Trust among Cybercriminals? Carding Forums, Uncertainty and Implications for Policing

Michael Yip

Web Science Doctoral Training Centre, Electronic and Computer Science, University of Southampton, Southampton, U.K.

Contact: my2e09@ecs.soton.ac.uk

Craig Webber

Institute of Criminal Justice Research, School of Social Sciences, University of Southampton, Southampton, U.K.

Contact: c.webber@soton.ac.uk

Nigel Shadbolt

Web and Internet Science Research Group, Electronics and Computer Science, University of Southampton, Southampton, U.K.

Contact: nrs@ecs.soton.ac.uk

To cite this article:

Yip, M., Webber, C., and Shadbolt, N., 2013. Trust among Cybercriminals? Carding Forums, Uncertainty and Implications for Policing. *Journal of Policing and Society*.

Trust among Cybercriminals? Carding Forums, Uncertainty and Implications for Policing

At the beginning of the 21st Century, before the power of online social networking became apparent, several studies speculated about the likely structure of organised cybercrime (Mann and Sutton 1998; Brenner 2002). In the light of new data on cybercriminal organisations, this paper sets out to revisit their claims. In collaboration with the Serious Organised Crime Agency (SOCA), this paper examines the structure of organised cybercrime by analysing data from online underground markets previously in operation over the Internet. In order to understand the various structures of organised cybercrime which have manifested, theories are drawn from social psychology, organised crime and transaction cost economics (TCE). Since the focus is on how uncertainty is mitigated in trading among cybercriminals, uncertainty is treated as a cost to the transactions and is used as the unit of analysis to examine the mechanisms cybercriminals use to control two key sources of uncertainty: the quality of merchandise and the identity of the trader. The findings indicate that carding forums facilitate organised cybercrime because they offer a hybrid form of organisational structure that is able to address sources of uncertainty and minimise transaction costs to an extent that allows a competitive underground market to emerge. The findings from this study can be used to examine other online applications that could facilitate the online underground economy.

Keywords**:** organised cybercrime; carding; underground economy; trust; transaction cost economics; social network

Introduction

> Without a more comprehensive research study to determine who participates in crime on the Net—who provides demand and who supplies illicit services and products—we are not really in any position to speculate about typical NetOffenders
>
> (Mann and Sutton 1998: 223)

In one of the first studies of cybercrime that used newsgroups and forums as the data source, Mann and Sutton highlighted the paucity of research into this emerging problem (1998). It is a fascinating article to return to in 2013 because the questions raised are still challenging criminologists and law enforcement today. One of the most interesting aspects of this study is the speculation that hacking would move from the creative to the acquisitive; from hacking

for the challenge to a financial endeavour. They also speculate on the problems for law enforcement, unused to this new method of doing (criminal) business and learning the trade. They suggested that some parts of the internet were becoming similar to the old rookeries of London, lawless and unfamiliar to the police. This article draws on more recent forums for its data source and explores the way that such forums have evolved to facilitate trust and financial crime on a huge scale. Carding forums are now closer to the legitimate world of high finance, than the low life of Gin Lane.

According to the latest U.K. National Security Strategy (HM Government 2010), cybercrime has been assigned as a Tier-One threat to the United Kingdom, alongside international terrorism. Similar actions have also been taken in the U.S. [1] and Australia [2]. Recent cybersecurity statistics (PwC 2012; IC3 2012) conclude that cybercrime remains as the primary threat facing nations, corporations and people in 2013. In order to tackle cybercrime, it is vital for the policing community to understand the factors which has turned cybercrime into the persistent problem we are facing today. The purpose of this paper is to study the structure of carding forums on the web and to demonstrate how trust is an integral quality of them. Carding is the buying and selling of stolen credit card data (Peretti 2008). We do not ignore the role of the agent in the construction of cybercrime forums, but for the purposes of our argument here, we will focus on the theories and accounts that help explain how forums are structured to create trust among thieves, and what this implies for the policing of them (see also Webber and Yip 2013 for a discussion of the agent perspective on underground forums).

[1] http://money.cnn.com/2012/03/02/technology/fbi_cybersecurity/index.htm
[2] http://www.aic.gov.au/about_aic/research_programs/staff/~/media/staff_presentations/tomison_adam/2011-02-trends.pdf

Several recent cybercrime studies (Thomas and Martin 2006; Franklin et al 2007; Holt and Lampke 2010; Yip 2011; Yip, Shadbolt and Webber 2012) indicate that autonomous cybercriminals or "cyber-entrepreneurs" (Brenner 2002; Wall 2008) are collaborating and trading extensively over the Internet via different channels such as Internet Relay Chat (IRC)[3] or on discussion forums (Holt and Lampke 2010). Furthermore, the "underground economy" appears to be highly competitive (Thomas and Martin 2008) with vendors supplying goods and service such as stolen credit cards, hacking and money laundering services to meet the demand (Peretti 2008). In particular, the lure of a lucrative return from trading in this underground economy has led to a continuous influx of skilful individuals into the cybercrime ecosystem and thus giving rise to a comprehensive "division of labour" (Gambetta 2000; Moore et al 2009; Wall 2008) which continuously supplies the resources that facilitate the commission of cybercrime. However, with the uncertainties surrounding computer-mediated communications (Jarvenpa and Leidner 1999; Walther 1995; 1996) such as anonymity and the need to span time, culture and space, a key question is, how do cybercriminals sustain sufficient levels of trust for collaborations to thrive?

This problem was raised by Brenner (2002) who speculated on the organisational structure of online crime groups. Drawing from observations of physical crime groups such as the Mafia as well as trying to understand the functionalities facilitated by the Internet, Brenner concluded that online crime groups would almost certainly "emphasize lateral relationships, networks instead of hierarchies" (2002: 50). To what extent is this claim true? Is it still true? Will it hold true for the future? These are the questions this paper will try to address.

[3] The Internet Relay Chat (IRC) is a command-based communication tool that operates over the Internet. However, it uses the IRC protocol rather than the Web (HTTP).

As proposed in various organised crime literatures (Cohen 1977; Pearson and Hobbs 2003; Hobbs 2001; Morselli and Petit 2007; McIllwain 1999; Van Calster 2006; Levi 2008; von Lampe and Johansen 2003; 2004; Lo 2010), the studying of organised crime should treat the relationships or "criminally exploitable ties" as the unit of analysis. This view is adopted in this paper. More precisely, this study focuses on the quality of relationships between the collaborations which is reflected by the presence of trust. Since the existence of a collaborative tie requires the presence of trust (Coleman 1993; Gambetta 2000; Dasgupta 2000; Weerman 2003) and trust requires the mitigation of uncertainties, it can be seen that uncertainties are obstacles to collaborations. By applying transaction cost economics (Williamson 1979; 1991; 1993), uncertainty is treated in this paper as a *transaction cost* to a collaborative tie and it is assumed that cybercriminals have rational incentives for minimising this cost, an assumption that is implicit in many organised crime literatures regarding network structures (Williams 1998; Hobbs 2001; Pearson and Hobbs 2003; Morselli 2001; Morselli and Petit 2007; Kenny 2007; Lo 2010). Since previous studies demonstrate that the underground economy is thriving, this implies that cybercriminals have been able to minimise this cost sufficiently so that they are able to collaborate. The question here is how they have managed to do so. Therefore, in collaboration with the Serious Organised Crime Agency (SOCA), this study examines the ways in which trust is sustained in the underground economy and the implications this has on the structure of organised cybercrime, and in turn how it can be controlled (Williams 2007; Wall and Willams 2007). This is achieved through a qualitative analysis of the actual conversations between cybercriminals in online underground markets better known as "carding forums" (Holt and Lampke 2010; Peretti 2008; Glenny 2011; Poulsen 2011). These forums are the site of tutorials, similar to newsgroups studied by Mann and Sutton (1998); a business market that is enabled by methods of creating and

maintaining trust; and a site that is at once public and private. They are also increasingly surveilled by law enforcement, such as the FBI in America and the Serious Organised Crime Agency (SOCA) in the UK. They have since been analysed by the authors using a variety of methodological approaches from Social Network Analysis (Wasserman and Faust 1994), to case study research using the interpretive tradition of symbolic interactionism, discourse analysis and conversation analysis (Webber and Yip 2013; Yip, Shadbolt and Webber 2012). This has allowed us to forge a unique synthesis between social and computer science. There is insufficient space here to go into any detail, and the nature of the forums are such that their provenance is confidential[4].

