Dis-organised Crime: Towards a Distributed Model of the Organization of Cybercrime

Original article

Dis-organised Crime: Towards a Distributed Model of the Organization of Cybercrime

David S. Wall*

Abstract: There exists a widespread and uncritical assumption that the internet and society have been brought to their knees by Mafia-driven organised crime groups. Yet, this rhetorical narrative is not supported by research into the organisation of online crime groupings which finds that the organisation of crime online follows a different logic to the organisation of crime offline, a difference which is also reflected in organised crime groupings. Such findings identify instead a "disorganised" or distributed model of organization, rather than a hierarchical command and control structure. This article maps out the logic behind the organisation of criminal behaviour online before looking critically at the organised cybercrime debates. It then draws upon a simple analysis of the structures of known cybercrime groups and three case studies to explore their organization.

Keywords: Cybercrime – Mafia -- Organised crime -- Organisation of criminal behaviour

*David S. Wall is Professor of Criminology, Centre for Criminal Justice Studies, School of Law, University of Leeds, Leeds, UK.

Email: d.s.wall@leeds.ac.uk

The European Review of Organised Crime 2(2), 2015, 71-90

ISSN: 2312-1653

Introduction[1]

There exists an uncritical assumption in many media reports, police accounts, industry white papers and even academic publications that the internet and society have been brought to their knees by Mafia-driven organised crime groups. A simple Google search using the terms

“cybercrime” and “Mafia” reveals many such articles. Yet, upon further reading, the link between the two is often implied or the evidence to support the claim is scant, with little explanation of what the ‘mafia’ are, or even what “cybercrime” is. The latter is either discussed generically, usually with little regard for different cybercrime types, or a specific cybercrime type is fixated upon. The fact that the “command and control/ Mafia” rhetoric structures debates about the organization of cybercrime is not entirely surprising because it has long permeated the study of organised crime. Only in recent years have researchers sought to seriously challenge the viability of this narrative, see for example, Woodiwiss (2000), Woodiwiss and Hobbs (2009), Varese (2010), Campana (2011), Hobbs (2013), Lusthaus (2013), Lavorgna and Sergi (2014), Savona and Riccardi (2015).

When applied to the study of the way that cybercrimes are organised, the reductionism implied by the Mafia conspiracy myth not only confuses the public and policy makers, but it can also lead to the misdirection of police resources and also researchers’ efforts. As McCusker has observed, there is “a tension between logic and pragmatism” (2006: 257). The logic of the organised crime narrative suggests that the internet potential for generating high profits at low risk will attract organised crime groups. But, as McCusker and also Lavorgna and Sergi, (2014: 25) have observed, whether these groups or gangs have the capacity to pragmatically exploit the internet is not yet clear. Though, recent threat reports suggest that traditional mafia style organised crime groups may be beginning to migrate some areas of their operations to the internet to carry out more sophisticated versions of their existing criminal practices (EC3, 2014: 11). Of course, this sort of claim is not new and the rebuttal is that all crimes, not just cybercrimes, are organised in one way or another, so, it is important to understand more clearly the manner of such organisation. What is clear is that it is important to intellectually challenge the stereotypical Mafia conspiracy myth as a prime shaper of the cybercrime debates in order to forward our knowledge base and encourage more useful operational and analytical concepts to be developed; even if we end up re-engaging some of the narrative if a strong enough evidence base to support the association is subsequently found.

Drawing upon existing literature and an analysis of the structure of some of the known cybercrime “groups”, using data assembled largely from media reports, this article argues that the distinctive nature of cybercrime does not lend itself to the practices of mafia, especially the geographically based practice of extortion through a combination of offering protection from wider threats, and the fear of non-compliance. Instead, a distributed model for understanding cybercrime will be introduced. The first part of this article will look at the cyber-threat landscape, then map out the logic of cybercrime and explore the ways that the organisation of criminal behaviour has been transformed by new technology. The second part will look critically at the organised cybercrime debates. It will also draw upon a simple analysis of the structures of known recent cybercrimes to look at their organisation and its distributed nature. The third part looks at three case studies involving different types of cybercrime to explore their organisation. The final part concludes.

The Cybersecurity Threat Landscape and the Organisation of Cybercrime

Two and a half decades on since the birth of the internet, it is clear that the cybersecurity threat landscape has changed dramatically as networked technologies have transformed the way that online crime is organised. These threats have been further escalated in recent years as cybercrime has become *more professional* (see the stuxnet construction described later), and *more stealthy* via Rootkits[2], such as Zeus and the BEEBONE Botnet (see description later) (Simmons, 2015). In this post script-kiddie world, the offenders no longer want to be known or even admired. Cybercrimes have also become *more automated*, see the example of Ransomware and Fake AV, as well as *much larger* as recent distributed denial of service (DDOS) attacks illustrate. They have also become *more complex* with the maturing of social network media and the crime potential of the "The Cloud". Furthermore, these trends are compounded by emerging networked technologies that are currently being planned or in progress. *Mesh technologies* will join our digital "devices" to develop lateral networks; *self-deleting* communications, such as Tiger texts or Snapchat will eradicate evidence, and *crypto-currencies* (Bitcoin, Robocoin, Dodgecoin, Litecoin etc.) will create alternative value-exchange systems that could challenge the banking systems. Collectively, these three technologies will (further) challenge policing and attempts at imposing governance, especially cross-jurisdictionally. Moreover, there are also new forms of new criminal service delivery, which mimic online business services to commit crimes. Crimeware-as-a-service enables criminals to compose cybercrime attacks without requiring expert knowledge of computers or systems, as was once the case. The general concern about these developments is that the fear of crime that they give rise to will reduce incentives for legitimate businesses to invest in networked activities, whilst further encouraging the infiltration by offline organised criminals into online markets. Thus, widening the reassurance gap between the levels of security that are being demanded by the public and the levels of security that governments and police bodies can realistically deliver. The widening reassurance gap is not helped by the additional fear introduced by fears of an internet take over present in media reporting. We, therefore, need to develop a more accurate and 'nuanced' dynamic and distributed explanation of the organisation of cybercrime.

