

DRAFT - The Organization of Cybercrime in an ever-changing Cyberthreat Landscape

Draft paper for the Criminal Networks Conference, University of Montreal in October 3rd and 4th 2011

David S. Wall, Criminology, SASS, Durham University, 32 Old Elvet, Durham, UK. DH1 3HN.
<d.s.wall@durham.ac.uk>

Abstract

Since 2009 we have witnessed a step-change in the level of danger posed by cybercrimes to individuals, organizations and national security. The analysis of the construction and delivery of these cybercrimes also provides an important insight into their organization. Malware such as Zeus, SpyEye, Stuxnet, and scareware (fake AV), alongside modern hacker groups each display new levels of threat as well as advanced sophistication and organization in terms of their design, construction and delivery. In the case of Scareware, for example, the software not only deceives the victim through social engineering but for the first time it also sends the victim's money directly to the perpetrator. Scareware differs from Phishing which uses technology to steal information, but still requires a human money mule to extract a victim's money from their bank in real time. On the topic of social engineering, we have also witnessed the 'power of the crowd' with regard to protest and whistle-blowing. It is a 'power' that is potentially open to criminal exploitation. Although the details of each form of offending can differ, a common trait found with each is that their organization is both flat, networked and also very small as offenders utilize the same networked technologies to organize cybercrime as they do to commit it.

In order to understand the above changes to the cyber-threat landscape we have to also understand the organization of the threats and this is the purpose of my talk. Today, I shall explore the organization of cybercrime, which I interpret as those criminal behaviours that have been transformed by networked technologies. 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. The third part will compare the organization of known cybercrime gangs with what is known about the way that the new threats are organised in order to draw out any similarities or differences. The fourth part looks at various new forms of cybercrime carried out by some of the gangs discussed in the previous section. The fifth and final part will explore new enterprise and network 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.

Key words – Organized Crime, cybercrime, Organized cybercrime, malware, network crime,

Introduction

Networked technologies have transformed the way that crime is organised on the internet (cybercrime), yet the (personal, corporate, national) information security debates over the organization of cybercrime tend to be dominated by two paradigms of traditional criminological thinking; the construction of the cybercriminal as a 'dangerous other' and the tendency to approach the organization of cybercrime and cybercriminals in terms of the hierarchical traditional (Mafia) model of organised crime. The application of both models to crimes of the internet is problematic because not only do they inaccurately reflect the organization of cybercrime, but they also shape cybercrime policy, especially the discussion over who is ultimately responsible for policing cybercrime. They are flawed because the internet has transformed the organization of crime in substantially different ways to the organization of more traditional crimes.

In a nutshell, there is no need to commit one large crime today on the internet when one person can commit many small crimes, typically in one or more of the three generic cybercrime groups found on the internet: Crimes against the machine (hacking etc.), Crimes using the machine (frauds etc.) and Crimes in the machine (pornography, hate speech, but also social networking offences). In each of these crime groups there is clearly a serious threat posed by outsiders the criminal others or 'bad guys', whether they be

hackers, fraudsters or other malicious outsiders such as paedophiles or hate-mongers. But, the limitations of the current thinking about the organization of cybercrimes in the prevailing threat model overlooks, for example, the insider threat. When it does consider it, the focus is upon the malicious insider who seeks to profit from their access privileges or to seek revenge from the organization. The well meaning insider is, for example, most overlooked in the prevailing threat model which underpins security debates. They are typically the compliant victim who is socially engineered (read conned) into divulging their personal information, their organizational access codes or simply falls for one of the many internet scams circulating at any one time. Insiders are an increasingly important part of the organization of cybercrime (Wall, 2011). The cybersecurity threat landscape has changed in recent years and we need to know more about how it has changes and what its implications are.

The first part of this paper 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. The third part will compare the organization of known cybercrime gangs with what is known about the way that the new threats are organised in order to draw out any similarities or differences. The final part will explore new enterprise and network 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.

The transformative impacts of networked technologies upon criminal activity

The internet and its networking technologies have had the following six major impacts. Firstly, they not only *globalise* the communication of information, ideas and desires but they also impact locally creating a *glocalising* effect. Secondly, they create the potential for *asymmetric* as well as *symmetric relationships*, one person can address many others at the same time. The technologies also allow for the many to also talk to the few. Thirdly, the surveillant aspects of the technology not only allow *synopticism* where the many do not know when the few are watching them and which can mediate their behaviour, but they also allow for *panopticism* where the many can watch the few with a simultaneous mediation of behaviour. Fourthly, 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 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 opportunities for criminals.

Crime can now be global, asymmetric, synoptic and panoptic, data trails can be captured to entrap victims, and this leads us to the sixth impact. Sixthly, and lastly, networked technologies and new social media and the five impacts described above also providing new forms of criminal opportunity and they are *changing the way that crime is taking place*. Indeed criminal labour itself is becoming deskilled and reskilled. The level entry skills have dropped as the technological developments of network technology (malware and delivery mechanisms) that help criminals has been automated to the point that it can now be rented or bought off the self. Another significant development is that the cost of technologies is relatively low.

The outcome of these transformations is that offenders can now commit crimes that were previously beyond their financial and organizational means on a global scale. Significantly, one person can now control a whole criminal process or part thereof and this 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 it is such a highly emotive and newsworthy, especially as commentators continue to resort to 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 has a powerful cultural logic, especially as the fraud statistics clearly show that the internet is increasingly being used by fraudsters to steal large amounts of money from innocent victims. The main challenge, however, for policy makers and practitioners is to identify exactly who the fraudsters 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.