Trust and Criminal Capital

In order to examine the implications that trust has on organised cybercrime, it is important to first understand what trust is. A comprehensive definition of trust is given by Gambetta (2000) and forms the working definition from which we will work, albeit with awareness of the problems of assigning too rational an outlook on anyone, not least those engaging in carding related crimes:

> [T]rust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both *before* he can monitor such action (or independently of his capacity ever to be able to monitor it) *and* in a context in which it affects *his* own action
>
> (2000:217: *emphasis in original*)

In other words, trust is a mechanism for people to "cope with risk and uncertainty in interactions with others" (von Lampe and Johansen 2003: 103). Considering trust as a "property of collective units" such as ongoing relationships, groups and collectives (Lewis

[4] We have, however, been granted ethical approval for the use of these forums by our University Ethics Committee.

and Weigert 1985: 968), if person A trusts person B then person A *relies* on B's "integrity in the *absence of sufficient means to control* this other person's behaviour" (von Lampe and Johansen 2003: 103). Therefore, trust presupposes a situation of risk and that the risk can be avoided at the expense of the associated advantages (Luhmann 2000: 96).Those who decide to trust have *purposefully and voluntarily chosen* to accept the risk in the hope of favourable returns concerning their own actions under uncertain circumstances (McCarthy et al 1998: 156). Trust then, is a product of *rational expectation* of the other to behave in a certain way in circumstances that are not formally controlled and without any "moral residue" (Dasgupta 2000: 52; Hardin 1996: 28). However, due to the "limits of our capacity to achieve full knowledge of others, their motives and their responses to endogenous as well as exogenous changes" trust is also a "fragile response to our ignorance" (Gambetta 2000: 218). The rationale in trust is bounded by our capacity to anticipate the future behaviour of others. It is this *bounded rationality* which necessitates us to trust in the first place. Therefore, to trust someone, one has to "interpret" the context to which the trust relates in order to find good reasons to trust. When one's interpretations become acceptable, the awareness of the "unknown, unknowable and unresolved is suspended" (Möllering 2001: 412-414). Through this combination of interpretation and suspension, one can then make the ultimate leap of faith that is required in most trust relationships.

Nevertheless, with so many unfavourable conditions surrounding co-offending, it leaves one to wonder why co-offending is such a common phenomenon (Weerman 2003). Thus, a natural question is: what makes one willing to co-offend? Furthermore, what makes someone attractive as a co-offender? In order to answer these questions, it is important to understand why it is necessary for people to collaborate in the first place. The main reason for

collaboration is due to the need for social capital (Bourdieu 1986; Coleman 1988). As Burt (2000: 347) explains, social capital is "the contextual complement to human capital" and "inheres in the structure of relations between actors and among actors" (Coleman 1988: 98). In other words, social capital refers to the advantages that arise from connections with others. There are many kinds of social capital including obligations, expectations and trustworthiness, social norms and access to resources such as skills and information (Bourdieu 1986; Coleman 1988; Portes 1998; McCarthy et al 1998; Uzzi 1997; Granovetter 1973 and 1985). In crime, this is the "criminal capital" that facilitates the commission of crimes (McCarthy and Hagan 1995; 2001)

Ultimately, one is only willing to bear the risks and co-offend because it is *profitable* to do so (Weerman 2003: 404). Following this proposition then, it is evident that one is an attractive co-offender if one has "something to offer", such as information, specialised skills or other scarce resources (McCarthy and Hagan 2001). However, since trust is a functional prerequisite to social relationships then an attractive co-offender also has to be sufficiently trustworthy for others to take the risk and trust they will not mess up their part in a deal (Lewis and Weigert 1985; Gambetta 2000). This raises another question: how can one determine who is trustworthy? As explained by Dasgupta (2000), trustworthiness not only depends on the history of the people since there is a boundary on how much we know, but also their incentives to pursue their self-interest and cheat in the current context. In other words, to be trustworthy requires one to convince others that they would not be opportunistic (Williamson 1993: 458). Therefore, the control of opportunistic incentives is critical to the promotion of trust and hence, collaboration (Powell 1990; Williamson 1993; Jones et al 1997). There are two main forms of controls: institutional means and social norms (Coleman

1988; Hardin 1996). Regardless of the form of control, the ultimate goal is to ensure that dishonest behaviours are appropriately punished and that the "enforcement agency" itself is credible and trustworthy (Dasgupta 2000: 49).

However, there are occasions where collaboration between criminals could occur in the absence of trust. In such cases, collaboration would only occur if possibility of betrayal is minimised using procedural arrangements such as testing and counting merchandise as well as anonymity and segmentation (von Lampe and Johansen 2003; 2004). Furthermore, violence is used to ensure contract compliance and criminals emerge as "entrepreneurs of trust via the threat and utility of violence" (Pearson and Hobbs 2003: 341). But, here the Internet presents another interesting deviation from traditional 'off-line' criminal collaboration. The use of violence as a safeguard for trust is not as easily available for collaborations over the Internet since virtual communication is often anonymous and spans across time, space and culture (Walther 1996; Jarvenpaa and Leidner 1999; Grabowski and Roberts 1999; Sandywell 2010). Furthermore, since trusting someone requires one to form an opinion and stereotype using the social information gathered on the person (Dasgupta 2000; Luhmann 2000; Tajfel 1982), trust over the Internet is even more difficult to achieve because the transfer of social information over computer-mediated communication (CMC) is reduced due to a lack of nonverbal and social context cues (Walther 1995; 1996). In other words, trust building over CMC requires more time investment than in Face to Face relationships.

.

As already mentioned, recent studies (Thomas and Martin 2006; Franklin et al 2007; Holt and Lampke 2010; Yip 2011) indicate that cybercriminals are extensively trading over the Internet with market-driven dynamics (Powell 1990). In essence, these "cyber-entrepreneurs" (Brenner 2002) are similar to the "free-trading entrepreneurs" engaged in drug dealing

(Pearson and Hobbs 2003; Morselli 2001). Further similarities can be found in the ways they interact as both studies report that the structure of the organised crime studied is not of a hierarchical orientation but rather, "flexible networks and partnerships" (Pearson and Hobbs 2003: 344) between individual entrepreneurs who seek to "exploit specific types of entrepreneurial activities" (Brenner 2002: 45). Therefore, the exchanges between cybercriminals, at least in the underground economy, do not place emphasis on thick trust (Khodyakov 2007) or bonding capital (Lo 2010), that is, the strong interpersonal relationships such as families and close friends[5]. Rather, their relationships are built on thin trust (Khodyakov 2007) and these weak ties (Granovetter 1973) provide unique access to resources and opportunities outside of their immediate social circles (Burt 2000; Hobbs 2001; Pearson and Hobbs 2003; Lo 2010; Granovetter 1973; Uzzi 1997). Therefore, for cybercriminals to develop weak ties in the underground economy, they must be able to overcome the obstacles imposed by CMC on the transmission of social information that is necessary for them to develop thin trust. In other words, cybercriminals require mechanisms that facilitate the development of *initial trust* (McKnight et al 1998). The focus of this paper is on one such mechanism: carding forums (Glenny 2011; Poulsen 2011). In order to understand the reasons why carding forums facilitate trust and thus collaboration between cybercriminals, this paper takes a unique approach by treating uncertainty, the main obstacle as well as the prerequisite to trust, as a transaction cost.

Transaction Cost Economics (TCE) and Social Structures

Since the aim of this paper is to address the structure of organised crime, the focus lies on the exchanges between the cyber-entrepreneurs (Brenner 2002; Morselli 2001; Hobbs 2003; Lo

[5] Although, see The Authors 2012 for a discussion of the need to be aware of the way that cybercrime can drift on and off line.

2010). Transaction cost economics (TCE) is therefore a suitable framework for this study because it focuses on the structure of governance by examining the transactions between parties (Williamson 1979). There are three behavioural assumptions in TCE (Williamson 1979; 1991; 1993): bounded rationality, opportunism and risk neutrality. While the first two are aligned with the conditions of trust, the latter refers to the assumption that individuals are neither risk-averse nor risk-seeking. This assumption on risk neutrality is later addressed by Chiles and McMackin (1996) who argue that risk and trust have important implications for governance structure. So for the purposes of this paper, we regard this element as saying more about the creation of forums as a governance structure than an assumption that can apply to active agents.

Based on these three assumptions, the principle argument behind transaction cost economics is that firms (can be an individual, group or corporation) have the incentive for *economising transaction costs*. There are three fundamental elements in transaction costs (Williamson (1979; 1991) frequency of transactions, asset specificity and uncertainty. The frequency of transactions refers to the likelihood of the transactions to recur over time. Asset specificity refers to the amount of assets required for a particular transaction which would otherwise have little to no value in other contexts. Both frequency and asset specificity influence the potential costs of mistrust due to uncertainty, thus driving a need for the trading parties to "devise a machinery" to "work things out" (Williamson 1979: 254). According to transaction cost economics (TCE), the incentive for minimising transaction costs influences the structure an organisation is likely to adopt (Williamson 1979; 1991; 1993; Thorelli 1986; Powell 1990). There are many types of economic institutions but they all fall in between the two extreme types of structures: markets and hierarchies. The dynamics of a typical market is summarised by Powell (1990):

> Markets, as described by economic theory, are a spontaneous coordination mechanism that imparts rationality and consistency to the self-interested actions of individuals and firms…The market is open to all comers, but while it brings people together, it does not establish strong bonds of altruistic attachments. The participants in a market transaction are free of any future commitments. The stereotypical competitive market is the paradigm of individually self-interested, noncooperative, unconstrained social interaction.
>
> (1990: 302)

On the other hand, in a hierarchical structure, there are

> clear departmental boundaries, clean lines of authority, detailed reporting mechanisms, and formal decision making procedures…The strength of hierarchical organization, then is its reliability – its capacity for producing large numbers of goods and services of a given quality repeatedly – and its accountability – its ability to document how resources are being used
>
> (1990: 303)

In the absence of transaction costs, market structure is desired because it offers choice, flexibility and opportunity (Powell 1990: 302). Firms in a market are more likely to enjoy benefits from economies of scale (Brynjolfsson et al. 1988). However, the need for minimising transaction costs leads to the need for coordination. Therefore, a more elaborate governance structure such as a hierarchical structure is justified when it can offer considerable reduction in coordination costs which would otherwise be present in market-oriented structures (Williamson 1979; Thorelli 1986; Powell 1990). This market-hierarchy argument will be used to demonstrate why carding forums are so well-suited for facilitating organised cybercrime. However, this should not be taken to mean that we afford all humans with pure rationality, it is bounded by context, messy and complicated (Giddens 1984; Granovetter 1985). However, the structure of the forum and the methods of minimising transaction costs no doubt enable crime where trust is an essential requirement and networking facilitates business relationships.