The Transformation of Criminal Behaviour Online

Networked technologies have—in three main ways—brought about a fundamental transformation of criminal behaviour and a very different logic of organisation to that found in offline organised crime. Firstly, network technologies not only *globalise* the communication of information, ideas and desires, but they also impact locally by causing a *glocalising* effect, which is the global impact upon the local. For example, a scam committed from one country upon victims in another will create a need to expand policing there in order to deal with it. Secondly, network technologies create the potential for *asymmetric relationships* where one person can victimise many at the same time. Thirdly, network technologies and associated social network media are creating *new forms of networked social relationships* that act as the source of new criminal opportunities (Wall, 2007; Wall, 2013a) and crimes such as stalking, bullying, fraud, sexting and sex-extortion etc. The upshot

is that crime can now be global, informational, and distributed (see Castells, 2000), but also simultaneously synoptic and panoptic, and data trails can be captured to entrap victims. Crimes online (cybercrime) can be committed at a distance, much more quickly and in much greater volume. This “cyber-lift” marks out cybercrimes as different from crime offline.

New forms of criminal opportunity are being created that are also *changing the way that crime is taking place*. Criminal labour, because committing crime is a form of labour, is rapidly becoming deskilled and reskilled simultaneously (see Wall, 2007: 42). Furthermore, as indicated earlier, the entry level skills of cybercrime have fallen as technologies have become automated to the point that malware can now operate by itself (see Fake AV/ Ransomware, Stuxnet later), or be rented or bought off the shelf via crimeware-as-a-service. In many ways, the technology has effectively “disappeared” in that its operation is intuitive and offenders no longer require the programming skills that they once did. Another significant development has been the drop in the cost of technologies which has dramatically reduced the start-up costs of crime.

Put in simple terms, networked technologies create an environment in which there is no need for criminals to commit a large crime at great risk to themselves anymore, because one person can now commit many small crimes with lesser risk to themselves. The modern bank robber can, for example, contemplate committing 50m X £1 thefts themselves from the comfort and safety of their own home, rather than commit a single £50m robbery with its complex collection of criminal skill sets and high levels of personal risk (Wall, 2007: 3, 70). The impact of these transformations upon crime is that the average person can, theoretically, now commit many crimes simultaneously in ways not previously imagined and previously beyond their financial and organisational means, and on a global scale. If not a bank robbery, then they can commit a major hack, DDOS attack, hate speech campaign, or fraud; see for example, the case of Lomas who scammed 10,000 victims out of £21m (BBC, 2015). The fact that one person, or a few, can now control whole criminal processes has profound implications for our understanding of the organisation of cybercrime. In a rather cynical way, the internet has effectively democratised crimes such as fraud that were once seen as the crimes of the powerful and the privileged. There is, however, an underlying (almost ideological) assumption that a new internet mafia is forming. As mentioned earlier, all crime is organised, but all crime is not “organised crime”, so we need to briefly understand how cybercrime differs from other crimes.

Mapping out Cybercrime

As to what constitutes cybercrime is very contentious, because whilst everybody agrees it exists, not everybody is in agreement as to what it is (Wall, 2007: 2014b). The following brief outline of cybercrime helps us understand how cybercrimes are organised. The “transformation test” (Wall, 2007) is one way of separating cybercrimes from noncybercrimes. This is where the impact of networked technologies (the “Cyber-lift”) is removed from the crime to see what would be left. The range of cybercrimes described in the literature varies in terms of its *mediation by technologies*. At one end of the spectrum are cyber-assisted crimes[3] that use the internet in their organisation, but

which would still take place if the internet was removed. At the other end of the spectrum are Cyberdependent crimes that are *of* the internet. They are the spawn of the internet, and if the internet (networked technologies) is taken away, then they simply disappear. Of course this cannot be done and the "transformation test" is simply a mnemonic that helps establish a principle. In between the cyber-assisted and cyber-dependent crimes are a range of hybrid Cyber-enabled crimes, that include most types of frauds. They are existing crimes in law, but are given a global reach by the internet, for example, Ponzi frauds and pyramid scams. Take away the internet, and these crimes still happen, but at a much more localised level. They lose the global, informational and distributed lift that is characteristic of "cyber". Once the level of mediation by technology has been identified then the *Modus Operandi* needs to be considered. We therefore need to distinguish between (1) crimes against the machine (hacking, DDOS attacks etc.), which are very different from (2) crimes using the machine (frauds etc.) and (3) crimes in the machine (extreme pornography, hate speech, and social networking originated offences). Yet, the distinction between them is rarely made. Finally, the treatment of cybercrimes also needs to be differentiated by *victim group,* whether victims are individuals, organisations (inc. corporate) or nation states (see Wall, 2005/10, 2014b). Each has different implications for understanding the levels of victimisation experienced, but also the offenders and the way that they organise cybercrimes. We shall come back to this later.

