Honour Among (Cyber)thieves?

Jonathan Lusthaus

ExLegi-Institute, Department of Sociology
University of Oxford
Abstract

It is well known that criminals, who operate outside the law and the protection of the state, face difficulties in cooperating due both to the requirement of secrecy and a deficit of trust. For cybercriminals the anonymity of the Internet creates further challenges, making it even more difficult to assess trustworthiness and enforce agreements. Yet, contrary to expectations, collaboration among cybercriminals is prevalent and a sophisticated industry is emerging. The purpose of this paper is to address this puzzle in relation to profit-driven cybercrime. It draws on existing empirical studies, along with a collection of interviews with former cybercriminals (and hackers) that provide a valuable form of data on micro-level and often secretive interactions. It examines four key mechanisms that lead to improved cooperation: reputation, appearance, performance and enforcement. It also addresses the rarely discussed, and somewhat counterintuitive, role that offline interactions may play in enhancing collective action among cybercriminals.

Keywords: cybercrime; cooperation; trust; extra-legal governance; offline dimension
Honour Among (Cyber)thieves?

By Jonathan Lusthaus

In recent times, cybercrime has emerged as a significant global challenge. The early hackers of the 1960s, whose central motivation was intellectual curiosity, have now been joined in large numbers by those seeking profit or to perpetrate other harm. Among profit-driven cybercriminals, the focus of this present paper, business is thriving (EC3, 2014: 11). They are increasingly professional and increasingly organised, leaving behind the stereotype of the lone teenage hacker as the fundamental model of a cybercriminal (Ablon et al., 2014: ix; EC3, 2014: 19). Cybercriminal structures now range from small “crews” that carry out jobs together to large forums that can attract thousands of members and provide an online marketplace, or “criminal eBay”, where cybercriminals from across the world can do business (see, for instance, Davies, 2010; Krebs, 2015; Drömer and Kollberg, 2012).

On these forums, individuals trade a plethora of illicit goods, such as malware\(^1\) or stolen credit card data, and offer their services for hire, such as hacking or renting out a “botnet”\(^2\) (Holt and Lampke, 2010; Décary-Hétu and Dupont, 2013). These marketplaces play an important role in the underground economy, by providing online hubs for disparate actors to coalesce around where they can trade, network and learn. Some forums are focused on a specific sub discipline, like hacking, while others cover a very broad range of activities useful to cybercriminals, from technical products to money laundering services. Forums exist in countless languages, but the key marketplaces are usually in Russian or English (EC3, 2014: 19-20).

\(^1\) Malicious software such as viruses and worms.
\(^2\) A botnet is a network of infected computers that can be used to harvest data, send spam or carry out attacks, depending on the interests of its botmaster.
The cybercrime industry has grown to become sophisticated and specialised. While many cybercriminals operate online, in some parts of the globe “cybercriminal businesses” have even emerged, operating out of physical office space with pseudo-corporate structures (Lusthaus, 2014). Illicit enterprises now range enormously in scope from identity theft and fraud to blackmail and extortion to intellectual property violations and spam among others. Many schemes are centred on exploiting sensitive information that has been obtained for monetary gain. But some approaches do not always fit this model, such as when an extortion attempt might make use of distributed denial of service attacks (DDoS) to overwhelm a system (Lusthaus, 2014).

The offenders involved in cybercrime are increasingly specialised (Ablon et al., 2014: ix; EC3, 2014: 19). High level hackers and coders continue to find roles within the industry, but they have been joined by others who may not have technical excellence, but can help plan operations, make use of “off the shelf” malware, “social engineer” victims and provide “cashing out” services that can convert virtual loot into offline funds.

As cybercrime has evolved, so too have those researching it. Academic studies of cybercrime are no longer limited to computer science and related disciplines. While there are essential technical aspects to the phenomenon, a number of scholars have realised that there is also an important “human” dimension that needs to be addressed. There are a number of important subjects concerning the profiles of cybercriminal, how they are organised and how they operate. Such topics are well suited to research by social scientists, who can bring their methodologies and theories to bear on a novel subject, thereby making an important contribution to the examination of this new challenge. What has been a niche area in the social sciences is now fast flowering. The earlier literature attempting to comprehend the new phenomenon in conceptual
terms (for instance, Grabosky, 2001; Wall, 2001; Wall, 2007) has recently been joined by more empirically driven studies (Décary-Hétu and Dupont, 2012; Holt and Lampke, 2010; Hutchings, 2014). Gaining access to new forms of data, such as from the forums where cybercriminals congregate online, appears a key factor in driving progress in the field (along with, no doubt, the rising importance of cybercrime in public discourse). Scholars have also attempted to apply a number of theoretical frameworks to aspects of the cybercrime case, including social learning theory (Skinner and Fream, 1997), deindividuation theory (Demetriou and Silke, 2003), and routine activity theory (Yar, 2005).