Uncertainties in the Underground Economy

Carding involves a wide array of facilitating cybercrimes including those belonging to the category of "computer-assisted crimes" such as virtual robberies and thefts as well as "computer integrity crimes" such as hacking and cracking (Peretti 2008; Wall 2008). It is argued in this paper that there are two main sources of uncertainty carders face when trading in the underground economy:

- **Quality** of the goods and services.
- **Identity** of the trading partner, that is, whether the person is a true cybercriminal, an dishonest trader (a "ripper") or a law enforcement associate.

Quality Uncertainty

As observed by Thomas and Martin (2006) as well as Franklin et al (2007), carding has been active on the Internet Relay Chat (IRC). However, both studies have reported the prevalence of dishonest traders, known as "rippers". Herley and Florêncio (2010) argue that the impact of the 'rippers' on the underground economy can in fact be highly significant. They question why someone would sell bank accounts worth more than $2000 for only $0.50. Using the economic theory of asymmetric information better known as the "market for lemons" theory (Akerlof 1970), they argue that the majority of the goods and services traded over openly accessible channels such as the IRC are in fact "lemons" that are worth very little. The "market for lemons" theory addresses the problem of uncertainty in markets (Akerlof 1970). The theory Akerlof proposed is that uncertainty in the market arose because the sellers have more information about the true quality and value of the goods than the buyers. Hence, information is asymmetrical. Since buyers have incomplete information about the goods, they are unwilling to pay the price the sellers ask and so no quality goods are sold. Herley and

Florêncio (2010) argue that a lemon market will be produced if the following conditions are met:

- An incentive exists for the seller to pass off a low quality product as a higher quality one.
- Either there exist a continuum of seller qualities or the average seller type is sufficiently low.
- Asymmetry of Information.
- Sellers have no ways for credibly disclosing the quality of their goods.
- Lack of Quality Assurance or Regulation.

So, how is the stolen data market a lemon market? From the definition offered by Powell (1990: 302), a competitive market is made up of "individually self-interested, noncooperative, unconstrained social interaction". Therefore, it can be assumed that in a stolen data market, there exists an incentive for the sellers to pass off a low quality product as a higher quality one. Furthermore, from previous studies on stolen data markets (Thomas and Martin 2006; Franklin et al 2007), there certainly exists either a continuum of seller qualities or the average seller type is low. Lastly, as observed by Thomas and Martin (2006), even administrators in the IRC channel can be cheats. Therefore, there is also a lack of trustworthy regulatory system for trading over the IRC. In essence, the underground economy as that observed on the IRC do exhibit all the characteristics associated with that of a market for "lemons".

Identity Uncertainty

However, there is one more source of uncertainty in the underground economy that is potentially more costly than quality uncertainty: the true identity of a trader. Aside from dishonest traders, the cybercriminals also face the additional threat from law enforcement

associates such as undercover agents and informants pretending to be cybercriminals. However, it appears that the cybercriminals are well aware of this threat:

> *This[6] may be obvious to most people on this site, but I want to say it out loud for those who dont get it.*
> *We ARE visited by Governmental Agencies. Thats a fact. And without a doubt these Governmental Agencies are looking very close at certain members and maybe at this site as a whole.*
> *PLEASE keep that in mind when posting specifics about business, or giving away your drop addys[7] to others, etc., etc. Try to deal with people that you know for a fact you can trust.*
> *Also, bear in mind that at some point one of these governmental agencies might get it in their thick piggy heads to set up some type of Sting Op. So again--be careful of who you deal with.*

By using transaction cost economics (TCE), the above demonstrates that the cost of uncertainty can be too high for conducting serious business in scale (Williamson 1979; 1991; Chiles and McMackin 1996) over the openly accessible channels such as the IRC. Therefore, according to Akerlof's theory, such markets would fail, or at the very least, unable to scale. As Herley and Florêncio (2010) argue, the more serious underground businesses occur within closed organisations. The question here is why? What makes underground markets successful in closed organisations such as the carding forums discussed below, but not over the IRC?

Carding Forums as Domesticated Markets

Dimitry Golubov, a.k.a. *Script*, launched one of the first carding forums called Carderplanet in 2001 (Glenny 2011: 48). Carderplanet was designed to be the place where data thieves from all over the world could trade stolen data and related goods and services. However, with

[6] Where quotations from forums are used we present them as they appear, spelling and grammar mistakes included.
[7] This refers to the address of a drop location.

the Internet booming, it is not surprising to find that Carderplanet was not alone. Andrew Mantovani, a 20 year-old part time business student in Arizona was also a member of a cybergang but one that mainly stored stolen data (Grow and Bush 2005). He realised that there was a need for a place to trade stolen data online and after meeting David Appleyard, a mortgage broker in his 40s, they founded ShadowCrew in 2002. A snapshot of ShadowCrew is shown in figure 1.

ShadowCrew was officially shut down by law enforcements as part of Operation Firewall in 2004 (U.S. District Court 2004). According to the U.S. Department of Justice, members of ShadowCrew trafficked at least 1.7 million credit card numbers and caused total losses of at least $4 million[8]. The same operation also led to the demise of Carderplanet.

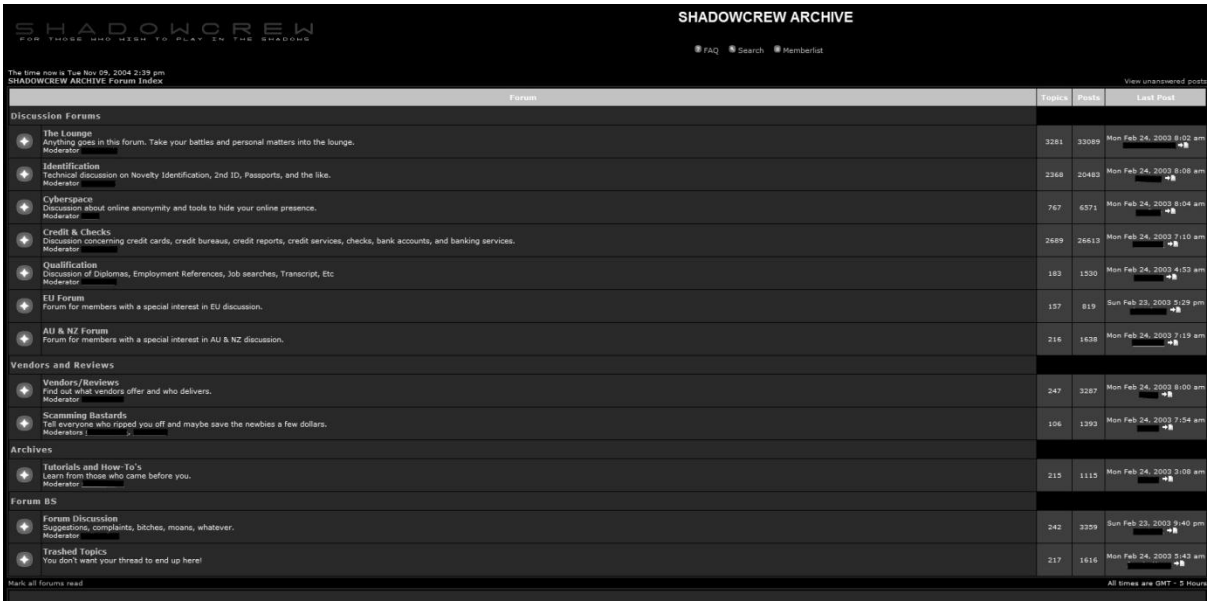

Figure 1: Snapshot of ShadowCrew.

In order to fill the void left by Carderplanet and ShadowCrew, two carding forums emerged in 2005-2006: CardersMarket and Darkmarket (Glenny 2011; Poulsen 2011). Cardersmarket was founded by a security expert turned carder called Max Butler (aka Iceman). At the same

[8] http://www.justice.gov/opa/pr/2004/October/04_crm_726.htm

time, Renukanth Subramaniam[9], a.k.a. *JiLsi*, launched Darkmarket and both forums were engaged in a bitter board war[10] (Glenny 2011; Poulsen 2011). This board war shows that carding forums are popular and valuable venues for cybercrime. The question is what do they offer that make them such popular venues? The following part of this paper looks to carding forums as the source of a unique data set. A forum stores the entire public facing discussions engaged in by carders. Once taken down by law enforcement, they are rarely available again to the public. Studying these forums has allowed us to understand the human foibles that pure quantitative network analysis cannot achieve (Webber and Yip 2013; Yip, Shadbolt and Webber 2012). What we demonstrate, therefore, is a form of analysis that places as much emphasis on the individuals as it does on the social network (Yip et al 2012). By doing so, we can see the way that rationality is indeed bounded by contradictions and complexities, but that the function of the forum remains conducive to the commission of credit card fraud on a massive scale.