The Logic behind the "Organised" Cybercrime Debate

The debate over organised crime groups and the internet will arguably run on forever because the topic is so highly emotive and newsworthy. It also carries a powerful cultural logic that is rarely challenged, especially as various statistics clearly show that the internet is increasingly being 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 comparatively little is actually known about them or how they are organised.

Susan Brenner prophetically stated in her 2002 study of organised criminal activity on the internet that organised cybercrime would most likely manifest itself in "transient, lateral and fluid" forms. Especially as networks of criminals (Brenner, 2002, p. 1), rather than replicating 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 organisations have evolved in response to real world opportunities and constraints that are largely absent in cyberspace. Almost a decade and a half on, Brenner's 2002 prediction still stands, as new forms of online criminal organisation tend to differ greatly from the command and control mafia model. Lavorgna and Sergi, found, in their study that "there is still lack of clear evidence concerning the real presence of organised crime in the eSociety and the extent to which organised criminal groups use the

Internet” (Lavorgna and Sergi, 2014: 25; also see Lusthaus, 2013).

The criminal commercialisation of the botnet—(robot) networks of infected computers that can be operated remotely by criminals—has been a major crime multiplier since its emergence in 2004 onwards. Virus writers originally sold the IP addresses of computers infected with their remote administration Trojans to spammers (C’T, 2004; Wall, 2007). The latest iteration of the botnet is to bundle it in with crimeware-as-aservice (Walker, 2014), which is effectively a suite of malicious software constructed by criminals to hire out to other criminals. It is a classic example of the deskilling and reskilling process mentioned earlier. Whereas it was once the case that cyber-criminals needed a sophisticated knowledge of programming and systems, today the opposite is the case. Now, would-be criminals can hire the software to commit crimes such as online frauds or DDOS attacks and so on. Crimeware-as-a-service can be created by an individual or very small group of people who then maintain it. Even the actual sales process is automated!

The rise of crimeware coincided with the emergence of the stealthy “high-tech” gang[4], as opposed to the “script kiddie” who wanted to be known for his or her exploits. An early 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). Again, the composition of these “gangs” was relatively small; which reflects McGuire’s (2012: 58) analysis of the organisation of online crime, especially the online centric “swarms” and “hubs”.

Other hi-tech gangs were exposed in “Operation Firewall” between 2004 and 2005, which led to the investigation and prosecution of “shadowcrew”, an international identity theft network that hosted online forums which 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 organisation. The, then, head of e-crime at the Serious Organised Crime Agency (SOCA) (National Crime Agency since 2013) 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 tend to 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). More recent examples, would suggest that this model still persists, though some of these roles have now been deskilled and automated (see earlier) and they distance themselves even more from the actual crime by operating crimeware-as-a-service. The opportunity to commit crime is now being offered to criminals along the same principles as, say, the distribution of music is now being delivered as a (streaming) service via Spotify, Apple Music, and others.

Listed below are examples of some known cybercrime groups/ forums operating between

2000-2015, including their areas of main criminal activity and an indication of years active. Although the initial emphasis was upon groups operating during the decade 2000-2010, others were later added. Little difference was found in the construction of later groups, such as GameOver Zeus (Sandee, 2015), Lizard Squad (2015)[5] or even forums such as Darkode (Kelion, 20015). Please note that because of their distributed nature these examples are not entirely exhaustive, they are merely intended to be illustrative and a representation of a cadre. Furthermore they are not mutually exclusive as there was often overlap between them. Often the same individuals might be involved in more than one gang; or it may be a later iteration of a previous grouping.

- **Carding and ID theft Operations** - International Carder's Alliance (see McMillan, 2006); IAACA (the International Association for the Advancement of Criminal Activity); CarderPlanet (until 2003); Darkprofits (until 2003); Shadowcrew; (until Operation Firewall 2004/5); The Rock Phish gang (2006-2008); Avalanche (2009 thought to be a successor of the Rock Phish gang); Mazafaka (2005); TJ Maxx Gang (2005-2007).
- **Botnet operations** - Rustock (2006-2011); Warezov (Storm Botnet) (2006-2008); Blackcarder; Storm Worm (2007-2008); Celebrity Spam (based upon Storm); Koobface (2009-2010); Asprox (2008-2010); Mariposa (2008-2009); Zeus (2007); Gameover Zeus (2011+); Conficker (2008-); Waladec (2009-2010)
- **Cybercrime Hubs -** Tartu, Estonia – Cybercrime server – 2005-2008 (cybercrime businesshostingRogue DNS servers); The Russian Business Network (2006-)
- **Spammer Operations -** Superzonda (2003)
- **Malware Development and Distribution Specialists** - The Hangup Team (2012); Drink or Die (1993-2001)
- **Auction fraud -** Romanian eBay Fraud Gangs (2009-2011)
- **Hackers/hactivist** – Anonymous (2004+); LulzSec (2011-) (and copycat LulzRaft 2011); Team Poison (2008-2012, 2015); Impact Team (2015); Lizard Squad (2015)
- **Scammers** - Sakawa Boys (Ghana) (2012+)