While some of these approaches fall within rational action theory, a number of important concerns within the paradigm have yet to be widely explored in the context of cybercrime. Chief among these is the issue of how cybercriminals cooperate with each other in the anonymous, and inherently low-trust, environment of online crime. This issue has found only rare mention in the literature (Dupont, 2014; Yip et al., 2013; Lusthaus, 2012), but is important not only to comprehending the still somewhat mysterious world of cybercrime but should also be of relevance to broader literatures on trust, cooperation and extra-legal governance. This is because cybercrime appears to present an “extreme” case where cooperation is emerging in a particularly low trust environment.

Criminals, who operate outside the law and the protection of the state, face difficulties in cooperating due both to the requirement of secrecy and a deficit of trust. Actors in the underworld: cannot rely on the state to protect property rights; often do not have access to reliable information on goods and services; find it difficult to freely advertise illicit wares; and can never be sure if their partners are honest criminals or
undercover agents (Campana and Varese, 2013: 265). In response to such apparent challenges, a relatively significant body of literature has emerged examining how trust can be buttressed in a number of criminal (among other extra-legal) settings, leading to successful cooperation where it would naturally seem unlikely (Gambetta, 1993; Gambetta, 2009; Varese, 2001; Skarbek, 2011; Levi, 2008; Reuter, 1983; Wang, 2011).

But for cybercriminals the anonymity of the Internet creates further challenges on top of those facing conventional criminals. It is difficult to assess trustworthiness and enforce agreements when one doesn’t even have physical interactions, which would normally indicate the identity of partners. This is not to mention that if one did manage to identify their collaborators, they might be dispersed around the globe. Such an environment appears to offer little hope for physical violence, which has often been a pillar of enforcing cooperation in traditional crime. As a result of these challenges, it might be expected that cybercriminals would often act alone and not in collaboration with others. Nonetheless, in recent years cybercriminals have increasingly formed links with other criminals. It would not be overstating matters to say that there is a now a fully-fledged cybercrime industry, with clear elements not only of low-level collaboration, but also facets of broader organisation and governance (Holt and Lampke, 2010; Kshetri, 2010; Moore et al., 2009).

The purpose of this paper is to address this puzzle of how cybercriminals have managed to overcome their trust problem to achieve fairly wide-scale cooperation. In so doing, it will apply core aspects of rational action theory to cybercrime that have yet to be investigated in much depth. In order to answer this question, this paper will draw on existing empirical studies, which often rely on data from online
cybercriminal trading forums. A core addition to this body of knowledge will be a collection of interviews with former cybercriminals (and hackers) carried out by the author. These interviews provide a valuable form of data on often micro-level (and secretive) interactions, which are very difficult to observe through other means. The interview participants include both arrested/convicted and self-identified cybercriminals, and span a range of jurisdictions. They also range from low-level offenders to the highest echelons.

The focus of the paper is on profit-driven cybercrime. While there may be some parallels with other forms of cybercrime, these fall outside the scope of the article. The first section of the article will introduce the key theoretical concepts necessary to address this question from a rational action perspective. Coming out of that discussion, the following four sections will each address one mechanism that enhances cooperation and how it applies to profit-driven cybercriminals. The final section will address the role that offline interactions may play in cybercriminal cooperation. This is a somewhat counter-intuitive aspect of cybercrime and is often overlooked in many studies. But it may provide a vital piece of the puzzle.

**Trust, Trustworthiness and Cooperation**

In order to cooperate with one another, cybercriminals must overcome the risks of doing business with anonymous fraudsters, thieves and extortionists, and also the lack of any legal recourse for agreements to be enforced. How do they overcome these challenges? In other criminal settings *trust* has been suggested as a possible explanation for co-offending (Campana and Varese, 2013: 264; McCarthy et al., 1998). It is not unreasonable to take trust as a starting point for investigations of
cooperation in the cybercrime context.

The first step in this process is to define trust and understand how it operates. As Dasgupta (1988) puts it, trust is: “correct expectations about the actions of other people that have a bearing on one’s own action when that action must be chosen before one can monitor the actions of those others” (p. 51). In a similarly influential formulation Coleman (1990) sees the phenomenon as:

“In an incorporation of risk into the decision of whether or not to engage in the action. This incorporation of risk into the decision can be treated under a general heading that can be described by the single word “trust”. Situations involving trust constitute a subclass of those involving risk. They are situations in which the risk one takes depends on the performance of another actor” (p. 91).

It is important to distinguish here between the concepts of trust, trustworthiness and enforcement. The problem of trust is that not everyone is trustworthy. In attempting to counteract this problem, mechanisms might be sought to make individuals more trustworthy, thereby reducing the risk involved in transactions (Hardin, 2001). But one might also sidestep direct trustworthiness altogether and place responsibility for a transaction in the hands of a third party (although then perhaps creating a new indirect problem of trust with that party). Third party enforcement can be carried out by the state or its endorsed agents, along with a number of extra-legal actors capable of performing similar functions in different contexts (Gambetta, 1993; Varese, 2001; Dixit, 2004). There are also aspects of self-enforcement that can be carried out by the individuals themselves.