This paper will argue that the debate over organised crime online can only be advanced by looking at the ways that crime is organised online. The paper will therefore begin by briefly outlining 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 wholly mediated by the internet - are being organised, a detailed analysis of scareware, a relatively new form of malicious software, will follow. The paper will show that the organization of crime online, when it involves 'true' cybercrimes (Wall, 2007: 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 actually 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 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 early 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' 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 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, 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 listed in Table 1, 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 very like small cottage-industries in structure. They can be driven by an individual or by a very small group, but not always, because the organising principle can simply be a common idea. 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.

Table 1: Some of the cybercrime gangs known to have operated between 2000 and 2010

a) Carding and ID theft Operations

- **Shadowcrew** - Operation Firewall 2004/5 - the ShadowCrew were a gang dedicated to identity theft, bank account pillage, and the fencing stolen goods on the WWW. They did not meet. Part of the ICA.
- **The Rock Phish gang** – 2006-2008 - were a notorious phishing gang that reinvented itself as Avalanche.
- **Avalanche** – 2009+ thought to be a successor of the Rock Phish gang (Zeus - 60% of Phishing attacks in 2009)

- **Carder Planet and Darkprofits** – provided a www facility for selling credit card details – allegedly part the ICA
- **International Carder's Alliance (ICA)** who use known Web sites and IRC (Internet Relay Chat) channels to coordinate their online attacksⁱ.
- **Mazafaka** – 2005 - Ivan Maksakov was a 21-year-old Russian mechanical engineering student - One man gang? Part of the ICA – Cards & ID theft -
- **IAACA** (the International Association for the Advancement of Criminal Activity) affiliated to ICA – cards and ID theft
- **TJ Maxx Gang** – Albert Gonzales and Co - hacking of more than 90 million credit and debit card numbers

b) Botnet operations

- **Rustock**,
- **Warezovⁱⁱ (Storm Botnet)** - (2006-2008) created by W32/Waresov worm, is a mass-mailing worm that sends code file via e-mail attachments to addresses found on infected computers. Became inactive in 2007, bu reemerged in 2008.
- **Blackcarder**,
- **Storm Worm Gang**,
- **Celebrity Spam Gang** – each group controls botnets
- **Koobfaceⁱⁱⁱ** - spreads via social networking sites (mostly Facebook) by social engineering victims to click on fraudulent web sites to give information or accept infected downloads. Koobface is a botnet for hire.
- **Asprox^{iv}** – botnet used mainly for phishing scams. Discovered active server pages on poorly configured web sites and embedded malicious iframes and external javascript references.
- **Mariposa** - the Mariposa Botnet (Mariposa is a multi-faceted piece of malware, neither trojan, worm or virus). Has many forms and created the Koobface botnet. 13 M compromised computers, including many on fortune 1000 list. The Mariposa command-and-control structure was infiltrated by the Mariposa Working Group to observe the communication channels used by the suspected botmasters. The channels send information from compromised computers to the offenders - similar to those used by the Zeus, Conficker and Koobface botnets or as shown recently in the Google/Aurora operation. The Mariposa botnet spread extremely effectively via P2P networks, USB drives, and MSN links.^v
- **Zeus**
- **Conficker**
- **Waladec**

c) Cybercrime Hubs

- **Tartu, Estonia^{vi} – Cybercrime server – 2005-2008** – cybercrime business hosting Rogue DNS servers, Intranet of Cybercrime, Network of Sock4 Proxies, Replacing Ads, Hijacking queries, Fake Antivirus software

d) Spammer Operations

- **Superzonda** – spammers based in South America who specialize in creating and disseminating spam.

e) Malware Specialists

- **The Hangup Team** – were a gang of Russians who develop malware for sale to hackers. They have links with the spamming industry which uses their botnets as spamming platforms.
- **The Russian Business Network** – are responsible for drive-by downloads - alleged links to the Russian government (Allegedly moved to China and Taiwan) (“MPack (packer kit) and its IcePack add-on are being offered, as well as iframe exploits.”)
- **Drink or Die** – a group that distributed Warez (pirated software). They claimed to be non profit, but were highly organized and security-conscious. They cracked the security in new software and then released it.

f) Auction fraud

- **Romainan eBay Cybercrime Gangs**^{viii} - 2010 3 unconnected ebay gangs in Romainia.

g) Hactivist

- **Anonymous** - – (see later)
- **LulzSec** – (see later)

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 to hand 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). In many ways cybercrimes, by their very informational, networked and global nature, go against the very grain of the traditional model of organised crime. Indeed, the following detailed examples of Stuxnet (a crime against the machine), scareware fraud (a crime using the machine), and Whistleblowing (crimes in the machine) and their organization, upon which the remainder of this paper is based, shows 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 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 a core group of four or five people, with a broader group from whom 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).

Stuxnet represents a 'paradigm shift' (ENISA, 2010a) in malware threats and is distinct from other malicious worms because: a) its primary method of entry into operating systems is, amongst other potential entry means, through USB sticks b) like other worms it establishes a rootkit as well as a backdoor connections which allows external control c) unlike other worms, it aggressively attacks specific types of SCADA^{ix} systems produced by particular manufacturers d) the July 2010 Stuxnet worm had a kill date and limited scope and sought particular system configurations – indicating that it was intended to hit specific targets, but did not find its target this time. In the absence of further information conspiracy theories quickly evolved which mapped the Stuxnet threat onto contemporary political divisions. A particular concern was that the 2010 attack was specifically targeted at Iranian (nuclear) processes.