The detailed composition of each of the above is actually quite hard to quantify; partly because (as stated earlier) they continually change composition and mission, and partly because the media coverage of the cases involving them are often framed in terms of more conventional organised crime debates than reflecting the actual operation of the grouping. The reportage tends to reify them and their activities, turning what are often quite abstract activities into “things” that are much easier to report upon and communicate, but which lose their essence in translation. What the list does show, however, is the relatively new forms of networked criminal organisation that depart from the more traditional forms in the organised crime debates. Although these gangs specialised in a range of different offences, they display many similar organising characteristics. Some are drawn together by the crime, but many are distributed affinity groups, formed around “affinities”, shared interests or common goals (see Eschle, 2004; and Gamson, 1992) which they share through distributed networked media. In brief, they display common characteristics in that they are fairly ephemeral and amorphous in terms of organisation and flex according to the demands and opportunities of the day. They also seem to be self-contained and almost akin to small cottage-

industries in structure (see further McGuire, 2012 and also Yip et al., 2013). They are often driven by an individual or by a very small group, but—not always, because the organising principle is often affinity with central common idea or even an ethic. They can also be very reactive in response to circumstances (see for example Anonymous). So, just because they are Russian or Eastern European in origin, or are based upon servers in those countries, it is not prima facie evidence of a link to a hierarchical organised crime group. 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" based protection, thus evading two well-known hooks of traditional organised crime organisations—finance and physical protection.

The key difference between cybercrime and traditional crime lies its informational nature, networked structure and global reach (see Castells, 2000 as outlined earlier, but also BBC, 2007; Goodin, 2007a&b; Wall and Williams, 2007). So we find that cybercrime is increasingly taking on a participatory or "Wiki" form of co-production via collaborative efforts. The offenders are literally distributed across the internet and not geographically located in one single place. A useful illustration of such a collaboration can be found in Wall (2007: 66-68) where an online group instructs a "newbie" on how to commit a hack. In this example the 'group' is bound together by a reputational economy in which a hierarchy of respect orders the members. It is a model that has persisted, and persists in many contemporary cybercrime forums, see for example the reports of the takedown of the Darkode hacking forum (Kelion, 20015). Thus, cybercrimes and cybercriminals, by their very informational, networked and global nature go against the very grain of the traditional model of socially and geographically rooted organised crime models. As observed earlier, cybercriminals evade control by traditional organised crime groups in much the same way as they evade control by, say, government.

These forms of organisation reflect the fourth and fifth categories of the UNODC (2002) organisational crime forms—in contrast to the Standard, Regional and Clustered hierarchies. These fourth and fifth categories are the "Core groups" with relatively tightly organisation, but unstructured groupings, often surrounded by a network of individuals engaged in criminal activities, and "Criminal networks" which are loose and fluid networks of individuals, often drawing on individuals with particular skills, who constitute themselves around an ongoing series of criminal projects (UNODC, 2002: 34).

Exploring the Organisation of Cybercrime: Three Case Studies

Below are three examples of cybercrime and indications of their organisation. Stuxnet is a (state sponsored) crime *against* the machine (Leyden, 2015), Fake AV/ Ransomware fraud are crimes that *use* the machine and data leakage is (potentially) a crime in the machine because of the appropriation of data (See Wall, 2005/10; 2014b).

Crimes against the Machine – STUXNET

Stuxnet was a form of state-sponsored malware that was used within an intranet (rather than the internet) to sabotage industrial control systems (SCADA) by seeking out a particular operating system and a specific piece of hardware—the centrifuges of an Iranian Nuclear reactor. What is known, or deduced, about its organisation is that it was created by a hacker group commissioned by, or with links to, governments (Halliday, 2010). Stuxnet's creation suggests a small core group, possibly as small as four or five people, but with access to a broader group from whom specific expert help was provided (Halliday, 2010). It is believed that the commissioners of Stuxnet, not only obtained key information about the targets from insiders within the organisations who made the machines and systems that the software was designed to attack (Falliere et al., 2010), but, they also used insiders within the target organisation to introduce the malware into the intranet. Although Stuxnet is not unique in requiring insider complicity, see, for example, the Hydraq Trojan (Symantec, 2010; Wall, 2013b), it has, however, highlighted the insider threat issue, which is a major concern today. The discovery of custom-built malware variants of this type (such as Duqu, a Stuxnet variant) will continue this practice (Zetter, 2010).

Crimes Using the Machine – Fake Anti Virus/ Ransomware

Fake AV and Ransomware are types of malicious software that possess similarities in that they both obtain money from the victim by extortion. The former is very subtle and the latter more overt. Both originate from the earlier "scareware", which defrauded its victims by scaring them into paying for software that offers to fix their computer. Once infected, the computer screen would freeze and then the screen image would appear to shatter and the pieces fall to the bottom of the screen. A skull mocking the victim would then appear in the void. The victim would have to buy a code in order to release the screen. Scareware evolved into the more covert Fake Anti-Virus (Fake AV) software that emulates the trusted signs and symbols—the look and feel—of an operating system to subtly deceive victims into paying for software patches, which they do not need, without them being aware that they had been scammed. Ransomware, in contrast is a variant of Scareware that emerged in the late 2000s and combined some of the more brutal elements of scareware with a colder and more professional delivery, including helplines to guide the victim through the payment and code release process. Once a victim's computer becomes infected by Ransomware, he/ she is asked to make a payment, often using crypto-currency (typically Bitcoins), in order to get a code that releases their data.

