anonymous may have be faked (Leyden 2011; Donoghue and Roberts 2011). Whilst this ability to manipulate its presence potentially obfuscates any full understanding of Anonymous or LulzSec, the arrest patterns that have emerged since investigations into their organization suggest a globally dispersed network (or assemblage) of disparate individuals and small groups who have little functional unity other than to follow the cause.

> Anonymous is not an organization ... [rather, it is] ... the first internet-based superconsciousness. Anonymous is a group, in the sense that a flock of birds is a group. How do you know *they're* a group? Because *they're* travelling in the same direction. At any given moment, more birds could join, leave, peel off in another direction entirely (Landers 2008).

Anonymous also seems to have coalesced a number of hacker groups to form a '"loose coalition of Internet denizens", Anonymous consists largely of users from multiple internet sites such as 4chan, 711chan, 420chan, Something Awful, Fark, Encyclopedia Dramatica, Slashdot, IRC channels, and YouTube. Other social networking sites are also utilized to mobilize physical protests. Anonymous has no leader and is reliant on the collective power of individuals acting in such a way that benefits the movement' (VFC 2009, 45). There is also some evidence to suggest that members of Anonymous have been mentored by older members of Chaos Computer Club. Drawing further upon information from the reports of the various arrests (See Wall forthcoming) reveals that Anonymous is a structure comprised of 'cells' of individuals

who could coordinate attacks by using downloaded software. There is no stated leader, but there does appear to be a leadership group which utilises chat rooms to organise the decision to make launch an attack.

Discussion and Conclusion

All three groups creating Stuxnet, Scareware and also Anonymous and LulzSec illustrate quite different motivations and, in the case of the Stuxnet creators, a high degree of professionalism, possibly with some state involvement. They also indications that a key driver of the groups is reputation as the participants show pride in their work and they also seek peer approval. At the core of the group dynamic is a reputational economy. Each crime type illustrates slightly different models of organization, but differences that are variations on a theme. With Stuxnet Malware (though a contested view), the offenders were small (possibly professional) group of about four or five who drew upon the services or help of others—and affiliates. Scareware was driven by the Kingpin with the idea and bankroll and who was introduced to an Affiliate via a Broker to gain access to victims online. The Kingpins then use online banking services themselves, or through a Money Mule, to transfer the stolen money to their own account (possibly via a Lynchpin who might launders it). The hacker groups are, disorganised in the traditional sense, but coalesced to formed an assemblage around a set of ideas/ ethics, to protect Wikileaks, who in this case is the affiliate.

These apparently different forms of organization probably have more similarities than discontinuities. They all comprise of individually very small (*de minimis*) crimes organised by a few individuals. They each seek the assistance of others, usually to solve a problem related to the criminal activity being designed, built or carried out. They also tend to involve the use of affiliates to access the relevant victim groups. They are networked crimes and very fluid. Sometimes individuals just fall out of the loop, so the structure is ephemeral. One thing that is certain is that it is flat and lacks a hierarchical command and control form. As stated earlier, 'assemblage' is a better description of the way that the various cells relate to each other. They all point, say, in one direction in terms of their intentions, but do not necessarily have any common functional unity. In the case of Anonymous, for example, each cell or grouping follows the idea. There are not necessarily any relationships or even communications between cells outside the nucleus, just an identification and affiliation with the idea.

The Scareware story and those of other true cybercrimes seem a million miles away from the vision of traditional organised crime invoked in Mario Puza's various Mafia novels. To understand the cyber-threat landscape it is important to acknowledge the different ways that cybercrimes are organised. The very nature of (true) cybercrimes being informational, global and networked (and increasingly automated) has encouraged different, flatter, forms of organization than the hierarchies of control found in more traditional forms of offending. The technologies allow far fewer people to control the whole criminal process; even fewer when the crime is automated

as with scareware, and networking process tends to undermine attempts to effect control (Wall 2007, 39). However, whilst scareware, phishing and other forms of cybercrime do not display the classic signs of organised crime, they do display distinctively different organizational traits, not least their ephemeral nature, their stealth and a marked similarity to an unethical e-commerce business model rather than the Mafia. What this tells us is that the organization of crime online follows a different logic to both organised crime and also the organization of crime offline. As stated earlier, it is by comparison to the paradigm, a dis-organised model. This is an observation that has implications both for law enforcement as well as prevention, because it is a logic that lends itself to a relativist rather than absolutist conceptualisation of cybercrime that is so often encountered. In other words, cybercrime by its very nature cannot be eradicated, it can only regulated and managed to minimise its impacts, this means that counter-cybercrime strategies, including prevention, therefore need to focus upon much more upon the regulation and management of cybercrime, including, but not exclusively, using disruptive technologies, in order to minimise its impact. What this analysis also practically suggests is that it is dangerous to put convicted cybercriminals in general prisons for it is there where more traditional organised crime may get their hooks into them and turn them to their own purposes.

This chapter is based upon a paper presented to the *Third Annual Illicit Network Workshop, University of Montreal*, Montreal, 3–4 October 2011. A more full and developed version can be found in the middle chapters of Wall (forthcoming).

References

Adamoli, S., Di Nicola, A., Savona, E., & Zoffi, P. (1998). european institute for crime prevention and control, HEUNI, Retrieved from http://www.heuni.fi/uploads/mmadzpnix.pdf. Accessed 13 Mar 2013.

Anderson, C. (2006). *The Long Tail: Why the Future of Business is Selling Less of Mor*e. New York: Hyperion.

BBC. (2007). 'Arrests made in botnet crackdown', BBC news online, 30 November, [Online]. http://news.bbc.co.uk/1/hi/technology/7120251.stm. Accessed 13 Mar 2013.