Analysis of Stuxnet's structure and its pathways through computer systems shows that organizational insiders are likely to have provided information crucial to its creation, installation and propagation through various systems. A more detailed analysis of Stuxnet can be found in the research by Falliere et al. (2010), but in short, it is a form of malicious software that can be used to sabotage SCADA (Supervisory Control And Data Acquisition) based industrial control systems ranging from water utilities to gas pipelines to power stations, including some nuclear power plants. Stuxnet represents a 'paradigm shift' in malware threats because of the way that it enters sometimes closed operating systems via insiders through infected USB sticks; it propagates itself by establishing a rootkit as well as backdoor connections that can allow external control; and also attacks only specific types of SCADA systems produced by specific manufacturers. Although a range of antecedents exist, the most recent iteration of Stuxnet, discovered in mid-2010, was found to have infected approximately 100,000 systems worldwide, although the evidence is mixed as to whether or not it has found its specific target and as to what impact it had (BBC, 2011).

Where Stuxnet contrasts with the design and function of preceding threats is that it is a 'large, complex piece of malware with many different components and functionalities' and constitutes a particularly complex threat (Falliere et al., 2010). Falliere et al. (2010) estimate that Stuxnet took many months to create and was the work of a fairly large and highly skilled team. Important is the fact that the malware needed to be directly introduced into the target environment by an insider because the most sensitive SCADA systems are usually kept unconnected to the internet. Falliere et al. (2010) argue that removable drives, typically USB sticks were the most likely means by which the malware was introduced into the system: it '... may have occurred by infecting a willing or unknowing third party, such as a contractor who perhaps had access to the facility, or an insider' (2010). More significant is the observation that the designers of Stuxnet will have needed to possess very detailed knowledge about the design of the SCADA particular systems to be attacked. This information could only be obtained with the assistance of an insider, very likely the result of careless practice by a well-meaning insider which led to a data spill that was capitalized by a hacker.

Although Stuxnet is not unique in requiring insider complicity, see, for example, the Hydraq Trojan (Symantec, 2010). 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, 2010). The example suggests a

small organizational group that draws in assistance and information from outsiders. What is not known is whether the assistance was obtained complicitly or illegally.

Recent example of 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, scareware signifies an important trend in the evolution of cybercrime. Not only is it a good example of a 'true' cybercrime spawned purely by the internet (see further Wall, 2007, 2008), but possibly for the first time, it provides evidence of a complete crime being committed entirely by malicious software in large numbers. Software 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. 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.^x

How does scareware work?

Scareware is an aggressive fraud technique that uses routines set in malicious software (malware) to shock victims into paying for software that they do not need and which, in some cases, may actually cause further damage to their computers. User's computers are typically infected by emails that socially engineer them into opening infected attachments by clicking onto www sites, or by infecting frequently accessed and trusted www sites. The 'FakeAV153' Trojan, for example, found by Symantec to be the second most downloaded malware in 2009, displays false antivirus alerts and lowers security settings on compromised computers (Symantec, 2010). Once installed, the scareware remains dormant for a period of time so that the attack cannot be directly linked to the point of infection. The standard attack typically occurs when users will unexpectedly become inundated with messages that tell them their computer has been infected and that they have to immediately download, and pay for, software that will solve and prevent the problem, else (it is claimed) their system will be damaged permanently or even destroyed.

Scareware evolution

In its earliest forms, scareware savagely distressed its victims into complying. Typically the user's screen would freeze, as was the case with mid-2000s derivations of 'Nightmare' - the first scareware programme from 1991 (*India Times*, 2007). A skull would suddenly appear and emit a loud mocking shriek, alternatively the screen would appear to fragment and fall in pieces to the bottom of the monitor – and then the skull might appear. The action and message would panic victims into buying the software, but it would also leave them feeling cheated and humiliated. Scareware has subsequently evolved and more recent incarnations are becoming more professional in appearance. The most prevalent forms of scareware currently circulating, Antivirus 2009 and Antivirus XP, for example, have the general 'look and feel' of a major software brand, so much so that users find it hard to distinguish the scam 'pop up notices' from messages from their own operating system. See Table 1. Some versions of scareware even maliciously suggest that it is being endorsed by the manufacturers (Leyden, 2009b).

More recent iterations of scareware in late 2009 and early 2010 scare victims into paying for a remedy, but by increasing victims' anxiety levels rather than by distressing them through shock. Some examples warn users that images of child pornography are located on their computer and state that they can only be removed with specialist removal software which has to be downloaded and paid for (Leyden, 2009a). Other (clever) adaptations are known to audaciously threaten to sue down-loaders who specifically use BitTorrent software to pirate music, video or software. In the scareware tradition (as it has now become), such infected computers will suddenly display a note from a company allegedly representing the various industries stating that pirated content has been detected on the user's computer and request a payment in compensation. Where this version of scareware varies from its predecessors is that a second pop-up notice subsequently presents the user with a convincing online invoice for a licence for the music, video or software they have downloaded - presumably based upon the actual downloads the user made when using BitTorrent. Users are also presented with a facility to pay their payment by credit card. Although very professional in appearance, the weak point of this particular scareware is that the payments being requested are considerably higher (in the region of \$400) than the \$30 or being requested by the more conventional scareware and so jeopardise the scam by inciting victims to question or resist making the payment.

With most of the more recent examples of scareware, not only do the pop-notices convince victims that they have a genuine problem, but post-payment notices from the downloaded software indicate the removal of the malware and give the appearance of it actually having performed a therapeutic function. This helps reassure victims and leaves them feeling that they have been provided with the service that they paid for, not realising that they have been defrauded. In some cases, the scareware has been known to actually perform a basic and genuine function, such as clearing out unwanted or discarded files, which can frustrate attempts at a criminal prosecution.