Both *Fake AV and Ransomware* signify an important milestone in the evolution of cybercrime. Not only are they good examples of a "true" cybercrime being spawned purely by the internet (see further Wall, 2007: 47, 2008), but possibly for the first time, they provide evidence of the large scale total automation of a criminal process by malicious software. The malware not only infects the victims' computer and conducts the scam, but it also takes the victim's money and deposits it into

the offender's bank account without the offender being present. Other prevalent forms of "true" cybercrime such as Phishing (ID Theft), by comparison, are also automated by software, but only to the extent that they "socially engineer" personal financial information from victims and send it directly to the offenders. Offenders then need to employ a third party, a "money mule", to monetarise the stolen ID information by removing money from victim's accounts (Leyden, 2010).

Fake AV is the more interesting of the two offspring of scareware because whilst it is deceptive, it also deliberately operates on the margins of criminality avoiding prosecution. Fake AV operations are, 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, especially frauds, but also in the organisation of crimes against the machine (hacking, DDOS etc.) and crimes in the machine relating to content (such as extreme pornography etc.). A successful Fake AV project will require the establishment of a financial partnership between the "Kingpin" (or "Merchant"), whose ideas initiate the project and who has access to the malware to be used. An "Affiliate" will introduce the Kingpin 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 mainstream Affiliate Marketing practices, a secondary tier of players, the "brokers", are used to bring together Kingpins and Affiliates and broker their relationship on a commission basis. This model of activity is roughly similar to that of the structure of Carderplanet, a forum for selling stolen credit card details online that is documented in greater detail in Holt and Lampe (2010), Glenny, (2011) and Yip et al, (2013). But the structure also occurs with regularity in investigations into "darkweb" or "darknet" activities (see for example, Martin, 2014). So, the relationship between the various actors is different, if not oppositional, to the "command and control" Mafia-type relationship because the participants are networked and 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, using brokers and affiliates (recently replaced by crimeware as a service). In fact, Ransomware is now provided as a service, Encryptor RaaS, via the Tor network (the Darkweb) (see Dela Paz, 2015).

An analysis of Fake AV scams also assists our understanding of the victim market place. Firstly, the overall number of offenders trying to emulate the financial success of the "pioneer Kingpins" quickly increased in number and, not only diluted the victim market, but also diminished the individual yield from the scam and its overall attractiveness to criminals. One response by the successful Kingpins was to police new entrants by informing the cybersecurity companies of their activities. Secondly, although the growth in size of the offender pool increased the numbers of players and different Fake AV programmes circulating, many of these were "re-skinned" and given a new appearance, but remained variations of the originals with similar code. This means that the security industry, using its security software, could 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 potential victims more risk averse and suspicious of Fake AV, thus further reducing the likelihood of victims falling for the scam. Thirdly, a trend noticed from 2009 onwards has been to encourage victims to buy the Fake AV 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 threatens the business of the successful Kingpins and also the legitimate security industry, whose brands are being counterfeited or exploited. As a result, the Kingpins effectively act alongside (though not with) the legitimate security industry to protect their own interests by seeking to close down the offenders. Microsoft famously used intellectual property laws to police this crime in lieu of criminal law (Leyden, 2009). A fourth trend emerged when some of the original scareware Kingpins redeveloped their Fake AV in favour of more quasi-legitimate versions that not only have carefully constructed terms and conditions, but also have a visible therapeutic effect on the computer. These new versions discard unused files and empty caches, thus improving customer satisfaction and making prosecution almost impossible.

The proliferation of wholly automated crime means that we are entering the era of "the long tail" of crime, mimicking Chris Anderson's analysis of business in the information age. Anderson (2006) 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) and have the proceeds of the crime sent to their bank account whilst they are asleep. That is what is different about Fake AV and Ransomware.

New Crimes in the Machine – Data Leakage and Social Networking Media

The comparatively recent example of the contentious protection by hacker groups of Wikileaks is another interesting example of the breadth of cybercrime and also provides an insight into its organisation. Wikileaks, which it must be strongly emphasised is *not* a criminal organisation, though it is often treated as such in some of the security debates and discussions, is 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 which are used to spread its messages. Of more importance to this article is the fact that Wikileaks has invoked the support of powerful affinity 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 bring to the fore 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 deviant missions (of which some are criminal) and also the complexity of the organisation of cybercrime. Prior to taking up the Wikileaks cause, Anonymous, a group encouraging civil disobedience amongst 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).