In these terms, rational actors will seek to reduce the amount of risk involved in any action with a partner, or avoid the action entirely if the risk is deemed too great.
Within societies, there are a number of institutional mechanisms that can assist in reducing this risk, including formal contracts and legal systems to enforce them. There are also more informal mechanisms that might be employed such as relying on past interactions to determine trustworthiness (Axelrod, 2006; Gibbons, 2001) or reputation systems that can disseminate information on those you haven’t met directly (Cook et al., 2009). But even with such mechanisms, some element of risk will always remain. Court systems may not function efficiently or transparently in various jurisdictions or a partner that one has dealt with over a number of years might suddenly disappear with a large sum of money.

For those operating in the criminal underworld, the level of risk is compounded by having no recourse to institutions of the state. As part of this class of outsiders, cybercriminals can only make use of more informal mechanisms to minimise their trust problem. In some regards, it might be expected that cybercriminal efforts to enhance cooperation would be similar to those of conventional criminals. Like conventional criminals, cybercriminals also face the challenge of building partnerships with potentially untrustworthy parties, while facing law enforcement scrutiny that limits the openness with which they might operate. But due to the novel criminal environment provided by cyberspace, precisely how cybercriminals establish and maintain cooperation, organisation and governance may differ in certain ways.

This environment provides both advantages and challenges to cybercriminals. Anonymity, which is ostensibly available online (but is by no means guaranteed), provides a shield against law enforcement interest and allows cybercriminals to advertise themselves (and their wares) relatively openly online. But anonymity also means that it is difficult for cybercriminals to know whom they are dealing with and
ultimately whether to trust them. For instance, if a certain cybercriminal reputation is tarnished, the cybercriminal in question can abandon his/her nickname and use a different handle. This is not to mention that physical enforcement becomes very difficult when dealing with unknown parties, who may also be operating from a far away jurisdiction.

The rest of this paper examines what mechanisms cybercriminals employ to address these challenges and enhance cooperation. Mechanisms, in this case, are those processes which reduce the risks for cybercriminals to collaborate together. In terms of buttressing trustworthiness, there are three conventional mechanisms that likely apply: reputation; performance and appearance (Sztompka, 1999: ch 4). But there is also an alternative mechanism that does not involve direct trustworthiness, instead making use of avenues of enforcement. Each of these four overarching mechanisms will be discussed in turn. Following that, the final section will address the role that offline interactions play in cybercriminal cooperation. This is a point that is rarely discussed in the literature and in some ways appears counterintuitive: some of the ways certain cybercriminals enhance cooperation may involve sacrificing their anonymity and partnering with collaborators in the offline world. The very loss of anonymity and the protections that it affords, may act as an important factor in encouraging collaboration with other criminals, by reducing risks of untrustworthy partners and enhancing enforcement options. Rather than offering a new means of making sense of cooperation among cybercriminals, this offline element will be subsumed into the broader discussion of how the trustworthiness (reputation, appearance, performance) and enforcement mechanisms might enhance cooperation.

Reputation
It is clear that reputation is central to how cybercriminals assess trustworthiness and engage in cooperation. As one senior security firm officer and former hacker put it: the “whole world revolves around reputation, everything revolves around reputation…” (Lusthaus, 2012: 93). Former spammer Dave explained the importance of reputation in this way:

…most of these guys, it’s small circles of friends. Little groups all like associates. That’s why I said at the beginning like reputation. So if your reputation gets tarnished and you get pushed out of your little bubble, word spreads pretty fast among the other little bubbles close to your bubble. Like you tell your friends, your friends tell your other friends oh that guy he fucking ripped me off, he’s no good. So then you’re working with, instead of the higher caliber people who are dealing with large sums of money then they would probably have to work with like Nigerians or, I don’t know, someone who doesn’t have that much cash. It wouldn’t be worth it (Author, 2012a).

But how is a cybercriminal reputation built? If two cybercriminals interact with each other on a regular basis, it is not difficult to see how this might build familiarity and ultimately reduce the perceived risks of doing business together. This could be due to parties being able to incrementally test their partner’s ability and willingness to carry out their side of the bargain, but also that over the course of this relationship each side can sanction the other for defections, perhaps leading to greater compliance (see Axelrod, 2006; Klein and Leffler, 1981; Abreu, 1988). On the other hand, repeated interaction itself may actually incentivise cooperation over the course of dealing. Schelling (1980) argues that trust can be achieved because parties may recognise they have more to gain from a “tradition of trust” than from cheating in one instance (pp. 134-135).
There is some evidence that repeated interactions among cybercriminals builds reputations for trustworthy behaviour. For instance, in their study of underground forums, Motoyama et al (2011) finds that a significant amount of personal messages responding to trading (advertisement) threads came from prior acquaintances (p. 75). This suggests that a number cybercriminals on those forums felt more comfortable dealing with existing partners rather than engaging with new ones, although other factors might also be involved. Former North American cybercriminal, Scott, supports this point. His preference was to work with people he already knew or had worked with previously before: “Once I found someone that could do a certain thing or provide a certain service well or whatever, I would just keep using him until he no longer could, ripped me off, or quit/disappeared or whatever” (Author, 2015b).