Inside a Carding Forum

Much like conventional online discussion forums, carding forums are used mainly for trading carding goods and services. However, as shown in figure 2, each forum is typically divided into a series of sub-forums each dedicated to a particular type of content such as trading, tutorials, discussions and a blacklist of dishonest traders (the "rippers"). Users can start topics, also known as threads, which others can reply to. The forums also offer private messaging functionality which is often used by carders to carry out more detailed negotiations. Members are free to network with one another to engage in discussions and trading. A typical advert from a vendor is as shown in figure 3. Interested parties could either contact the vendor via private messaging on the forum or other means of contacts such as email or ICQ.

[9] http://www.guardian.co.uk/technology/2010/jan/14/darkmarket-online-fraud-trial-wembley

[10] http://www.wired.com/techbiz/people/magazine/17-01/ff_max_butler?currentPage=1

However, these functionalities are common features amongst many online discussion forums so how do they facilitate the reduction of uncertainty in the underground economy?

Figure 2: Sub forums on ShadowCrew.

Mechanisms for Uncertainty Mitigation

As already discussed, this paper argues that there are two major sources of uncertainty and hence transaction cost in the underground economy:

- **Quality** of the goods and services.
- **Identity** of the trading partner, that is, whether the person is a true cybercriminal, an dishonest trader (a "ripper") or a law enforcement associate.

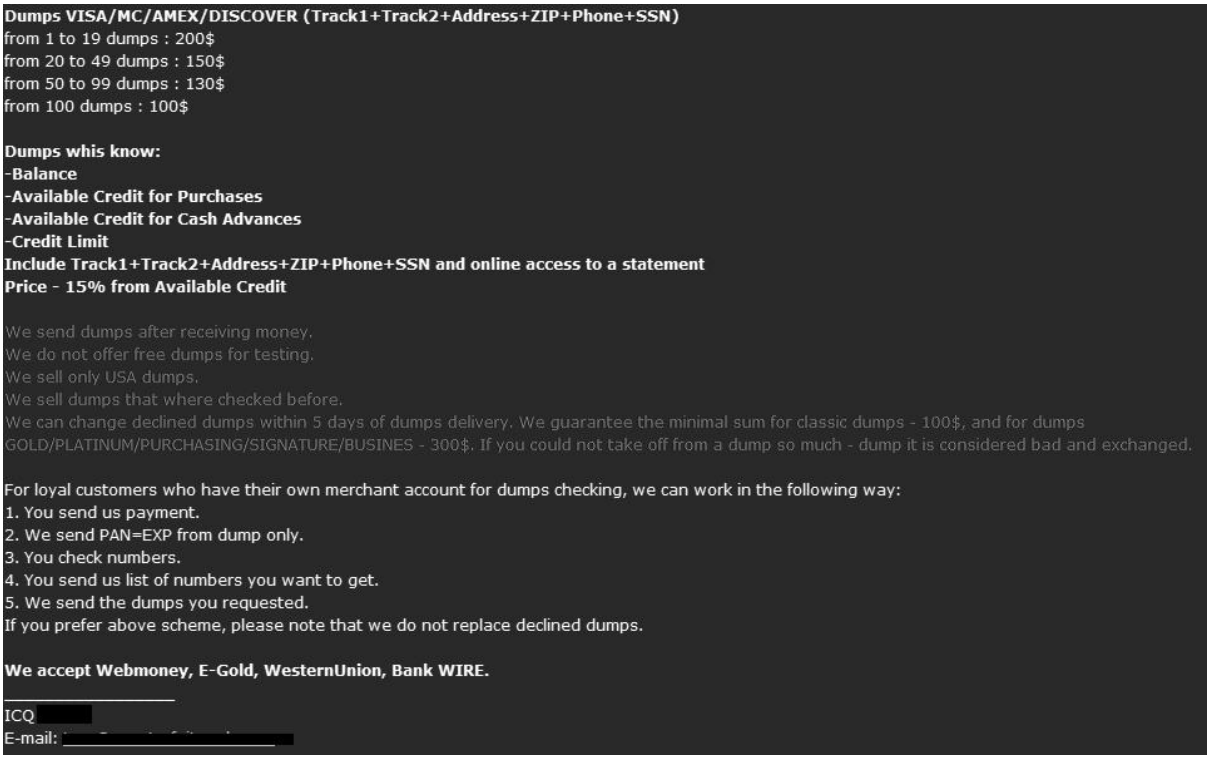

Figure 3: A typical advert for stolen credit card data.

The cost mitigating mechanisms offered by a carding forum are shown in figure 4. By using carding forums, uncertainties surrounding the quality of traded commodities are mitigated through two mechanisms: a sophisticated review system and an exchange service known as the escrow service, commonly used in legitimate forms of transaction (Glenny 2011). Uncertainties around the identity of the traders are mitigated by allowing the cybercriminals to engage in social interactions in open discussions and knowledge exchange. Lastly, both of

these mechanisms are enforced through a well-defined management hierarchy. Each of these components is discussed in the following sections.

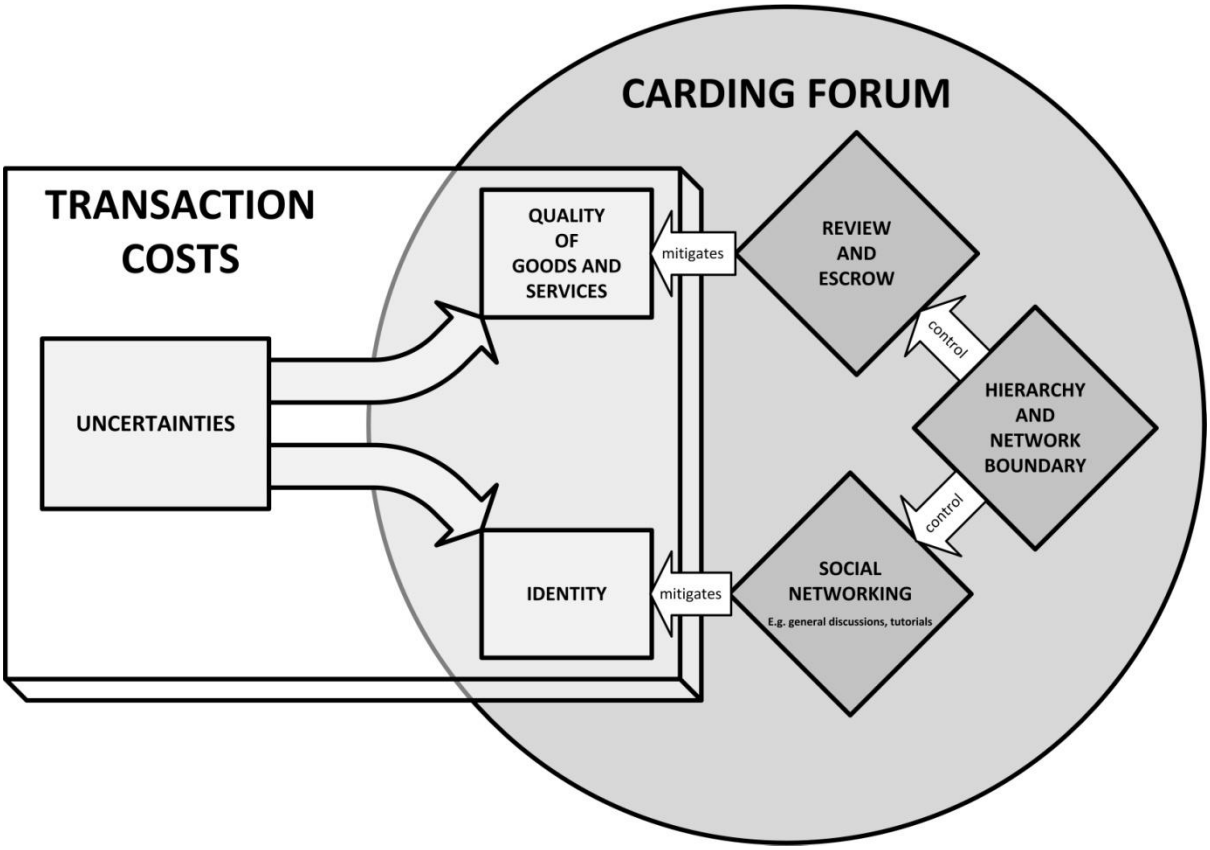

Figure 4: Transaction cost mitigation by carding forums.

Quality Assurance: Review and Escrow

Reputation is the primary tool for trust preservation in the underground economy and reputation is attached to the nickname of a user. Therefore, the nicknames are treated like brands (Lusthaus 2012). However, it is important to realise why reputation is needed in the first place. It is needed because many who want to collaborate have no prior knowledge or experience with each other. Accumulating a reputation by behaving well over time is difficult and requires too much time because many cybercriminals refuse to deal with those without a reputation in the first place. In other words, for cybercriminals to collaborate with one another, they must be able to trust each other without requiring previous experience.