Since taking up the Wikileaks cause in 2010, Anonymous have successfully attacked a number of different organisations that have tried to prevent Wikileaks from carrying out their mission. Firstly, they have hacked into and exposed the weaknesses of the organisations in order to humiliate them, such as taking client data, though not using it. Secondly, they have prevented access by launching DDOS Attacks (Distributed Denial of Service). Not only have these attacks achieved their goal of disrupting the target organisations, but they also seem to have caused some reputational damage to those organisations 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, it is alleged, had a fairly small core of about six members (Weisenthal, 2011) supported by a group of about 5-6 others. This information was obtained in 2011 from other hacking groups who released the personal information of LulzSec members on the internet. The internet relay chat (IRC) logs were leaked to *The Guardian,* but the membership was independently confirmed (Poeter, 2011) Whether Anonymous and LulzSec were true hacktivists or just young rebels looking for a cause (or both) is still quite unclear because of the varied and responsive nature of their activites, but what can be observed from them as a case study is that their organisation, like that of the Stuxnet builders and Ransomeware and Fake AV peddlers is flat and distributed. 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 there are suspicions that a so-called leaked FBI report on the profiles of Anonymous may also have been faked (Leyden, 2011; Donoghue and Roberts, 2011). Whilst this ability to manipulate its presence potentially obfuscates any deep understanding of Anonymous or LulzSec, the arrest patterns that have emerged since investigations into their organisation suggest a globally distributed network (or possibly 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 utilised to mobilise 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 may have been mentored by older members of Chaos Computer Club. Drawing further upon information from the reports of the various arrests 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 that utilises chat rooms to organise the decision to launch an attack.

Conclusion: Towards a Distributed Model of Organised Crime Online

The organisation of Stuxnet and Fake AV/ Ransomware and Anonymous /LulzSec each illustrate quite different sets of offender motivations, levels of professionalism and organisation, but they also indicate some similarities in terms of their organising principles. The core group dynamic of all three appears to be based upon a reputational economy that binds the group together, and personal status within this type of group is therefore related to the participant's individual reputational strength. Furthermore, the similarities continue, with Stuxnet Malware (though a contested view), the offender group was a small, possibly professional, group of about four or five people who drew upon the services or help of others and affiliates. Fake AV and Ransomware were driven mainly by the Kingpin (who had the idea and the bankroll), and who was introduced to an Affiliate via a Broker to gain access to victims online. The Kingpins then used online banking services themselves, or occasionally through a Money Mule, to transfer the stolen money to their own bank accounts, possibly via a Lynchpin who might launder it. The hacker groups were, in comparison, more distributed, but coalesced to form an assemblage around a set of affinities, ideas/ ethics, to protect Wikileaks, who is also the affiliate in this case.

In all three examples the Kingpins sought the assistance of a broader group of participants who exist outside the central grouping, but within the idea frame (the crime), and who can help to solve problems related to the criminal activity being designed, built or carried out. There may even be a further layer of individuals linked to the group who are outside the idea frame and who will give advice on specific issues. Sometimes individuals just fall out of the information loop, or they are pushed out, or they leave, which makes the structure ephemeral. One thing that is certain is that the structure 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 (after Deluze, see argument in Haggerty and Ericson, 2000). They all point 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 core idea. The interesting corollary here is that this distributed type of organisation does bear some similarities to the organisation of many offline organised groups in the UK, see Sergi's (2015) "English Activity" model, and also in many countries in Europe without

large socio-geographical Mafia organisations (see Europol, 2015 and Savona and Riccardi, 2015). They also reflect the UNODC organised crime group typologies (4 & 5) (2002: 34). It must be pointed out, however, that whilst there are some apparent similarities between the two and the modern geographically located OCG may use internet based technologies to organise themselves (such as email and mobile phones), the differences are much greater. The online OC members discussed here are entirely different from the (offline) OC members in that they may never have met and they may be distributed across different countries and not know it, plus the crimes committed are primarily informationally based.

The Stuxnet, Ransomware/ Fake AV or Anonymous stories and others 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 organisation 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 Fake AV/ Ransomware, and networking process tends to undermine attempts to effect control (Wall, 2007: 39). However, whilst Fake AV/ Ransomware, phishing and other forms of cybercrime do not display the classic signs of organised crime, they do display distinctively different organisational 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 organisation of crime online follows a different logic to both organised crime and also the organisation 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 be regulated and managed to minimise its impacts. This means that counter-cybercrime strategies, including prevention, therefore need to focus 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 (Wall, 2013c).

References

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

BBC (2007) Arrests made in botnet crackdown, *BBC News Online*, 30 November, available at: http://news.bbc.co.uk/1/hi/technology/7120251.stm [accessed on 13th March 2013].

BBC (2015) ‘Promoter of £21m pyramid scam ordered to pay back £1’, BBC News Online, 15 July, available at: http://www.bbc.co.uk/news/uk-england-bristol33536824 [accessed on 15 July 2015].

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

Campana P (2011) Eavesdropping on the Mob: the functional diversification of Mafia activities across territories, *European Journal of Criminology* 8(3): 213-228.

Castells M (2000) Materials for an explanatory theory of the network society, *British Journal of Sociology* 51(1): 5–24.

C’T (2004) Uncovered: trojans as spam robots, *C’T Magazine*, 23 February, available at: www.heise.de/english/newsticker/news/44879 [accessed on 13th March 2013]. Dela Paz R. (2015) Encryptor RaaS: Yet another new Ransomware-as-a-Service on the Block, *FORTINET Blogs, Security Research, threat landscapes and analysis*, 29 July, available at: http://blog.fortinet.com/post/encryptor-raas-yet-another-newransomware-as-a-service-on-the-block

Dimitrova C (2004) Busting “Shadowcrew” and “Darkprofits”, *The Sofia Echo*, 18 November, available at: http://sofiaecho.com/2004/11/18/633159_bustingshadowcrew-and-darkprofits [accessed on 8th April 2015].