Repeated interaction is an important aspect of online reputations, but there is a broader complication in relation to cybercrime that must be addressed: one’s online reputation can be somewhat (or entirely) unrelated to one’s offline existence. The reputation of a cybercriminal is often not tied to the real offline person (who ideally remains anonymous), but to their online nickname or handle (Author, 2015a). Cybercriminal “niks” are effectively the brand of a cybercriminal. One’s handle is the foundation of a reputation on the web, which incentivises maintaining that nickname or a variation of it. But there is also a competing incentive to change online names regularly in order to distance oneself from misdeeds against other cybercriminals or past crimes that might attract law enforcement attention.

Cybercriminals must calculate what approach to take. At one extreme, it appears, are those who change their nicknames as regularly as every three months. At the other are individuals who value their reputation over any risk, keeping the same handle for their
entire career (Lusthaus, 2013a). Dave fell into the latter category: “I picked a random name out of the dictionary and I always stuck with that name. The best advice I had from someone was when I was probably about 15 on the Internet was he told me: have one name and use it and get a reputation” (Author, 2012a). Others might undertake more of a hedging approach by either using variations of the same name or linking new names to old ones and providing a trail of sorts for existing partners to follow (Author, 2011a).

While cybercriminals might build a reputation through repeated interactions with other individuals and maintain that reputation through their brand (nick)name, the next question is how information about their reputation may be learned by others not directly known to them. After all, not every interaction between cybercriminals will be part of a long dyadic process, and even those that are dyadic will require the initial step of participants deciding whether the risk is low enough to engage in the original interaction. One possible answer is that information about individual cybercriminals could pass through social networks, thereby allowing cybercriminals to learn important details about potential partners. But, as Granovetter (1985, p. 490) tells us, a better source “is information from a trusted informant that he has dealt with that individual and found him so”.

There is certainly evidence for this proposition in the underground economy. Referrals are a common vetting tool for conventional criminals and cybercriminals employ similar means online. Scott explained that “word-of-mouth” is the “best option” for gauging reputation: “If you are looking for someone to provide a service you need and you have some other people you are already working with on other things, its always good to ask them first if they know a good cashout guy, or dumps
vendor, id vendor or whatever it may be” (Author, 2015b). To help the referral process, cybercriminals also list potential referees when introducing themselves on forums and elsewhere to allow others to vet them (Lusthaus, 2012: 85-86). But on the Internet, one can also engage in background checks rather than just rely on the word of others. Cybercriminals have the advantage of being able to compare a user’s “online footprint” to the information they have drawn directly out of him/her. Of course, some cybercriminals might take this even further and hack (potential) collaborators to check their backgrounds and verify their claims (Author, 2015b).

In large groups, the cost of requesting referrals or doing background checks on other members is high. Major forums can have up to thousands of members so it’s likely that many users would not know each other or have mutual acquaintances who can make a “safe” introduction. As a result, in order to reduce risks, forums and other online institutions have had to find ways of formalising the reputation mechanism within their structures. So far the literature has identified a range of tools employed for this purpose. A number of forums have reputation scales where users can be rated according to their past actions, either by forum officers or all members depending on the case. These ratings can then be used by members in deciding whether to collaborate with a specific individual (Décary-Hétu and Dupont, 2013) and can potentially lead to an efficient market (Mell, 2015). Motoyama et al. (2011) find evidence that higher reputation scores correlate to a greater number of private messages from other users (usually indicative of interest in doing business, but not always).

Aside from numerical scales, some forums also have reviews and feedback options so that buyers can provide qualitative information on their experience of interacting with
certain sellers (Holt, 2013a: 173; Holt, 2013b: 2). These systems appear to be very important in choosing potential partners:

If you are advertising your service on a forum etc, then you have your own thread where people leave feedback for your service and products etc. Kind of like eBay, you do business with the guy, you leave feedback in his thread saying if he was helpful and legit or not or if you had any problems etc. If you see someone on there that has been dealing with several other people you know for awhile and the people you already know and trust are leaving good feedback, then probably ok to deal with him (Author, 2015b).

There can also be specific “name and shame” sections on some forums for users to self-report scammers. Being publicly shamed in this way can damage reputations, lead to ostracisation, along with acting as a deterrent to other would be “rippers” (Lusthaus, 2012: 89). Some forums also have formal ranks, such as “trusted members” among others, if users prove their “criminal credentials to the administrator and moderators”. Such ranks are a means for forums to provide more tangible evidence of a good reputation. This acts in conjunction with a number of more “elite” forums which often require new members to be vouched for by at least two existing members (Author, 2015b). This reduces the need to seek referrals with each new partner on the forum. In some sense, all potential partners are pre-vetted.