Alternatively, a recent strain of scareware (e.g. AnVi Antivirus) socially engineers users into uninstalling their existing security packages by using 'pop up' messages which claim that their legitimate security software is 'uncertified' and should therefore be removed, else their computer's performance will decrease. This technique contrasts with rogue software such as the Conficker worm which stealthily disables security software and/or its ability to acquire updates (Leyden, 2010). From the offender's perspective, the advantage of social engineering rather than technical approaches is that they are less likely to be picked up by security software in the first place and that they deceive the user into being complicit, which makes the case for the prosecution harder to prove.

How prevalent is the scareware threat?

The various annual threat reports from the cyber-security industry indicate a year-on-year increase in online threats. Symantec's computer security threat report for 2009, for example, shows that 1,656,277 cyber-threats were detected in 2008, which represented a 2.65 fold (1 million) increase when compared with 2007. In turn, the figures for 2007 represented a 4.4 fold increase on those for 2006 (Symantec, 2009a). Much of this increase can be explained by the rising threat of scareware which continued throughout 2009. In their October 2009 report on Rogueware, Symantec observed a dramatic increase in scareware threats during the first six months of the year in comparison to the last six months of 2008 and they identified 250 variants of scareware in circulation (Symantec, 2009b). The Anti-Phishing Working Group (APWG) similarly found that

scareware threats had increased seven fold during the first half of 2009 from 22,218 in January to 152,197 in June (APWG, 2009: 1).

The substantial increase in scareware threats was probably due to the increased use of search engine optimization (SEO) techniques (see glossary) used by Affiliates or Brokers to assist them to distribute the scareware. In their scareware study, online security provider Finjan found that 1.8m unique users were redirected to rogue anti-virus site over a period of 16 consecutive days and that SEO techniques radically escalated the hit rate to between 7 and 12 per cent (Finjan, 2009: 4). Perhaps the most worrying findings are those from researchers from Google who, in analysing 13 months of reprocessed data from Google's malware detection infrastructure, found that fake anti-virus software (as it is also referred to) accounted for 15 percent of all types of malware identified by their search (Rajab et al., 2010; BBC, 2010). It is important to note here that not all of scareware threats will result in victimisation; however the indications are that many are doing so as the malware becomes more sophisticated.

How does scareware impact upon its victims?

When victimisation occurs, the average individual loss per victim to scareware is estimated to vary between US \$10 and US \$50 (Symantec, 2009b; Finjan, 2009); which is about the cost of a domestic security software package. Although these losses breach the fraud laws of most jurisdictions (e.g. s.7(1) UK Fraud Act 2006) they are a category of fraud that is becoming known as micro-frauds (Wall, 2010) and characterised by being individually small in impact, but significant only in their global aggregate. Importantly, they are deemed to be individually too small to be acted upon, often being written off by victims (both individual and corporate) or deemed not significant enough to devote policing resources to in the public interest (Wall, 2010). This characteristic causes particular reporting problems on the occasions when victims do feel victimised because not only may they be deterred from reporting them because of the complexities of the reporting process, but even if victims do report the fraud to police, then they are likely to feel dissatisfied. This is because police very often request that victims report their loss to the banks first since it is they who are regarded as the victims when losses involve credit cards. Frustratingly, when they do so the banks often refuse any liability arguing that the victim consented to the payment. Whilst there is some truth in the bank's assertion that victims are (unintentionally) complicit and willing, offenders are getting away with fraud and making money out of it (see later). Furthermore, the fact that this fraud is wholly automated means that the fraud is asymmetric and one fraudster can scam many people at any one time across jurisdictions, so the potential aggregate losses could be huge. Together, these factors combine to obscure the true financial impact of scareware, whilst also increasing the cash yield, speeding up the scam process and reducing the risk to the offender.

How are scareware scams organised?

The organization of a typical scareware operation is effectively a 'criminal' reflection of the structure of 'Affiliate Marketing'; 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 scareware to be used, an 'Affiliate' whose role it is to introduce the Merchant to the Consumer (e.g., by infecting victims' computers), and the Consumers ('victims') who are encouraged to part with their money. The Affiliates are 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 scareware. As found with 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.

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 highly likely that they never meet, so their relationships tend to be ephemeral and project based. Today, Kingpins seek to conduct their business as quietly as possible with a veneer of professionalism 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 relationship between the Kingpin and Affiliate is sometimes frustrated because the latter work to different criminal agenda and may not share the Kingpin's desire for stealth. This is because it is in the Affiliate's interest to maximise their own criminal opportunities by installing additional software, for example, malware linking them to botnets (robot networks of remotely administered computers) that will enable the Affiliates to independently access the victim's computer at a later date for their own criminal purposes. To protect themselves, Kingpins will not only pay affiliates a fee for the installation of the software on individual computers, usually in the region of \$0.15 to \$0.55 cents, sometimes more, but they may also compensate them for not injecting additional software into victim's computers that could unmask the scam. This compensation may be either a set fee or a proportion of the take from successful scams. Estimations of the sums of money yielded from scareware operations vary from report to report, but they are all large. Symantec have estimated that a full scareware operation can yield upwards of \$850,000 (Symantec, 2009b) which represents approximately 30,000 scams of just under \$30 each (my calculation). Such sums are entirely feasible since these scams take place on a global scale and that the scareware has the ability to route the profit straight into the offender's bank account. The actual recoverable gains do appear to be somewhat lower than the estimate, however, as is also found with recoveries from Phishing prosecutions, the recovered assets are still comparatively large. In June 2009, for example, two of a number of US defendants prosecuted by the Federal Trade Commission for a 'scareware' scam settled a \$1.9m judgement against them for \$116,697 worth of assets on the basis that they were unable to pay the full amount (FTC, 2009).