Therefore, there must be a mechanism capable of minimising the risk of opportunistic intents and facilitates the development of initial trust (Williamson 1993; McKnight et al 1998).
To solve this problem, the cybercriminals have developed two reputation-based systems:

- Reviewed Vendor
- Escrow service

In order to finally mitigate the problem of developing initial trust with potential buyers, the fastest route for a vendor is by obtaining the status "Reviewed Vendor". This is achieved by having their goods and services reviewed by a trustworthy individual, most often, the senior members of a carding forum who are personally appointed by the administrators (more on this in the next section).
Below is a typical review of a vendor:

> *Hacker451*[11] *has already been reviewed for his ability to pul credit reports at will and in a variety of different way.*
>
> *Last week Neo contacted me and asked if I could review his CC Dumps.* [12] *I agreed. Below is the review--I think most will be VERY happy with Hacker451.*
>
> *Hacker451 Provided a number of VISA Gold, Platinum, Corporate, and regular Dumps for review.*
>
> *In doing this review it was determined that the most strenuous test that one could do would be a CASH ADVANCE in a Hostile Enviroment. A LOT of folks may think that this was an unfair test, since most the other Dump suppliers on this board have certainly NOT undergone so dramatic a test. In truth, it was unfair, but there was a need for a dump supplier which could provide dumps that yeilded a sufficient profitable margin.*

[11] Pseudonyms created by the authors are used throughout when using extracts from the forums.
[12] Credit Card Dumps, the collection of data needed to produce a fake credit card or buy goods remotely over the Internet, for example. Often a dump can contain hundreds of credit card details (See Peretti 2008).

That being said--we put Hacker451's cards to the test. Amounts were requested at a minimum of $1K to a max of...Well, it was a decent amount .

The results were very Good and cash was delivered without question. The results were so good, that additional CASH Advance testing WILL be done. There were Declines, BUT it seems lower than the 20% decline range quoted by other sellers. And these are certainly better performing dumps than I have seen with other vendors recently.

VERY IMPRESSED with Hacker451 and his Dumps. From what I have seen and heard thus far—Hacker451 is THE man to see about dumps.
Hacker451IS A VERIFIED AND REVIEWED SELLER OF CC DUMPS (TRACKS).

Those looking to purchase merchandise would then look to buy from vendors who hold the "Reviewed Vendor" status and if the service is good then they would remember the nickname and collaboration could recur. Therefore, gaining the status of a Reviewed Vendor can be seen as a long term solution for those looking to remain in the business beyond the transaction (von Lampe 2004).

However, this could be too much trouble for those looking to make transactions only on occasions. This is where an alternative mechanism comes into play: escrow service.

> A vendor would provide the escrow officer with a sample of his wares (a dozen or so credit card numbers and PINSs) while the potential buyer would send the money to him at the same time. The escrow officer would then test the wares and, if they delivered the cash as promised, he would release the money to the vendor and the dumps and PINS to the buyer.
>
> (Glenny 2011: 55)

Below is an extract from a carding forum asking for an escrow service:

Trickster: Do you plan to make an escrow service?
It must be some respected and trustworthy
member of our community.

Cardpro: Of course, we have Reviewed Vendors,
but sometimes there are such deals that
need escrow as a guarantee.

It is clear from this extract that not everyone can be an escrow officer. In order to be one, one must be a trusted member and more importantly, they must be trusted by both the vendor and the buyer. Furthermore, the extract also shows that the trust signals from a Reviewed Vendor may not be enough for certain types of transactions. This further highlights the importance of trust in cybercriminal trading. From our observations, an escrow officer usually charges a 5-10% commission for the service.

In essence, both systems facilitate the development of a type of trust called institution-based trust (McKnight et al 1998: 475) where "one believes the necessary impersonal structures are in place to enable one to act in anticipation of a successful future endeavour". Furthermore, McKnight et al (1998) argue that institution-based trust promotes the growth of initial trust because firstly, it provides an ordered predictable setting (situational normality) and as discussed in a previous section, a predictable context is vital to the development of trust (Gambetta 2000; Dasgupta 2000). Secondly, both systems provide "structural assurance" where risks are mitigated due to some form of guarantee.

Identity Assurance: Social Networking

Aside from uncertainties over the quality of the goods and services offered, the cybercriminals are also uncertain about the true identity of their trading partner. That is, they have trouble identifying whether their trading partner is a fellow cybercriminal, a ripper or a law enforcement associate pretending to be a cybercriminal.

As already introduced, carding forums commonly have dedicated sections for general discussions and tutorials. These sections facilitate the social networking between the cybercriminals and this facilitates the trust mechanisms already introduced.

In essence, the primary resource these sub-forums facilitate is the transfer of information which can be specialised knowledge (such as technical tutorials) or general information about related goods and services as well as potential threats. Below is an extract from a forum thread warning others of potential threat from a law enforcement agency:

> *I have been told to post this by a friend of mine Hax0r who I have trusted for years and also has done business with vendors on this forum now and back in the ** days. He was made an offer by law enforcement to help out in a sting operation on this forum. This offer was made IN PERSON at his work. Not that it couldn't be faked but he said they were the "real deal" and had identification and everything.*
> *I am posting this for him as he asked me to do so to remain anonymous. I would not recommend any new formed relations or not pursue any team work that was recently planned out if you have any chance of getting screwed because of this garbage. He did not help these guys, nor does he plan on it... but I am sure if they pin point the right people, they will do whatever law enforcement tells them to.*
> *SO BE CAREFUL.*

By offering a space for cybercriminals to engage in reciprocal and mutually beneficial acts such as the exchange of valuable information, these are the symbolic interactions through which in-group identity and group classification can be developed (Fehr et al 2002; Tajfel 1982; Ashforth and Mael 1989). This allows the members to develop an understanding of the prototypical characteristics of the group and this implicitly gives them the ability to identify those who do not belong to the group. In other words, social networking facilitates the emergence of informal social control in the underground economy (Williams 2007; Wall and Williams 2007).

This is demonstrated by an extract from a forum thread where members of the carding forum engage in a topic that touches on regret, risk and the difference between a ‘normal’ life and that of a carder:

> *Looper123: People who's life is carding and other type of frauds (so no fucking students who do this part-time) :*
> *Do you sometimes wish you just had a normal life, with this I mean normal job, no stress about ops, making money, Law Enforcement etc?*
> *or are you 100% happy with ur 'underground ops life' ?*
> *I would appreciate any input/thoughts*
> ---
> *Dumpster: I wish I had a normal life. Turn back the clock and all, but fuck it I am where I am.*
> ---
> *CardPhreak: Are you kidding me!!! Normal life with no stress.*
> *No such thing, there will always be stress unless you live in fantasy land.*
> *There may be different types of stress but it will always be there.*
> *As for regret. I regret being too honest and living the so called normal for far too long before I found out how much money could be made in this business.*
> ---
> *Looper123: there is a HUGE difference between 'normal life stress' and this business's stress.. I think you just started out in this business.. i wanna hear ur thoughts after 5 months*
> ---
> *CardPhreak: It is like any other business, what makes it different is the Law Enforcement, so I would not say "fuck 'em" The thing is there is not much to regret until you get busted. The hard question is would you regret what you had done after that?*
> ---
> *Dumpster: Some parts of it I love. I'm a total loaner outsider, some by choice and some by the fact I've never been the type of guys that gets the girls or anything. Doing what I'm doing kind of makes me feel like I'm doing something...something a little risky...then when i do something, I still sometimes feel guilty about the people I'm doing it to. I hate that part of it. I'm never going to have a normal life even if I try, so this life, as ****** says, "For those who wish to play in the shadows" I love the shadows. I love doing things in the shadows. That's where I'm comfortable.*

The last post by *Dumpster* reminds us that understanding the structure of the forums must not be pursued at the expense of the agency of those involved, their human foibles. Our argument in this paper maybe about the structure of carding forums and how this facilitates trust to enable an illegal profit-making enterprise, but we are also aware of the actors' own conflicts (see Webber and Yip 2013 for a fuller account of this argument). Lastly, by giving the cybercriminals an open and asynchronous space to socialise, it gives rise to a historical account of behaviour which is archived and made navigable. In essence, the discussion sub-forum becomes a rich source of social information for the forum members to form an accurate opinion of others when they are making initial trust decisions (Dasgupta 2000) as well as facilitating the strengthening of existing trust relationships (McKnight et al 1998).

Control: Hierarchical Management and Network Boundary

Having a reliable reputation system alone is not enough for the market to develop and this is why the underground markets over the IRC will fail (Herley and Florêncio2010). Due to the ways in which online discussion forums are designed, carding forums have an inherently hierarchical management structure (U.S. District Court 2004; Paget 2008). Such a management hierarchy is shown in figure 5.

So, what are the benefits of this hierarchy? Firstly, the most obvious function of a management hierarchy is the centralisation of authority (Tsai 2002).