The above discussion suggests that reputation is very important for cybercriminals to lower the risks of doing business with each other. But in order to make sense of how cybercriminals make use of reputation, it is important not to see their approach as entirely novel. This is particularly the case with illicit trading forums, which bear some similarity to legal online auction sites like eBay and employ analogous

---

3 R v Kelly and Others [Case Summary], Southwark Crown Court, 2011, 35.
4 Some other forums require payment to join which seems to operate as a different less clear test. It does not address reputation directly but may instead act as a signal of commitment, a bond or simply offset the administrative costs of running the site.
reputation systems (Dellarocas, 2003; Resnick and Zeckhauser, 2002; Diekmann et al., 2009). But there are also parallels between reputational systems on forums and offline historical examples from entirely different contexts (Milgrom et al., 1990; Greif, 1989). For instance, the Champagne fairs, a major centre of trade in medieval Europe, faced quite similar issues of trust and enforcement and addressed them in familiar ways. In this example, the problem was that merchants congregated from many different lands and then left, making the effective enforcement of contracts difficult. The fairs overcame this challenge with a system of private judges who kept records of merchants’ past behaviour, so that before engaging in a deal, traders would enquire with a private judge about their potential partner’s reputation (Milgrom et al., 1990). Cybercriminal forum reputational mechanisms like reviews, naming and shaming sections and numerical indexes appear to play an analogous role to that of private judges at the Champagne fairs. They effectively lower the cost of users having to personally investigate all other users they might deal with, by providing public information on past transactions within the community.

**Appearance**

Appearance is another important means for cybercriminals to demonstrate trustworthiness. But the way that appearance functions online is somewhat mysterious, even to the cybercriminals themselves:

I can’t think of how to explain it. You just get a feeling for how someone is after talking to them on the chat rooms, seeing how they respond, what sort of things they talk about, what sort of things they take an interest in. Very much like talking to someone, like we are talking now. I mean there are no facial expressions or anything like that go into it, but you can still judge someone fairly well just from text I think, sometimes
There is a difficulty attempting to comprehend appearance in relation to online interactions because many aspects of appearance are, traditionally, physical. Some aspects of physical appearance can’t be changed (or are difficult to do so), such as size, shape, skin colour and so on. Other aspects can be altered such as clothing or hair style, but still remain partially dependent on certain constraints, like budget. On the other hand, online appearance is almost entirely mediated and many aspects can be much more easily manipulated and faked. It is much more a construction of a persona. This section addresses appearance in these terms, with a focus on the personas that can be presented. But in terms of trustworthiness, it is particularly concerned with potential “tells” that cybercriminals rely on to ascertain aspects of their confreres’ “true appearance”. In a sense, these are the limitations for persona creation that remain despite the online nature of the interactions. These include: style; language/nationality; memberships/affiliations; time spent online.\(^5\)

In terms of style, Scott was in agreement with Sean that cybercriminals could get a sense of a user from the way they wrote and presented themselves. But he was a little more specific about what he looked for: he avoided people or talked about unnecessary issues, asked stupid questions and made unverified claims. In his view people who are serious about business are “generally quiet as can be in public (forums/chatrooms) and straight to business over PM’s etc”.\(^6\) He also watched for inconsistency in typing patterns or unusual offers/requests. These could be evidence that a nickname had been hijacked, taken over by law enforcement, or that something

---

\(^5\) While beyond the scope of this paper, it’s possible to view issues of cybercriminal appearance through a signaling theory framework: Lusthaus 2012; Décary-Hétu and Leppänen 2013. On signaling theory more generally see Spence 1973 and Gambetta 2009.

\(^6\) “PM” is short for private message.
else untoward was going on (Author, 2015b). On the other hand, style is not entirely beyond faking. Max Butler actively tried to vary his writing style to avoid similarities between his cybercriminal persona and security papers he had written as a white hat or posts made under his real name (Poulsen, 2011: 119).

The second key aspect of online appearance is language/nationality, which can play a number of different roles for cybercriminals – some negative some positive. This factor can deter cybercriminals from dealing with or trusting certain potential collaborators, as is the case with Russian-speaking cybercriminals who are often wary of English speakers. Following successful law enforcement operations against high-level forums in the 2000s, certain Russian-speaking cybercriminals appear to have become more guarded in their operations, choosing to operate only in the Russian language, possibly as a means of keeping out Western law enforcement, or at least making it one step more difficult for them (Glenny, 2011; Poulsen, 2011). Interviews I carried out with former cybercriminals suggested that relations between Western and Eastern European cybercriminals were somewhat hopeful in the early 2000s, but subsequently deteriorated (Author, 2015b; Author, 2015a). But potential prejudices are not limited to Russian-speakers. Former Western European cybercriminal Sean was open to working with a range of people regardless of age, gender or ethnicity, but there was one rider to this. He judged potential collaborators on their ability to speak English and generally those who did not speak English well would not be allowed into the groups he operated in. This seemed to be a practical measure to avoid confusion as much as anything (Author, 2011a).