Donoghue B and Roberts P (2011) FBI: Psychological Profile of Anonymous Leadership is a Fake, *Threat Post*, 15 September, available at:

http://threatpost.com/en_us/blogs/fbi-psychological-profile-anonymousleadership-fake-091511 [accessed on 13th March 2013].

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

EC3 (2014) *Internet Organized Crime Threat Assessment*, European Cybercrime Centre (EC3).The Hague: Europol, available at:

https://www.europol.europa.eu/content/internet-organized-crime-threatassesment-iocta [accessed on 1st April 2015].

Eschle C (2004) Constructing the “anti-globalisation movement”. In C. Eschle and B. Maiguashca (eds.), *Critical Theories, IR and 'the Anti-Globalisation Movement': The Politics of Global Resistance*. London: Routledge.

Europol (2015) Exploring Tomorrow's Organised Crime, The Hague: Europol, available

at:

https://www.europol.europa.eu/sites/default/files/Europol_OrgCrimeReport_web -final.pdf [accessed 15th June 2015].

Falliere N, Murchu L and Chien E (2010) *W32.Stuxnet Dossier: September 2010, version 1.0*.

Symantec White Paper, available at:

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf [accessed on 13th March 2013].

Gamson W (1992) The Social Psychology of Collective Action. In A. Morris and C. Mueller (eds.), *Frontiers in Social Movement Theory*. New Haven: Yale University Press.

Glenny M (2011) *Darkmarket: Cyberthieves, Cybercops and You*. London: The Bodley Head.

Goodin D (2007a) Botmaster owns up to 250,000 zombie PCs: He's a security consultant.

Jail beckons, *The Register*, 9 November, available at:

http://www.theregister.co.uk/2007/11/09/botmaster_to_plea_guilty/ [accessed on 13th March 2013].

Goodin D (2007b) FBI crackdown on botnets gets results, but damage continues: 2 million zombies and counting, *The Register,* 29 November, available at:

http://www.theregister.co.uk/2007/11/29/fbi_botnet_progress_report/ [accessed on 13th March 2013].

Haggerty K and Ericson R (2000) The Surveillant Assemblage, *British Journal of Sociology* 51(4): 605-622.

Halliday J (2010) Stuxnet worm is the work of a national government agency, *The Guardian*, 24 September, available at:

http://www.guardian.co.uk/technology/2010/sep/24/stuxnet-worm-nationalagency [accessed on 13th March 2013].

Hobbs D (2013) *Lush Life*. Oxford: Clarendon Press.

Holt T and Lampke E (2010) Exploring stolen data markets online: products and market forces. *Criminal Justice Studies* 23(1): 33–50.

Kelion L (2015) Darkode hacking forum forced offline, *BBC News Online*, 15 July, available at: http://www.bbc.co.uk/news/technology-33542490 [accessed on 15th July 2015].

Landers C (2008) Serious Business: Anonymous Takes On Scientology (and Doesn't Afraid of Anything), *Baltimore City Paper*, 2 April, available at:

http://www2.citypaper.com/columns/story.asp?id=15543 [accessed on 13th March 2013].

Lavorgna A and Sergi A (2014) Types of organized crime in Italy. The multifaceted spectrum of Italian criminal associations and their different attitudes in the financial crisis and in the use of Internet technologies, *International Journal of Law, Crime and Justice* 42(1):16-32.

Leyden J (2009) Bogus anti-spyware firm fined $1m, *The Register*, 5 December, available at:

http://www.theregister.co.uk/2006/12/05/washington_anti-spware_lawsuit/ [accessed on 13th March 2013].

Leyden J (2010) Bank insiders charged in ZeuS cybercrime smackdown, *The Register*, 8 November, available at:

http://www.theregister.co.uk/2010/11/08/zeus_moldova_bank_worker_arrests/ [accessed on 13th March 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, available at: http://www.theregister.co.uk/2011/09/16/anon_fbi_profile_fakery/ [accessed on 13th March 2013].

Leyden J (2015) Ukraine conflict spilling over into cyber-crime, warns former spy boss, *The Register*, 16 April, available at: http://www.theregister.co.uk/2015/04/16/cyber_war_keynote_infiltrate/ [accessed on 13th March 2013].

Lusthaus J (2013) How organised is organised cybercrime?, *Global Crime*, DOI:10.1080/17440572.2012.759508.

Martin J (2014) *Drugs on the Dark Net: How Cryptomarkets Are Transforming the Global Trade in Illicit Drugs*. London: Palgrave Macmillan.

McCusker R (2006) Transnational organized cyber crime: distinguishing threat from reality. *Crime*

Law and Social Change 46(4-5): 257-273.

McGuire M (2012) *Organized Crime in the Digital Age*. London: John Grieve Centre for Policing and Security & Detica.

McGuire M and Dowling S (2013) *Cyber crime: A review of the evidence: Summary of key findings and implications*. Home Office Research Report 75. London: Home Office, October.

McMillan R (2006) FBI: Cybercriminals Taking Cues From Mafia, *PCWorld*, 7 August, available at: http://www.pcworld.com/article/126664/article.html [accessed on 8 April 2015]

NISCC (2005) Targeted trojan email attacks, *NISCC Briefing* 08/2005, 16 June, available at: http://www.cpni.gov.uk/Docs/ttea.pdf [accessed on 30th January 2008].