Here is an example regarding the banning of a suspicious user:

> *He is dropped from the vendor list. I can't ban him outright since I'm not an admin, but that wouldn't do any good anyways. You guys with information on him need to apply some pressure - maybe PM HashTag about this?*

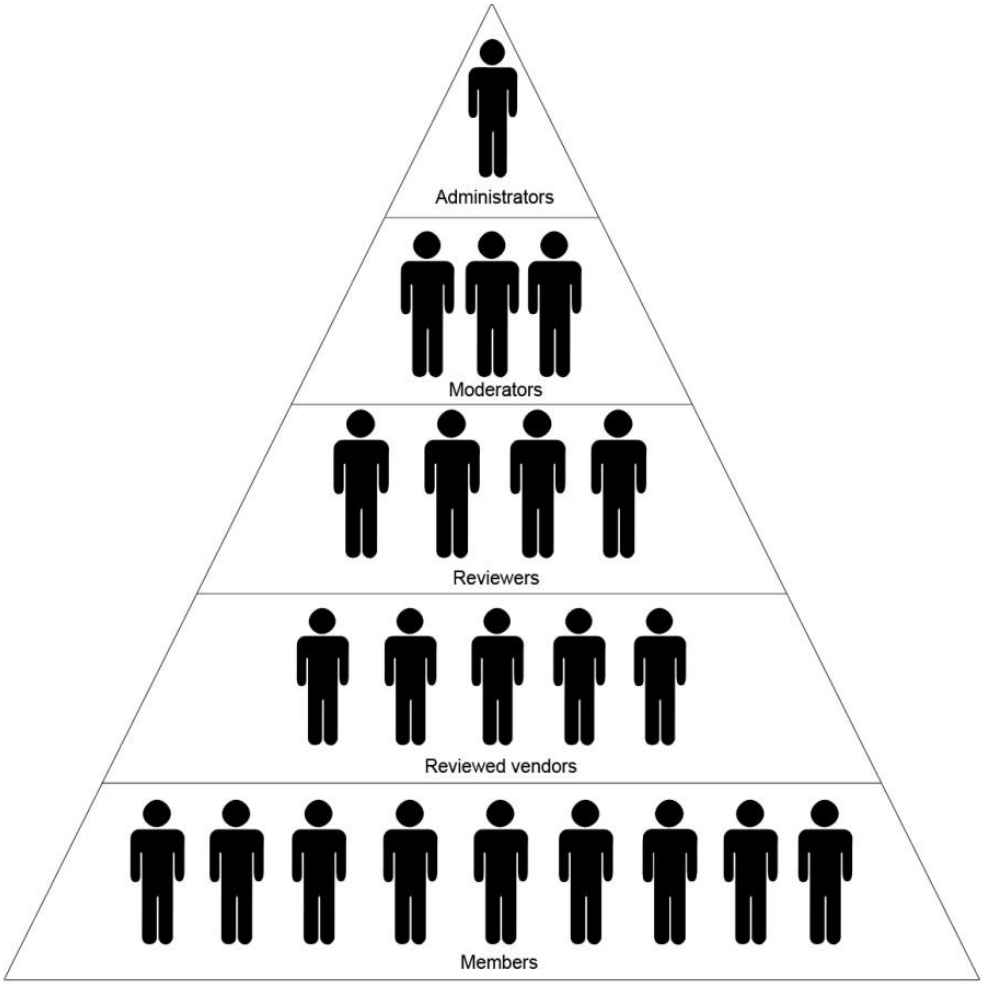

Figure 5: Typical management hierarchy on carding forums.

It is evident from this extract that the scope of privileges and functionalities of each role in the hierarchy are strictly adhered to. This is important as it allows critical decisions to propagate up the hierarchy, hence the centralisation of authority.

Secondly, this management hierarchy, as shown in figure 5, represents the clearest way of communicating trustworthiness based on commitment (Hardin 1996). Administrators are the owners of the forum (Glenny 2011; Poulsen 2011) and they are the ultimate decision makers of the forum. In terms of commitment, they are perceived as the most committed because they have committed resources such as money and time into operating the venue. Therefore, the trustworthiness of the administrators is more or less implicit from the forum members.

This has a domino effect on the establishment of initial trust in the market. From this single point, trust is propagated down the hierarchy as the occupiers of the roles below the administrators are either: (1) those trusted by the administrators personally or (2) trusted by the ones above in the chain of command (Glenny 2011; Poulsen 2011). In any case, trustworthiness is clearly communicated through this hierarchy and communication is fundamental to cooperation (Gambetta 2000):

Therefore, the management hierarchy of carding forums are instrumental in two ways: firstly, it gives a clear line of authority for centralised coordination and thus significantly reducing coordination costs which would otherwise exist in pure market environment such as those over the IRC (Williamson 1979; Powell 1990; Brynjolfsson et al 1988). Secondly, it facilitates the clear communication of trust among cybercriminals and allows trust to be reliably propagated through the social network.

However, even with a sophisticated trust mechanism including a hierarchy, it is useless unless it is properly enforced (Dasgupta 2000). That is, those who break the rules should be punished accordingly and banned users should be kept permanently away. Fortunately for the cybercriminals, another useful functionality facilitated by a forum is that it provides a network boundary through membership control. In effect, a forum segregates its members from other Internet users, giving the administrators full control on who should and should not be a member of the forum. Furthermore, membership facilitates accountability in any wrongdoing.

However, one of the most challenging problems for carding forum administrators is how an unwanted visitor such as an exposed “ripper” could be kept permanently away from the market? Afterall, the user could simply return and register under a different “nic” (Herley and Florêncio 2010; F.B.I. 2012). With the anonymity offered by the Internet, how can

administrators tell whether two users belong to the same person? As it turns out, this is one of the most difficult challenges for carding forum administrators. On the one hand, the only way in which they could keep exposed rippers from returning to the forum is by removing the ability to register altogether or at least for a long enough period to keep away the rippers who are less determined. On the other hand, they are faced with the demand for new members as they are the ones who provide new demands and supplies, ideas and opportunities to the market. This struggle is made explicit by the following extract from a forum post regarding the closing of registration:

ForumAdministrator: i hope to close it for ever so the rippers will not be able to register again and make more scammes

WiFiHiFi: And we would have no more new vendors, no more new intelligent members with new ideas, etc.

Colossus: Is membership registration closed?

ForumAdministrator: It is temporary closed due to release of popular Russian magazine called "Hacker". It was a special release only about carding. This magazine is being released by lamers and read by lamers and working not as informative tool but as a tool of attracting unnecessary attention of people who want "Everything and Now" without doing anything. We already encounter a huge flow of teenagers posting dumb questions, in wrong parts of forum, etc.

WiFiHiFi: And we would have no more new vendors, no more new intelligent members with new ideas, etc.

*ForumAdministrator:For those who have an expirience, knowledge, good attitude and behavior still may and do e-mail me for registering a new account at DarkCreditCarding forums. My e-mail for new registration is ******@******.net*
Our priority is to make forums clean and neat - better less and good rather than a lot and bad.

There are two common strategies used by administrators to deter unwanted guests from joining the forum: impose a cost to membership (F.B.I. 2012) or disabling registration altogether. On this occasion, the administrator chose to make it more difficult to register rather than removing registration altogether. This shows that new members are vital for the underground economy.

Implications for Cybercrime Policing

In summary, this paper has revealed why carding forums are repeatedly chosen by cybercriminals to operate online underground markets despite numerous previous takedowns by law enforcement (Glenny 2011; Poulsen 2011). There are several important implications for the law enforcement community.

Firstly, this paper has revealed that trust is vital in collaboration between cybercriminals and so, merely being in contact with other cybercriminals, such as that on the IRC, is not sufficient for serious trading to occur in scale (Herley and Florêncio 2010). In essence, the market will fail in the absence of trust as transaction costs are too high. Therefore, it is vital for the law enforcement community to prevent cybercriminals from developing trust and particular attention should be placed on preventing cybercriminals from forming initial trust in the first instance. This can be achieved in three ways: (1) a Sybil attack (Doucer 2002) whereby law enforcement increase the number of rippers or undercover agents in the underground economy in order to erode trust among cybercriminals. For future work, we aim to evaluate the effectiveness of this technique through the use of simulation and agent-based modelling (Carley et al 2002; Carley 2006); (2) increase the cost of misplaced trust such as more severe sentencing; (3) since it is shown that forums are facilitators of trust development among cybercriminals, the taking down of carding forums should be made a priority. Furthermore, the model shown in fig. 4 can be used for horizon scanning by examining

whether a particular web application is likely to be used to facilitate online underground trading.

Secondly, it is evident that there is no guaranteed trust in the underground economy. Even with a system such as a carding forum that is capable of providing multiple channels for trust to develop, there is still room for mistrust. Although this mistrust may lie partly with the naivety or carelessness of some cybercriminals, perhaps because they have a higher propensity for risk-taking (McCarthy and Hagan 2001; Chiles and McMackin 1996), this demonstrates that trust remains the primary vulnerability in organised cybercrime.

Thirdly, regarding police infiltration operations on carding forums such as Darkmarket (Glenny 2011), the findings from this paper show that it is important for undercover agents to focus not just on obtaining formal positions in the hierarchy but also to focus on portraying themselves as a true cybercriminal by demonstrating prototypical characteristics of the group. Since contents on the forums are archived and made navigable, any anomalies in their behaviour are recorded and can be called upon when accusations are made against them. Some of the trust "signals" cybercriminals or hackers normally expect from their colleagues are introduced by Holt (2010) and Lusthaus (2012).