In contrast, in some circles, having the right nationality or language can be a positive quality that might even encourage collaboration. Scott explained that poor English
might be a good sign for a “supplier” (of credit card data in his case), as many good suppliers came from Eastern Europe (Author, 2015b). Some cybercriminals might even pretend to be from Eastern Europe, trying to appropriate their good reputation in the industry (Author, 2015b). This was the case with Albert Gonzales, one of the leading cybercriminals of his era, who at one point adopted the nickname “Segvec” and was believed to be from Ukraine despite being Cuban American (Poulsen, 2011: 198).

The third significant aspect of appearance is tied to where certain cybercriminals are operating online and what affiliations they have. While this may interrelate with other mechanisms, membership of certain forums and other groups in itself helps create an appearance of trustworthiness. Frequenting the right places at the right times is one approach used by conventional criminals to identify each other, and filter out non-criminals. For instance, when Joseph Pistone infiltrated the Bonanno crime family in late 1970s New York as an undercover FBI agent, his initial strategy was to frequent “wise guy” bars and establish a criminal appearance by association (Pistone, 1987: 46). Parts of the online underground, which are often hidden, are even more difficult to accidentally happen upon (Lusthaus, 2012: 82-83). A user who is present in one of these places has to have at least some degree of knowledge and connections to be there in the first place (Author, 2012a).

This closely relates to the final element of appearance under discussion: time spent online. This is a good indicator that someone is not a “nube” (newcomer), or otherwise a ripper or law enforcement, in that they have managed to maintain a viable online presence for a considerable amount of time. The basic principle here links back to reputation in some ways. The longer one has been around for and attached to a
specific nickname or profile, the more time that has been invested. The bigger investment of time, the less likely someone is to jeopardise it and so the more trustworthy that person becomes. A number of forums list the starting date for each user on their profile, which demonstrates how long they have been around for. Another more esoteric means of determining whether someone is new to the scene is from their nickname. The longer, more complex and “decorated” a nickname is, the more likely that person is a young, immature “nube” (Author, 2015b; Author, 2011a). More experienced actors are often content with simpler, shorter nicknames.

Performance

It is clear that while cybercriminals might employ reputation or appearance to determine trustworthiness, these alone may not be enough to counter the risk involved in certain interactions. Some cybercriminals might require further assurances before making a deal or beginning an enterprise together and, in such cases, the performance mechanism becomes an important factor. This can be either generalised performance or a more specific variety of performance. The more generalised case sees cybercriminals displaying their bona fides as a broad advertisement for their services or goods. For instance, prowess demonstrations can be regularly found in online marketplaces. One method of demonstrating a certain skill or piece of knowledge, particularly in relation to less experienced/competent users, is to post tutorials on forums, which often have a dedicated section for this (Lusthaus, 2012: 87-88).

Performance also can be more specifically tied to a particular criminal endeavour. For instance, “money mules” sourced online might demonstrate their trustworthiness by successfully moving on small amounts of money deposited to them, after which they
may be entrusted with incrementally larger amounts (Lusthaus, 2012: 85). For those selling products on forums or in other settings, samples or test buys might play a similar role in assuaging any concerns over quality. There is evidence that the forum officers (or others they endorse) might be directly involved in this process, testing sellers’ products themselves. This reduces the need of individual users to verify the quality of goods in each case (or simply trust that they will be of sufficient quality). In a number of cases, those whose products have been verified will receive the title of being a “reviewed vendor” which might also be accompanied by a report on the quality of their goods. Being tested may be voluntary for sellers, but it is not difficult to see how it might help in their sales pitch if they are approved in such a way (Holt, 2013a: 173; Holt and Lampke, 2010; Yip et al., 2013: 13). Some might also advertise their verified status from other forums that they might be on, as a means of attracting more business (Holt, 2013b: 14).

Some of the performance checks employed by cybercriminals don’t necessarily relate to the product or service being offered, but are more subtly focussed on getting a sense of prospective (or returning) partners. Scott outlined his approach for assessing new partners, moving beyond appearance to employing clear tests. In these cases he would ask questions that only those in the field should know the answers to, such as a common problem with a certain brand of ATM. Otherwise Scott would seek possible red flags by going “the opposite way and make something up about it and see if he tries to agree with you on it”. Scott explained that it was important to carry out this evaluation in real time chat so that there was no opportunity to fabricate answers (Author, 2015b). He also thought similar tests were appropriate when trying to determine whether a formerly reputable nickname had been compromised or was being impersonated (either by law enforcement or a ripper):
If someone drops off out of nowhere and you haven't heard from them in a long time and they come back talking kind of strange with some weird excuse, it's always good to ask a verification question from the past that only they would know, just to make sure you are talking to the same person (Author, 2015b).