Poeter D (2011) Who is LulzSec?, *PC*, available at:

http://www.pcmag.com/slideshow/story/266414/who-is-lulzsec [accessed on 8 April 2015].

Rodgers L (2007) Smashing the criminal's e-bazaar, *BBC News Online*, 20 December, available at: http://news.bbc.co.uk/1/hi/uk/7084592.stm [accessed on 13th March 2013].

Sandee M (2015) GameOver Zeus – Backgrounds on the Badguys and the Backends, FoxIt, White Paper, 5 August, available at: https://www.fox-

it.com/en/files/2015/08/FoxIT-Whitepaper_Blackhat-web.pdf [accessed on 8 July 2015].

Savona E and Riccardi M (2015) (eds.) *From illegal markets to legitimate businesses: the portfolio of organized crime in Europe, Final Report of EU co-funded Project OCP* – Organized Crime Portfolio. Milan: Transcrime.

Sergi A (2015) Divergent mind-sets, convergent policies: Policing models against organized crime in Italy and in England within international frameworks, *European Journal of Criminology*, online version, doi:10.1177/1477370815578196.

Simmons D (2015) Europol kills off shape-shifting 'Mystique' malware, *BBC News Online*, 9 April, accessible from: http://www.bbc.co.uk/news/technology-32218381 [accessed 11 April 2015].

Symantec (2010) *Symantec Global Internet Security Threat Report Trends for 2009*, Volume XV. April, available at:

http://eval.symantec.com/mktginfo/enterprise/white_papers/bwhitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf [accessed on 13th March 2013].

UNODC (2002) Results of a pilot survey of forty selected organized criminal groups in sixteen countries, Global Programme Against Transnational Organized Crime, September, available at:

http://www.unodc.org/pdf/crime/publications/Pilot_survey.pdf [accessed on 8th May, 2015].

VFC (2009) *2009 Virginia Terrorism Threat Assessment, Commonwealth of Virginia*, Department of State Police. Virginia Fusion Center. March, available at:

http://www.infowars.com/media/vafusioncenterterrorassessment.pdf [accessed on 13th March 2013].

Wall D (2005/10) The Internet as a Conduit for Criminal Activity, in A. Pattavina (ed.) *Information Technology and the Criminal Justice System*. Thousand Oaks, CA: Sage. Wall D (2007) *Cybercrime: The transformation of crime in the information age*. Cambridge: Polity.

Wall D (2010) The Organization of Cybercrime and Organized Cybercrime. In M. Bellini, P. Brunst, and J. Jaenke (eds.), *Current issues in IT security*, Freiburg: Max-PlanckInstituts für ausländisches und internationales Strafrecht.

Wall D (2013a) Policing Identity Crimes, *Policing and Society: An International Journal of Research and Policy* 23(4): 437-460.

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

Wall D (2013c) Locking up Cybercriminals can do more harm than good, *The Conversation*, 10 July, available at:
http://theconversation.com/locking-up-hackers-could-domore-harm-than-good-15889 [accessed on 13th March 2013].

Wall D (2014a) Internet Mafias? The Dis-Organization of Crime on the Internet. In S.

Caneppele and F. Calderoni (eds.), *Organized Crime, Corruption, and Crime Prevention: Essays in Honor of Ernesto U. Savona.* Switzerland: Springer International Publishing.

Wall D (2014b) High risk cyber-crime is really a mixed bag of threats, *The Conversation*, 17 November, available at: https://theconversation.com/high-risk-cyber-crime-isreally-a-mixed-bag-of-threats-3409 [accessed on 13th March 2013].

Wall D and Williams M (2007) Policing Diversity in the Digital Age: Maintaining Order in Virtual Communities. *Criminology and Criminal Justice* 7(4): 391–415.

Warren P (2005) UK trojan siege has been running over a year, *The Register*, 17 June, available at: http://www.theregister.co.uk/2005/06/17/niscc_warning/ [accessed on 13th March 2013].

Weisenthal J (2011) Notorious Hacker Group LulzSec Just Announced That It's Finished, Business Insider, *Silicon Alley Insider*, 25 June, available at:

http://www.businessinsider.com/lulzsec-finished-2011-6 [accessed on 13th March 2013].

Woodiwiss M (2000) Organized Crime - The Dumbing of Discourse, *British Criminology Conference: Selected Proceedings*. Volume 3, available at:

http//:www.britsoccrim.org/volume1/017.pdf [accessed on 8th May 2015].

Woodiwiss M and Hobbs D (2009) Organized Crime and the Atlantic Alliance: Moral Panics and the Rhetoric of Organized Crime Policing in America and Britain. *British Journal of Criminology* 49(1): 106–128.

Yip M, Webber C, and Shadbolt N (2013) Trust among Cybercriminals? Carding Forums, Uncertainty and Implications for Policing, *Policing and Society* 23 (4): 516-539.

Zetter K (2011) DHS Fears a Modified Stuxnet Could Attack U.S. Infrastructure, *WIRED*, 26 July, available at http://www.wired.com/threatlevel/2011/07/dhs-fearsstuxnet-attacks/ [accessed on 13th March 2013].