Brenner, S. (2002). 'Organized cybercrime? How cyberspace may affect the structure of criminal relationships'. *North Carolina Journal of Law & Technology*, *4*(1), 1–41.

C'T. (2004). 'Uncovered: trojans as spam robots', *C'T Magazine*, 23 February. www.heise.de/english/newsticker/news/44879. Accessed 13 Mar 2013.

Donoghue, B., & Roberts, P. (2011). 'FBI: Psychological profile of anonymous leadership is a fake', Threat post, 15 September. http://threatpost.com/en_us/blogs/fbi-psychological-profile-anonymous-leadership-fake-091511. Accessed 13 Mar 2013

Duffy, D. (2005). 'Affiliate marketing and its impact on e-commerce'. *Journal of Consumer Marketing*, *22*(3), 161–163.

Falliere, N., Murchu, L., & Chien, E. (2010). W32.stuxnet dossier: September 2010, version 1.0, Symantec White Paper. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf. Accessed 13 Mar 2013.

Goodin, D. (2007a). 'Botmaster owns up to 250,000 zombie PCs: He's a security consultant. Jail beckons'. The Register, 9 November. http://www.theregister.co.uk/2007/11/09/botmaster_to_plea_guilty/. Accessed 13 Mar 2013.

Goodin, D. (2007b). 'FBI crackdown on botnets gets results, but damage continues: 2 million zombies and counting'. The Register, 29 November. http://www.theregister.co.uk/2007/11/29/fbi_botnet_progress_report/. Accessed 13 Mar 2013.

Halliday, J (2010). 'Stuxnet worm is the 'work of a national government agency'. The Guardian. 24 September. http://www.guardian.co.uk/technology/2010/sep/24/stuxnet-worm-national-agency. Accessed 13 Mar 2013.

Landers, C. (2008). 'Serious business: anonymous takes on scientology (and doesn't afraid of anything)'. Baltimore city paper, 2 April. http://www2.citypaper.com/columns/story.asp?id = 15543. Accessed 13 Mar 2013.

Leyden, J. (2010). 'Bank insiders charged in ZeuS cybercrime smackdown'. The Register, 8 November. http://www.theregister.co.uk/2010/11/08/zeus_moldova_bank_worker_arrests/. Accessed 13 Mar 2013.

Leyden, J. (2011). 'Leaked' FBI Anonymous/LulzSec psych profile is bogus: Feds say Anons wrote it: 'narcissism' comment may be true'. The Register, 16 September. http://www.theregister.co.uk/2011/09/16/anon_fbi_profile_fakery/. Accessed 13 Mar 2013.

NISCC. (2005). 'Targeted trojan email attacks'. NISCC Briefing 08/2005, 16 June. http://www.cpni.gov.uk/Docs/ttea.pdf. Accessed 30 Jan 2008.

Rodgers, L. (2007). 'Smashing the criminals' e-bazaar'. BBC News Online, 20 December. http://news.bbc.co.uk/1/hi/uk/7084592.stm. Accessed 13 Mar 2013.

Savona, E. (2012). Organized crime enablers, global agenda council on organized crime, world economic forum. http://www3.weforum.org/docs/WEF_GAC_OrganizedCrimeEnablers_Report_2012.pdf.

Symantec. (2010). Symantec global internet security threat report trends for 2009, Volume XV, April. http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf. Accessed 13 Mar 2013.

Tapscott, D., & Williams, A. (2007). *Wikinomics: How mass collaboration changes everything*. London: Atlantic Books.

VFC. (2009). 2009 Virginia Terrorism Threat Assessment, Commonwealth of Virginia, Department of State Police, Virginia Fusion Center. March, http://www.infowars.com/media/vafusioncenterterrorassessment.pdf. Accessed 13 Mar 2013.

Wall, D. S. (2005/10). 'The internet as a conduit for criminal activity'. In A. Pattavina (Ed.), *Information Technology and the Criminal Justice System* (pp. 77–98). Thousand Oaks: Sage (Revised March 2010). http://ssrn.com/abstract=740626.

Wall, D. S. (2007a). *Cybercrime: The transformation of crime in the information age*. Cambridge: Polity.

Wall, D. (2007b). 'Policing Cybercrime: Situating the public police in networks of security in cyberspace'. *Police Practice and Research: An International Journal*, *8*(2), 183–205.

Wall, D. (2010c). The organization of cybercrime and organized cybercrime. In M. Bellini, P. Brunst, & J. Jaenke (Eds.), *Current issues in IT security* (pp. 53–68). Freiburg: Max-Planck-Instituts für ausländisches und internationales Strafrecht.

Wall, D. (2013). Enemies within: Redefining the insider threat in organizational security policy. *Security Journal*, *26*(2), 107–124.

Wall, D. (forthcoming). *Cybercrime and the Culture of Fear: Policing the Reassurance Gap in Cybersecurity*. New York: Springer.

Warren, P. (2005). 'UK trojan siege has been running over a year', The Register, 17 June. http://www.theregister.co.uk/2005/06/17/niscc_warning/. Accessed 13 Mar 2013.

Weisenthal, J. (2011). 'Notorious hacker group LulzSec just announced that it's finished'. business insider. Silicon Alley Insider, 25 June, http://www.businessinsider.com/lulzsec-finished-2011-6. Accessed 13 Mar 2013.

Yip, M., Webber, C., & Shadbolt, N. (2013).Trust among cybercriminals? Carding forums, uncertainty and implications for policing. *Policing and Society*. (issue and page nos. as yet unknown).

Zetter, K. (2011). 'DHS fears a modified stuxnet could attack U.S. Infrastructure', WIRED, 26 July. http://www.wired.com/threatlevel/2011/07/dhs-fears-stuxnet-attacks/. Accessed 13 Mar 2013.