A suitable “verification question” might refer to a shared password from old business together, knowledge of who first introduced them to each other, or what project they first worked on together (Author, 2015b).

This discussion leads to a more general point of how cybercriminals can determine if other users are undercover agents. Performance appears to play a key role here, specifically relating to proof of one’s criminality. Some cybercriminals believe the only true method to unmask undercover agents is to force them to do something that is forbidden, such as hacking a website (Author, 2015c). This dovetails into the idea of “display crimes”, which are designed to provide proof of criminality. In conventional crime, the most stringent of such tests often involve carrying out a murder (Gambetta, 2009: 16-18). In cybercrime, the stakes are lower, but this performance test operates in a similar way.

**Enforcement**

Enforcement is the final mechanism under discussion in this paper. Enforcement can be carried out in three main ways: self-enforcement, collective enforcement by a group; or enforcement by a third party who may act on behalf of an individual or group. Punishment, coercion, monitoring, arbitration and guarantees are all treated as aspects of enforcement for the purposes of this section.
Cybercriminals only have limited enforcement options available when operating independently of online institutions like forums. Unlike in an offline context, they cannot employ violence. In very basic terms cybercriminals can sanction recalcitrant partners by refusing to continue cooperating with them. But cybercriminals also have some more punitive options open to them, including tools that appear to parallel the use of violence, but in weaker virtual terms. For instance, in the hacking group that Dupont (2014) studied, an alternative method of enforcement is described: the use of botnets to attack other hackers online through DDoS. Such attacks can be used collectively by the group against certain recalcitrant members or by members themselves against other members as a coercion or punishment tactic. Similar tactics have been used by competing forums against each other (Poulsen, 2011: 168).

There are also other forms of cybercriminal enforcement that have developed. “Doxing” involves the digging up of personal information and then publishing that information online to embarrass the person in question. It also effectively removes their anonymity, which is the most treasured possession of any self-respecting cybercriminal. Scott provides an example from his time online in relation to the downfall of a key cybercriminal player:

Take, for example, one cashout guy I used to know whose nick was XXXX7. His downfall came from under-estimating his supplier and deciding not to pay him $40k. Not soon after the rip was confirmed, he was kicked out of the IRC channel (where he was an operator at the time), banned from it, and the topic was changed to "Whoever wants to fuck XXXX click here". The link was to a page (on a hacked banking site lol) that had his picture, name, brothers name, address, phone, swift account #’s, bank acct numbers etc. Two to three weeks later he was busted (Author, 2015b).

7 Name removed to maintain anonymity.
This example demonstrates the seriousness of this form of punishment. Not only does it lead to embarrassment and a sense of violation, it also allows other actors online to make use of the posted information and engage in further violations (whether abusive or involving theft or fraud against him). More importantly, it may aid law enforcement in apprehending that person. Doxing can be carried out by any aggrieved member of the online community, but there are also professional doxing services that exist (Author, 2015b). “Swatting” is another punishment activity related to doxing, which is sometimes carried out by the same people. This involves duping emergency services into sending armed units to someone’s house or place of business, under the mistaken belief that there is an ongoing incident (Krebs, 2013).

Forums formalise and extend aspects of the enforcement mechanism to keep cybercriminals in line. The most widely documented and powerful sanction is exclusion from a forum by order of the administrator or moderators (Holt, 2013b; Holt and Lampke, 2010; Author, 2011a). But there are complexities involved. Scott indicated that sometimes bans might not be indicative of bad conduct, but rather biases of certain forum officers, who might be abusing their power or “hating”. As a result, those considering dealing with someone banned from a certain forum would best investigate further: “If it seemed like it was minor bullshit and possibly biased by the administrator or whoever, then you could still proceed if you thought it was worth it but obviously, be careful and take it as a warning ;-)”. On the other hand, if someone had been banned from a number of forums, then they are best steered clear of. In a sense, the idea of banning again links back to the reputation mechanism, in that the “best bet is to check into the feedback to see if other people (that you already trust/deal with) left feedback and talk to them and get their opinion” (Author, 2015b).
Linked to banning is the arbitration role that forum administrators often perform. The process is akin to an online trial and is seen across a number of forums (Davies, 2010; Motoyama et al., 2011: 75-76). Depending on the forum, the arbitrator may be a forum administrator or an otherwise well respected individual. Each side may present evidence to the arbitrator who then makes his/her decision (Author, 2015b). As a result of this process, punishments are be meted out, with exclusion being relatively common (Holt and Lampke, 2010: 44).