The implications of the scareware scam, its feasibility, its relative technical simplicity and the potential size of the yield are three fold. 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 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 (see glossary) 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 them falling for the scam. Thirdly, since there is now so much to gain financially, then the 'scareware-monger'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 with some of the more scurrilous scareware has been to encourage victims to buy the scareware solution bundled with branded proprietary security software 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 and the purchaser then realises they have become a victim. Such activity threatens 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, but they will have successors. The advent of this type of wholly automated crime means that are entering the era of "the long tail" of crime (mimicking Chris Anderson's 2006 analysis of business in the information age). 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.

What can we do about scareware?

As suggested earlier, the solution to scareware does not lie in creating new law because fraud and computer misuse are already illegal in most countries. Even the less invasive or detectable forms of scareware that do not breach criminal law are certainly covered by other law, and cases that emulate the look and feel of proprietary software can also breach intellectual property laws. Of all bodies of law, the strength of US law is probably the most important here since the majority of the scareware (53%) threats were found to come from computers based in the USA. The remainder were found in EU countries (20% +), with surprisingly small percentages in China (3%) or Russia (1%) (Symantec, 2009b) given the current media hype about computer misuse in those countries.

The main challenge to regulating scareware is that the offences arising from it are too small to act upon in the public interest and fall foul of the *de minimis* rule (Wall, 2007: 161). When combined with low levels of reporting by Individual victims, this characteristic limits potential criminal justice responses. Some law suits have been brought against Scareware operatives, such as the FTC case mentioned earlier, however, the case was settled prior to prosecution without any admission of guilt on the part of the defendants. Having said this, further legal action remains against others involved in the case and the defendants who settled were also prohibited by order from installing malicious programs on consumers' computers and employing 'scareware' tactics (FTC, 2009).

The most effective and quickest response to scareware (because the legal process can also be slow) is a combination of technological and educational solutions that narrow the criminal window of opportunity. Scareware can be quickly picked up by security software, and as with Phishing malware, computer users also quickly become aware of the potential risk it poses and cease to fall victim which makes them wary. Yet, scammers are becoming more adept at putting new spins on their trickery to undermine these counter-measures. They are quickly 're-skinning' their packages to give them a new look and feel and to make them much slicker (and as indicated earlier, more legitimate in terms of their claims) - which not only confuses users, but can also confuse the security technologies that use the checksum technique (see Glossary) by changing the signature of the software's. But, since most victims of scareware tend to be those who possess insecure computers - which is how the malicious software usually gets through the firewall into the machine - then the best form of defence is to encourage users to keep their operating systems updated and also to install security software.

A major problem experienced to-date in policing the micro-frauds that result from the likes of scareware has been the lack of an effective, consistent and easy reporting system. This has long meant that crucial strategic intelligence which identifies 'the bigger picture' of impact at a nation level has been lost, as has the important tactical criminal intelligence relating to the offenders, which hampers the police ability to investigate. Hopefully, new arrangements under the UK's *Cyber Security Policy* (Cabinet Office, 2009), complemented by the new *UK Cyber Crime Strategy* (Home Office, 2010) will combine with the *National Fraud Strategy* (NFA, 2009) and *E-crime Policing Strategy* (ACPO, 2009) to help to address the problem of scareware (NFA, 2009). As part of that policy, the Action Fraud reporting centre (referred to in earlier documentation as the National Fraud Reporting Centre and now supported by the National Fraud Authority), has from late 2009 received reports of fraud, including scareware related fraud. These and reports of other types of fraud and related cybercrime are then passed on to the National Fraud Information Bureau (NFIB) which analyses and builds up a national picture of online fraud. Located within the City of London Police, the NFIB also decides how the reported frauds are to be acted upon through its national tasking system (Cabinet Office, 2009). The NFIB works alongside the National Police Central e-Crime Unit (PCeU) which is based in the Metropolitan Police and set up as part of the ACPO National e-Crime Strategy (ACPO, 2009). The PCeU also operates in close collaboration with the Metropolitan Police's own Dedicated Cheque and Plastic Card Unit (DCPCU) which focuses upon the physical corruption of technological devices used in the banking system.

When frauds are found to have caused significant losses, or are clearly the product of organised crime, then the Serious Fraud Office or the e-crime unit of the Serious Organised Crime Agency (SOCA) may become involved. Whilst the many different types of policing organizations working in the field create an adverse potential for 'turf wars', they and their 'nested' parent strategies nevertheless represent a positive step towards providing a system of combating cybercrime related fraud at a national level - only time will tell whether or not these arrangements will be effective.

Recent example of crimes in the machine – social networking media, *whistleblowing and hacktivists*

The recent example of Wikileaks (which is not a criminal organization, though it is treated as such in some of the security debates and discussions) nevertheless illustrates the potential for malicious use of the internet.

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. 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 have emerged two powerful hacker groups such as Anonymous and LulzSec who seek to disrupt the activities of the detractors of Wikileaks in order to punish them and also highlight the political issues Wikileaks has exposed. Technically, these offences fall under the crimes against the machine category listed earlier, however they are discussed here because of their link to Wikileaks. But they also illustrate the symbiotic relationship between different 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, 2005: 45). Table 2 illustrates the various operations carried out by Anonymous.