Fourthly, regarding the structure of cybercriminal groups, Brenner (2002) speculated that cybercriminals will engage in "lateral relationships", networks instead of hierarchies". However, although network is the ideal form of organization for the cybercriminals due to its inherent flexibility and adaptability (Powell 1990; Thorelli 1996), the prevalence of mistrust in the underground economy means that adopting a purely lateral network organisation structure is inappropriate due to the high transaction costs involved (Williamson 1979 and 1991; Powell 1990; Chiles and McMackin 1996). Therefore, contrary to Brenner's speculation, the hierarchical mode of organisation *did* make the transition into the cyber underworld.

However, the form of hierarchical organisation appearing in cybercrime, namely the carding forums, is different from that of traditional crime groups observed by Brenner (2002). In carding forums, the management hierarchy is there for administrative and regulatory purposes and not necessarily coordinating the allocation of resources and members of the forums are certainly not in the direct command of hierarchy. Members are autonomous individuals free to pursue their self-interest to a limited extent.

Furthermore, this paper has only demonstrated that a hybrid form of organisation structure facilitates the emergence of scalable trading among cybercriminals. Since there exists a wide variety of online crime groups as introduced by Lusthaus (2012), the hybrid structure revealed in this paper should not be treated as the definitive structure of organised cybercrime.

Therefore, this paper concurs with Brenner's speculation ten years ago that:

> … as opposed to the localized, rigid, and often provincial hierarchical organizations that have so far characterized criminal groups, regional, or even global, collations will develop. These collations will be composed of sole cybercrime entrepreneurs and members of diffuse, loosely-structured opportunity groups, criminal associative entities that come together to exploit specific types of entrepreneurial activities…
>
> This new model means there are no set, fixed, easily tracked criminal organizations. It also means online criminals can collaborate as necessary but run relatively little risk that their colleagues in crime will be able to inform on them to law enforcement because partners in crime will no longer know who their collaborators are or where they are located
>
> (2002: 45)

Hence, it is important to recognise that the disruption of a carding forum is merely the disruption of one of many online underground markets currently operating over the Internet and remnants from these forums are free to continue their criminal ventures over other channels such as the IRC, ICQ or email with trusted contacts developed from their time on the forum.

Conclusion

By using data from online underground markets (known as carding forums) previously in operation over the Internet, this paper has revealed the vital role trust plays in the collaborations between cybercriminals. Using a mixture of theories from organised crime and transaction cost economics (TCE), this paper revisits previous criminological work on the structure of organised cybercrime a decade ago by Mann and Sutton (1998) and Brenner (2002). Furthermore, this paper has revealed the main reason why cybercriminals have repeatedly chosen to use online forums to operate online underground markets is due to the hybrid organisation structure they offer. It is revealed in this paper that the inherent structure of online discussion forums facilitates a comprehensive trust mechanism that is able to maintain a sufficient level of trust among cybercriminals for a scalable competitive market to emerge. This ability to maintain trust helps the underground economy to grow, giving the cybercriminals the incentives to innovate. It is this innovative drive which has ultimately turned cybercrime into the persistent problem we are facing today. Therefore, although Brenner was correct in predicting the preference for lateral networks, we have revealed that due to the need to maintain trust, a hierarchical management structure is required to oversee the lateral network of cybercriminals if an underground market is to succeed and grow. As such, we argue that profit driven cybercriminals will continue to pursue a hybrid organisation structure in order to host domesticated markets. Since online discussion forums possess such inherent structural properties, we therefore propose that law enforcement agencies should treat forum take-downs as priorities as they are the primary facilitators for the development of trust among cybercriminals, thus pivotal to the growth of the underground economy.

References

Akerlof, G., (1970). 'The Market for "Lemons": Quality Uncertainty and the Market Mechanism'. *The Quarterly Journal of Economics*, 84 (3), 488–500.

Arndt, J., (1979). ‘Toward a Concept of Domesticated Markets’. *Journal of Marketing*, 43 (4), 69–75.

Ashforth, B. and Mael, F., (1989). ‘Social Identity Theory and the Organization’. *The Academy of Management Review*, 14 (1), 20–39.

Bourdieu, P., (1986). ‘The Forms of Capital’. *In*: J. Richardson, (ed.) *Handbook of Theory and Research for the Sociology of Education*. New York, 241–258.

Brenner, S., (2002). ‘Organized Cybercrime ? How Cyberspace May Affect the Structure of Criminal Relationships’. *North Carolina Journal of Law & Technology*, 41 (1984), 1–50.

Brynjolfsson, E., Malone, T., and Gurbaxani, V., (1988). ‘Markets, hierarchies and the impact of information technology’. *MIT Center for Coordination Science Technical Report 106* http://econpapers.repec.org/paper/mitsloanp/2229.htm

Burt, R.S., (2000). ‘The Network Structure of Social Capital’, in R. I. Sutton & B. M. Staw, (eds). *Research in Organizational Behavior*, 22 (May), pp.345–423.

Carley, K.M., Lee, J., and Krackhardt, D., (2002). ‘Destabilizing Networks’. *Connections*, 24 (3), 79–92.

Carley, K., (2006). ‘Destabilization of Covert Networks’. *Computational & Mathematical Organization Theory*, 12 (1), 51–66.

Chiles, T.H. and McMackin, J.F., (1996). ‘Integrating Variable Risk Preferences, Trust, and Transaction Cost Economics’. *The Academy of Management Review*, 21 (1), 73–99.

Coleman, J.S., (1988). ‘Social Capital in the Creation of Human Capital’. *American Journal of Sociology*, 94, 95–120.

Dasgupta, P., (2000). ‘Trust as a Commodity’. *in*: D. Gambetta, (ed.) *Trust: Making and Breaking Cooperative Relations*. Department of Sociology, University of Oxford, 49 – 72.

Douceur, J.R., (2002). ‘The Sybil Attack’. *in*: *Revised Papers from the First International Workshop on Peer-to-Peer Systems*. London, UK: Springer-Verlag, 251–260.

F.B.I., (2012). ‘Manhattan U.S. Attorney and FBI Assistant Director in Charge Announce 24 Arrests in Eight Countries as Part of International Cyber Crime Takedown’ [online]. Available from: http://www.fbi.gov/newyork/press-releases/2012/manhattan-u.s.-attorney-and-fbi-assistant-director-in-charge-announce-24-arrests-in-eight-countries-as-part-of-international-cyber-crime-takedown [Accessed 23 Jan 2013].

Fehr, E., Fischbacher, U., and Gächter, S., (2002). ‘Strong reciprocity, human cooperation, and the enforcement of social norms’. *Human Nature*, 13 (1), 1–25.

Franklin, J., Paxson, V., Perrig, A., and Savage, S., (2007). ‘An inquiry into the nature and causes of the wealth of internet miscreants’. *In*: *Proceedings of the 14th ACM*

conference on Computer and communications security. New York, NY, USA: ACM, 375–388.

Gambetta, D., (2000). 'Can We Trust Trust?' in D. Gambetta, (ed.) *Trust: Making and Breaking Cooperative Relations*. Department of Sociology, University of Oxford, 213 – 237.

Gambetta, D., (2008). 'Trust's Odd Ways'. in J. Elster, O. Gjelsvik, A. Hylland, and K. Moene, (eds.) *Understanding Choice, Explaining Behaviour: Essays in Honour of Ole-Jørgen Skog.* Oslo: Unipub Forlag/Oslo Academic Press, 81–100.

Giddens, A., (1984). *The Constitution of Society*. Cambridge: Polity.

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

Grabowski, M. and Roberts, K.H., (1999). 'Risk Mitigation in Virtual Organizations'. *Organization Science*, 10 (6), 704–721.

Granovetter, M., (1973). 'The Strength of Weak Ties'. *The American Journal of Sociology*, 78, 1360–1380.

Granovetter, M., (1985). 'Economic Action and Social Structure: The Problem of Embeddedness'. in *Readings in Economic Sociology*. Blackwell Publishers Ltd, 63–68.

Grow, B. and Bush, J., (2005). Hacker Hunters [online]. *Bloomberg BusinessWeek Magazine*. Available from: http://www.businessweek.com/stories/2005-05-29/hacker-hunters [Accessed23 Jan 2013].

Hardin, R., (1996). 'Trustworthiness'. *Ethics*, 107 (1), 26–42.

Herley, C. and Florêncio, D., (2010). 'Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground Economy'. *Economics of Information Security and Privacy*, 33–53.

HM Government, (2010). *The National Security Strategy.* London: Her Majesty's Stationary Office

Hobbs, D., (2001). 'THE FIRM: Organizational Logic and Criminal Culture on a Shifting Terrain'. *British Journal of Criminology*, 41, 549–560.

Holt, T.J., (2010). 'Examining the Role of Technology in the Formation of Deviant Subcultures' . *Social Science Computer Review* , 28 (4), 466–481.

Holt, T.J. and Lampke, E., (2010). 'Exploring stolen data markets online: products and market forces'. *Criminal Justice Studies*, 23 (1), 33–50.