Table 2. Anonymous Activities

2006-07

- Habbo Hotel raids
- Hal Turner raid
- Chris Forcand arrest

2008

- Project Chanology
- Epilepsy Foundation forum invasion
- Defacement of SOHH and AllHipHop websites

2009

- No Cussing Club
- Iranian election protests
- Operation Didgeridie

2010

- Operation Titstorm
- Oregon Tea Party raid
- Operations Payback, Avenge Assange, and Bradical
- Operation Leakspin
- Zimbabwe

2011

- Attack on Fine Gael website
- Arab Spring Activities
- Attack on HBGary Federal
- Purported threat against the Westboro Baptist Church
- Wisconsin protests
- Bank of America document release
- Operation Sony
- Spanish Police
- Supporting 2011 Indian Anti-corruption movement in cyber space

Operation Malaysia
Operation Orlando
Operation Intifada
Operation Anti-Security
Operation Facebook
Operation BART

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. Not only have these attacks achieved their goal of disrupting the target organizations they also seem to have effected some reputational damage in the process through the negative publicity attracted by their weaknesses. LulzSec (derived from Laugh out loud) have either grown out of Anonymous or have taken up the Anonymous mission under a separate identity.

LulzSec has a fairly small core of about six members^{xi} supported by a group of about 5-6 others. This information was obtained in 2011 from other hacking groups who released personal information LulzSec members on the internet. The internet relay chat (IRC) logs were leaked to *The Guardian*, but the membership 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 activities, 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 been faked (Leyden, 2011; Cryptome, 2011). Whilst this ability potentially obfuscates any understanding of Anonymous or LulzSec, the arrest patterns that have emerged since investigations into their organization. It suggests 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 ... [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'.^{xii}

Table 3 Anonymous Arrests

December 2010 – 16 year old arrested for attacks against Visa, MasterCard and PayPal in conjunction with Anonymous' DDOS attacks against companies deemed to lack support for Wikileaks^{xiii}
January 2011 - United States search warrants^{xivxv} - In January 2011 – no arrests – mainly a statement
January 2011 - British arrests^{xvi} - five men between the ages of 15 and 26 with suspicion of participating in Anonymous DDOS attacks

March 2011 - Australian arrest^{xvii} - Matthew George - arrested for his participation in Anonymous DDOS activities. George participated in Anonymous IRC discussions – Participated in Operation Titstorm (protest responding to a plan by Australian Telecommunications Minister Stephen Conroy)

June 2011 - Spanish arrests^{xviii} - three alleged members of Anonymous arrested in Gijon, Barcelona and Valencia.

June 2011 - Turkey arrests^{xix} - 32 alleged members of Anonymous arrested for DDoS attacks on Turkish government Web sites. Arrested in a dozen Turkish cities.

July 19-12 - Arrests following Operation Avenge Assange^{xxxi} - Sixteen suspected members of "Anonymous" were arrested this morning in states across the country, from California to New York

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 are also mentored by older members of Chaos Computer Club.

Drawing upon information from the reports of the various arrests (Table 3) 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.

Conclusion: The organization of cybercrime

In summary, we at first sight some different models of organization with regard to each type of cybercrime. With Stuxnet Malware, the offenders were small group of about four or five who drew upon the services or help of others. Scareware was driven by the Kingpin with the idea and bankroll and who employed an Affiliate to Broker information about a victim, or the victims information, then a Money mule to get money out of the bank using cloned card or account details and then a Lynchpin who launders the stolen money. The hacker groups were, disorganised in the traditional sense, and formed an assemblage around a set of ideas, to protect Wikileaks. Yet, these apparently different forms of organization probably have more similarities than not. They are all very small and centred around an individual or few individuals. They also seek the assistance of others, usually to solve a problem related to the activity being designed, built or carried out. This is networked crime and is 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.

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, and indeed they are. At first sight many involved in law enforcement can be forgiven for either not seeing what the fuss is about, or simply seeing cybercrime as a technical problem. This is because their view of the world is largely based upon Peelian (after Robert Peel, the founder of modern policing) principles of policing in order to keep the dangerous classes off the streets, to maintain order and also enforce law. But, it is argued here that true

cybercrimes are of crucial significance because the malicious software's high level of automation, its ability to victimise asymmetrically and the capacity to manage fraudulently obtained gains represents a step change in online criminal practices. In this sense cybercrime has come of age and now poses a significant threat.

In understanding that threat 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. 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 needs 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.

NOTE: This project began during a fellowship kindly awarded by CEPS, the Australian Research Council's Centre for Excellence in Policing and Security at the ANU, Canberra and Griffith's University, Brisbane, Australia, it was subsequently developed through participation with the Cybercrime Research Group at the Max Planck Institute (Phillip Brunst, Marcello Bellini, Jocken Jaehnke and Jan Spoenle). I would like to thank both research groups. This paper includes research conducted with the involvement of Symantec on projects related to Scareware and also the Insider threat.

REFERENCES

- ACPO (2009) *ACPO e-Crime Strategy*, Association of Chief Police Officers,
<http://www.acpo.police.uk/asp/policies/data/Ecrime%20Strategy%20Website%20Version.pdf>
- Anderson, C. (2006) *The Long Tail: Why the Future of Business is Selling Less of More*, New York: Hyperion.
- APWG (2009) *Phishing Activity Trends Report, 1st Half 2009*, Anti-Phishing Working Group,
http://www.antiphishing.org/reports/apwg_report_h1_2009.pdf
- BBC (2007) 'Arrests made in botnet crackdown', *BBC News Online*, 30 November, [Online] Available at:
<http://news.bbc.co.uk/1/hi/technology/7120251.stm> (30 January 2008).
- BBC (2010) 'BBC Google warning on fake anti-virus software', *BBC News Online*, 28 April,
<http://news.bbc.co.uk/1/hi/technology/10088949.stm>
- Brenner, S. (2002) 'Organized cybercrime? How cyberspace may affect the structure of criminal relationships', *North Carolina Journal of Law & Technology*, vol. 4, no. 1, pp. 1–41.

- Cabinet Office (2009) *Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space*, <http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf>
- C'T (2004) 'Uncovered: trojans as spam robots', *C'T Magazine*, 23 February, [Online] Available at: www.heise.de/english/newsticker/news/44879 (30 January 2008).
- Cryptome (2011) 'FBI Psychological Profiles of Anonymous Leadership is a Joke', *Cryptome.org*, 5 September, <http://cryptome.org/0005/fbi-anon-psycho.pdf>
- Duffy, D. (2005) 'Affiliate marketing and its impact on e-commerce', *Journal of Consumer Marketing*, 22(3): 161 – 163.
- Falliere, N., Murchu, L. and 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 1 August 2011.
- Finjan (2009) 'Finjan Discovers a Network of 1.9 Million Malware-Infected Computers Controlled by Cybercriminals - Corporate and Government Computers Are Included', *Finjan Press Release*, 22 April, <http://www.finjan.com/Pressrelease.aspx?id=2238&PressLan=2139&lan=3>
- FTC (2009) 'FTC Settles with Two Defendants in Bogus Computer Scan Case', *Federal Trade Commission press release*, 25 June, <http://www.ftc.gov/opa/2009/06/winsoftware.shtm>
- Goodin, D. (2007a) 'Botmaster owns up to 250,000 zombie PCs: He's a security consultant. Jail beckons', *The Register*, 9 November, [Online] Available at: http://www.theregister.co.uk/2007/11/09/botmaster_to_plea_guilty/ (30 January 2008).
- Goodin, D. (2007b) 'FBI crackdown on botnets gets results, but damage continues: 2 million zombies and counting', *The Register*, 29 November, [Online] Available at: http://www.theregister.co.uk/2007/11/29/fbi_botnet_progress_report/ (30 January 2008).
- 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>
- Home Office (2010) *Cyber Crime Strategy*, Cm 7842, London: Office of Public Sector Information, March, <http://www.official-documents.gov.uk/document/cm78/7842/7842.pdf>
- India Times (2007) 'Scareware: Playing on your fears!', *India Times*, 21 February, <http://infotech.indiatimes.com/articleshow/1653102.cms>
- Kravets, D. (2010) 'Malware Threatens to Sue BitTorrent Downloaders', *Wired Threat Level blog*, 12 April, <http://www.wired.com/threatlevel/2010/04/ransomware/>
- Leyden, J. (2009a) 'Scareware tool dumps smut on Windows PCs: Rogue clean-up tool poses child abuse frame risk', *The Register*, 19 November, http://www.theregister.co.uk/2009/11/19/smut_scareware/
- Leyden, J. (2009b) 'Scareware slingers flaunt fake MS endorsement', *The Register*, 10 December, http://www.theregister.co.uk/2009/12/10/scareware_fake_ms_endorsement/
- Leyden, J. (2010) 'Scareware tries to trick marks into dropping defences', *The Register*, 20 August, http://www.theregister.co.uk/2010/08/20/social_engineering_scareware/
- 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/
- NFA (2009) *The National Fraud Strategy: A new approach to combating fraud*, National Fraud authority/ Attorney General's Office,

http://www.attorneygeneral.gov.uk/NewsCentre/News/Documents/NFSA_STRATEGY_AW_Web%5B1%5D.pdf

- NISCC (2005) 'Targeted trojan email attacks', *NISCC Briefing* 08/2005, 16 June, [Online] Available at: <http://www.cpni.gov.uk/Docs/ttea.pdf> (30 January 2008).
- Rajab, M., Ballard, L, Mavrommatis, P., Provos, N. and Zhao, X. (2010) *The Nocebo Effect on theWeb: An Analysis of Fake Anti-Virus Distribution*, Santa Clara: Google Inc., <http://krebsonsecurity.com/wp-content/uploads/2010/04/leet10.pdf>
- Rodgers, L. (2007) 'Smashing the criminals' e-bazaar', *BBC News Online*, 20 December, [Online] Available at: <http://news.bbc.co.uk/1/hi/uk/7084592.stm> (30 January 2008).
- Symantec (2009a) *Internet Security Threat Report Volume XIV: April*, 2009, <http://www.symantec.com/business/theme.jsp?themeid=threatreport>
- Symantec (2009b) *Symantec Report on Rogue Security Software July 2008 - June 2009*, October, http://eval.symantec.com/mktginfo/enterprise/white_papers/b-symc_report_on_rogue_security_software_WP_20016952.en-us.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
- Tapscott, D. and 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>
- Wall, D.S. (2007) *Cybercrime: The transformation of crime in the information age*, Cambridge: Polity
- Wall, D.S. (2008) 'Old tricks, new dogs - How to regulate cybercrimes', *Jane's Intelligence Review*, vol. 20, no. 10, pp: 45-47.
- Wall, D.S. (2010) 'Micro-frauds: Virtual Robberies, Stings and Scams in the Information Age', in T. Holt, T., and B. Schell (eds) *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, Hershey, PA (USA): IGI Global.
- Wall, D.S. (2010) 'Taking fright - The growing threat of scareware', *Jane's Intelligence Review*, vol. 22, no. 5, pp. 40-43
- Wall, D.S. (2011) *Organizational Security and the Insider Threat: Malicious, Negligent and Well-Meaning Insiders*, White Paper: Data Loss Prevention, Reading, UK: Symantec. https://www4.symantec.com/Vrt/offer?a_id=108920, accessed 1 August 2011.
- Warren, P. (2005) 'UK trojan siege has been running over a year', *The Register*, 17 June, [Online] Available at: www.theregister.co.uk/2005/06/17/niscc_warning/ (30 January 2008).