IC3, 2012. IC3 2011 Internet Crime Report. Available at: http://www.ic3.gov/media/annualreport/2011_IC3Report.pdf (Accessed January 29th 2013)

Jarvenpaa, S.L. and Leidner, D.E., (1999). ‘Communication and Trust in Global Virtual Teams’. *Organization Science*, 10 (6), 791–815.

Jones, C., Hesterly, W.S., and Borgatti, S.P., (1997). ‘A General Theory of Network Governance: Exchange Conditions and Social Mechanisms’. *The Academy of Management Review*, 22 (4), 911–945.

Kenney, M., (2007). ‘The Architecture of Drug Trafficking: Network Forms of Organisation in the Colombian Cocaine Trade’. *Global Crime*, 8 (3), 233–259.

Khodyakov, D., (2007). ‘Trust as a Process’. *Sociology*, 41 (1), 115–132.

Levi, M., (2008). ‘Organized Fraud and Organizing Frauds’. *Criminology and Criminal Justice*, 8 (4), 389–419.

Lewis, J.D. and Weigert, A., (1985). ‘Trust as a Social Reality’. *Social Forces*, 63 (4), 967–985.

Lo, T.W., (2010). ‘Beyond Social Capital: Triad Organized Crime in Hong Kong and China’. *British Journal of Criminology*, 50 (5), 851–872.

Luhmann, N., (2000). ‘Familiarity, Confidence, Trust: Problems and Alternatives’. in D. Gambetta, (ed.) *Trust: Making and Breaking Cooperative Relations*. Department of Sociology, University of Oxford, 94 – 107.

Lusthaus, J., (2012). ‘Trust in the World of Cybercrime’. *Global Crime*, 13 (2), 71–94.

Mann, D. and Sutton, M., (1998). ‘>>NETCRIME: More Change in the Organization of Thieving’. *British Journal of Criminology*, 38 (2), 201–229.

McCarthy, B. and Hagan, J., (1995). ‘Getting into Street Crime: The Structure and Process of Criminal Embeddedness’. *Social Science Research*, 24 (1), 63–95.

McCarthy, B. and Hagan, J., (2001). ‘When Crime Pays: Capital, Competence, and Criminal Success’. *Social Forces*, 79 (3), 1035–1060.

McCarthy, B., Hagan, J., and Cohen, L.E., (1998). ‘Uncertainty, Cooperation, and Crime: Understanding the Decision to Co-offend’. *Social Forces*, 77 (1), 155–184.

McIllwain, J.S., (1999). ‘Organized crime: A Social Network Approach’. *Crime, Law and Social Change*, 32 (4), 301–323.

McKnight, D.H., Cummings, L.L., and Chervany, N.L., (1998). ‘Initial Trust Formation in New Organizational Relationships’. *The Academy of Management Review*, 23 (3), 473–490.

Möllering, G., (2001). ‘The Nature of Trust: From Georg Simmel to a Theory of Expectation, Interpretation and Suspension’. *Sociology* , 35 (2), 403–420.

Morselli, C., (2001). ‘Structuring Mr. Nice: Entrepreneurial opportunities and brokerage positioning in the cannabis trade’. *Crime, Law and Social Change*, 35 (3), 203–244.

Morselli, C. and Petit, K., (2007). ‘Law-Enforcement Disruption of a Drug Importation Network’. *Global Crime*, 8 (2), 109–130.

Pearson, G. and Hobbs, D., (2003). ‘King Pin? A Case Study of a Middle Market Drug Broker’. *The Howard Journal of Criminal Justice*, 42 (4), 335–347.

Peretti, K.K., (2008). ‘Data Breaches: What the underground world of “carding” reveals’. *Santa Clara Computer and High Technology Journal*, 25, 375–414.

Portes, A., (1998). ‘Social Capital: Its Origins and Applications in Modern Sociology’. *Annual Review of Sociology*, 24 (1), 1–24.

Poulsen, K., (2011). *Kingpin: How one hacker took over the billion-dollar cybercrime underground*. New York: Crown Publishing.

Powell, W.W., (1990). ‘Neither market nor hierarchy: network forms of organization’. *Research In Organizational Behavior*, 12 (1), 295–336.

PwC, (2012). *UK Information Security Breaches Survey*. Available at: http://www.pwc.co.uk/audit-assurance/publications/uk-information-security-breaches-survey-results-2012.jhtml (Accessed January 29th 2013)

Sandywell, B., (2010). ‘On the Globalisation of Crime: the Internet and New Criminality’. in Y. Jewkes and M. Yar, (eds.) *Handbook of Internet Crime*. Devon: Willan Publishing, 38–66.

Tajfel, H., (1982). ‘Social Psychology of Intergroup Relations’. *Annual Review of Psychology*, 33 (1), 1–39.

Thomas, R. and Martin, J., (2006). ‘the underground economy : priceless’. *The USENIX Magazine*, 31 (6), 7–16.

Thorelli, H.B., (1986). ‘Networks: Between markets and hierarchies’. *Strategic Management Journal*, 7 (1), 37–51.

Tsai, W., (2002). ‘Social Structure of “Coopetition” within a Multiunit Organization: Coordination, Competition, and Intraorganizational Knowledge Sharing’. *Organization Science*, 13 (2), 179–190.

U.S. District Count, (2004). *Operation Firewall Indictment. U.S. District Court, District of New Jersey.* Available at: http://www.justice.gov/usao/nj/press/files/pdffiles/firewallindct1028.pdf [Accessed 31 Jan 2010].

Uzzi, B., (1997). ‘Social Structure and Competition in Interfirm Networks: The Paradox of Embeddedness’. *Administrative Science Quarterly*, 42 (1), 35–67.

Van Calster, P., 2006. Re-visiting *Mr. Nice*. On Organized Crime as Conversational Interaction. *Crime, Law and Social Change*, 45 (4), 337–359.

von Lampe, K., (2003). 'Criminally Exploitable Ties: A Network Approach to Organized Crime'. In E. Viano, J. Magallones and L. Bridel (eds.) *Transnational Organized Crime: Myth, Power, and Profit*. North Carolina: Carolina Academic Press, 9–22.

von Lampe, K. and Johansen, P., (2003). 'Criminal Networks and Trust. On the importance of expectations of loyal behaviour in criminal relations'. *In*: *The 3rd annual meeting of the European Society of Criminology (ESC)*. 102–113.

von Lampe, K. and Johansen, P., (2004). 'Organized Crime and Trust: On the conceptualization and empirical relevance of trust in the context of criminal networks'. *Global Crime*, 6 (2), 159–184.

Wall, D.S., (2008). *Cybercrime: The Transformation of Crime in the Information Age*. Malden: Polity Press.

Wall, D.S. and Williams, M., (2007). 'Policing Diversity in the Digital Age'. *Criminology and Criminal Justice*, 7 (4), 391–415.

Walther, J.B., (1995). 'Relational Aspects of Computer-Mediated Communication: Experimental Observations over Time'. *Organization Science*, 6 (2), 186–203.

Walther, J.B., (1996). 'Computer-Mediated Communication: Impersonal, Interpersonal, and Hyperpersonal Interaction'. *Communication Research*, 23 (1), 3–43.

Wasserman, S. and Faust, K., (1994). *Social Network Analysis: Methods and Applications (Structural Analysis in the Social Sciences)*. Cambridge University Press.

Webber, C. and Yip, M., 2013. Drifting on and off-line: humanising the cyber criminal. *In*: S. Winlow and R. Atkinson, eds. *New Directions in Crime and Deviancy*. Abington: Routledge, 191–205.

Weerman, F.M., (2003). 'Co-offending as Social Exchange. Explaining Characteristics of Co-offending'. *British Journal of Criminology*, 43 (2), 398–416.

Williams, M., (2007). 'Policing and Cybersociety: The Maturation of Regulation within an Online Community'. *Policing and Society*, 17 (1), 59–82.

Williams, P., (1998). 'The Nature of Drug-Trafficking Networks'. *Current History*, 97 (618), 154–159.

Williamson, O.E., (1979). 'Transaction-Cost Economics: The Governance of Contractual Relations'. *Journal of Law and Economics*, 22 (2), 233–261.

Williamson, O.E., (1991). 'Comparative Economic Organization: The Analysis of Discrete Structural Alternatives'. *Administrative Science Quarterly*, 36 (2), 269–296.

Williamson, O.E., (1993) ‘Calculativeness, Trust, and Economic Organization’. *Journal of Law and Economics*, 36 (1), 453–486.

Yip, M., 2011. An Investigation into Chinese Cybercrime and the Applicability of Social Network Analysis. *In*: *ACM Web Science Conference 2011, Koblenz, 14-17 June*.

Yip, M., Shadbolt, N., and Webber, C., 2012. Structural Analysis of Online Criminal Social Networks. *In*: D. Zeng, L. Zhou, B. Cukic, G. Wang, and C. Yang, eds. *IEEE International Conference on Intelligence and Security Informatics (ISI) 2012, Washington D.C., 11-14 June*. Piscataway: IEEE, 60–65.

Yip, M., Shadbolt, N., Tiropanis, T., and Webber, C., 2012. The Digital Underground Economy: a Social Network Approach to Understanding Cybercrime. *In*: *Digital Futures 2012: The Third Annual Digital Economy All Hands Conference, Aberdeen, 23-25 October*. Aberdeen.