ⁱ McMillan, R. (2005) 'FBI: Cybercriminals Taking Cues From Mafia: Online criminals cost the U.S. more than \$67 billion last year, the FBI says', *PCWorld*, 7 August, http://www.pcworld.com/article/122242/web_of_crime_internet_gangs_go_global.html

Cassavoy, L. (2005) 'Web of Crime: Internet Gangs Go Global: The face of today's malware author is more adult than you might expect', *PCWorld*, 24 August,

http://www.pcworld.com/article/122242/web_of_crime_internet_gangs_go_global.html

ⁱⁱ Goodin, D. (2008) 'WarezoV botnet rises from the grave', *The Register*, 16 October, http://www.theregister.co.uk/2008/10/16/warezovs_second_coming/

-
- ⁱⁱⁱ Villeneuve, N. (2010) 'Koobface: Inside a Crimware Network', *Infowar Monitor*, November, <http://www.infowar-monitor.net/reports/iwm-koobface.pdf>
- ^{iv} Landesman, M. (2010) 'Asprox Botnet', *About.com Guide*, <http://antivirus.about.com/od/virusdescriptions/p/asprox.htm>
- ^v HelpNetSecurity (2010) 'Massive Mariposa botnet shut down', *HelpNetSecurity*, 10 March, <http://www.net-security.org/secworld.php?id=8962>
- ^{vi} Trend Micro (2009) *A Cybercrime Hub*, Trend Micro White Paper, http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/a_cybercrime_hub.pdf
- ^{vii} Parrack, D. (2007) 'Cybercrime gang raises fear of new malware crime wave', 10 November, <http://tech.blorge.com/Structure:%20/2007/11/10/cybercrime-gang-raises-fear-of-new-malware-crime-wave/>
- ^{viii} eSecurityPlanet (2010) 'Romanian Police Arrest eBay Cybercrime Gangs: The gangs phished eBay account credentials, then used those accounts to sell fake or non-existent goods', eSecurityPlanet, 8 April, <http://www.esecurityplanet.com/headlines/article.php/3875316/Romanian-Police-Arrest-eBay-Cybercrime-Gangs.htm>
- ^{ix} SCADA systems (Supervisory Control And Data Acquisition) is a computing system that is used to monitor and also to control major industrial processes ranging from some manufacturing processes to the utilities (electricity, water etc.) that comprise the infrastructure. There has been much concern that SCADA systems will become the focus for cyber-terrorists or become a means of committing Cyberwarfare and after many years of prophesies proof of concept arrived with the discovery of the Stuxnet.
- ^x Moldova Zeus arrests – money mule insiders 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/ Zeus was a combination of asymmetric hacking via malware and the use of insider money-mules
- ^{xi} 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>
- ^{xii} 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>
- ^{xiii} Kirk, J. (2010), 'Dutch Arrest 16-year-old Related to WikiLeaks Attacks', *PCWorld*, 9 December, http://www.pcworld.com/businesscenter/article/213120/dutch_arrest_16yearold_related_to_wikileaks_attacks.html
- ^{xiv} Singel, R. (2011) FBI Knocks Down 40 Doors in Probe of Pro-WikiLeaks Attackers, *Wired*, 27 January, <http://www.wired.com/threatlevel/2011/01/fbi-anonymous/>
- ^{xv} FBI (2011) 'Search Warrants Executed in the United States as Part of Ongoing Cyber Investigation', FBI National Press Releases, 27 January, http://www.fbi.gov/news/pressrel/press-releases/warrants_012711
- ^{xvi} Reuters (2011) 'UK police arrest WikiLeaks backers for cyber attacks', Reuters, 27 January, <http://uk.reuters.com/article/2011/01/27/idINIndia-54454720110127>
- ^{xvii} Whyte, S. (2011) 'Meet the hacktivist who tried to take down the government', *Sydney Morning Herald*, 14 March, <http://www.smh.com.au/technology/security/meet-the-hacktivist-who-tried-to-take-down-the-government-20110314-1btkt.html#ixzz1YLb1BjKr>
- ^{xviii} Belaza, M. (2011) 'La Policía española golpea a Anonymous: Detenidos tres administradores de la red de ciberactivismo en España / Podrían ir a prisión por "interrupción informática" y asociación ilícita', *EL Pais*, 10 June, http://www.elpais.com/articulo/espana/Policia/espanola/golpea/Anonymous/elpepuesp/20110610elpepunac_3/Tes
- ^{xix} Albanesius, C. (2011) 'Turkey Arrests 32 'Anonymous' Members', *PCMag.com*, 13 June, <http://www.pcmag.com/article2/0,2817,2386803,00.asp>
- ^{xx} BBC (2011) 'Police arrest 'hackers' in US, UK, Netherlands', *BBC News Online*, 20 July, <http://www.bbc.co.uk/news/world-us-canada-14212110>
- ^{xxi} Winter, J. (2011) 16 Suspected 'Anonymous' Hackers Arrested in Nationwide Sweep', *FoxNews.com*, 19 July, <http://www.foxnews.com/scitech/2011/07/19/exclusive-fbi-search-warrants-nationwide-hunt-anonymous/#ixzz1YLdzDXtu>