Finally, forums also make use of escrow to directly enforce agreements. Escrow services are provided by forum officers in some cases, but other forum members can also offer this service, if they are able to garner sufficient trust. The way the system works is that the third party guarantor holds the money until the goods have been received/verified, although it is also possible to be the point of transition for both the vendor’s goods and customer’s money. Guarantors can require payment, often in the form of a percentage, but do not always (Yip et al., 2013: 14; Holt, 2013a: 173; Holt, 2013b: 11).

The presence of escrow in the cybercriminal underground is regularly noted, but how it functions in practice is rarely discussed in much depth. In particular, questions remain regarding how the escrow providers themselves are deemed to be trustworthy. This point again returns to the reputation mechanism. Those that perform the role of escrow providers must have an excellent reputation. They are usually “wise old men” who have been around the scene for a long period and have invested considerable time in building a reputation for honest dealing. They might be administrators or high level moderators, who are known to be trustworthy. While complete honesty is

---

8 See also US v. Andrew Mantovani and Others, United States District Court, New Jersey, 2004 [indictment].
impossible, it is very rare for a guarantor to engage in a scam, as to attain such a role requires a reputation earned over a number of years. Such a person has the “ultimate reputation” and preserving that hard earned reputation is actually a large part of how those individuals can make money (Author, 2015b).

A Place for Offline Interactions?

The four mechanisms discussed above appear to enhance cooperation among cybercriminals online. For a number of cybercriminals, who operate largely (or solely) online, it is very important to make use of these mechanisms. They must come to terms with the nature of doing business in cyberspace where they cannot see partners or physically enforce agreements. In some ways, this is the appeal of cybercrime. Former North American cybercriminal Lance saw matters this way: “the anonymity that is provided by being online enables a lot of these people to commit crime whereas they would not have committed crime if they had to show their face to other people” (Author, 2015a). As such, he had a general rule not to meet in person with people he had met online. There was simply too much risk involved.

With that said, it is often overlooked that cybercriminal interactions are not necessarily confined to the Internet. Everyone who engages in online crime exists physically somewhere. Their local context is often important for influencing who they work with, what type(s) of cybercrime they engage in and whether they become involved in cybercrime in the first place. A relatively large number of cybercriminals appear to have significant offline interactions and operations in running their business. For instance, Albert Gonzales had a number of associates that he operated with in person, both for business and socialising. One of their main activities was “war-
driving”, which involved driving past or positioning themselves near the WIFI signals of major “big box” stores in order to access the network and steal credit card information (Verini, 2010).

The most obvious case of offline organisation that has developed with the rise of cybercrime is the cash out crew. Such groups are charged with converting virtual gains into money or physical products. By virtue of the physical nature of the work, often involving making purchases from shops or withdrawing money from ATMs, it is not surprising that a number of such offenders are known to each other (Author, 2015b). But some examples go beyond cash out (and other) crews and suggest structures that have developed to the point of approximating illicit companies. For instance, in 2012 a group of cybercriminals was arrested in Moscow for making use of Carberp malware to steal tens of millions of rubles from online bank accounts. Led by two brothers, the group rented office space and appeared externally to be a legitimate technology company (Ragan, 2012). Similar corporate-like structures, offices and a local presence have been observed with regard to spam (Krebs, 2014), virtual currencies used by cybercriminals,9 and bulletproof hosting providers (James Graham et al, 2009: ch 5). In the Romanian town of Ramnicu Valcea, online fraud has become somewhat of a local industry (Bhattacharjee, 2011).

Even those cybercriminals who prefer online interactions will sometimes meet in person. Lance might have had a policy against physical meetings, but he had still met a small number of online partners in person both in the United States and abroad (Author, 2015a). Across the former cybercriminals interviewed for this project, it was relatively common for them to have spoken on the phone and/or met with at least

some of their online collaborators, although in many cases that number was small (Author, 2011a; Author, 2015b; Author, 2014a; Author, 2015-2016). Generally it was sensible only to meet with partners one was quite sure were not law enforcement agents (Author, 2015a). The most famous meetings between cybercriminals offline were probably the CarderPlanet conferences in the early 2000s, which saw a number of members of the forum come together for conventions held in Odessa, Ukraine (Poulsen, 2011: 73-74; Glenny, 2011: 66-67).

This offline dimension of cybercrime is somewhat puzzling when the primary advantages of cybercrime are often viewed as anonymity and the increased protection that it provides. But the relevance of these physical interactions may actually be in relation to cooperation. Physical interactions between cybercriminals might enhance cooperation because they serve to counteract some deficiencies of online interactions: the difficulties in verifying people’s true identities and the limited enforcement options available on the Internet. Dealing with locally known people reduces the uncertainty of collaborating with a nickname online which could be changed or disappear entirely. But while the reputation mechanism might be enhanced by operating in the physical world, the real value of offline interactions is most likely with regard to a strengthening of the enforcement mechanism.

The concept of “information hostages” may be helpful in making sense of this. An information hostage approximates the historical exchange of hostages in order to buttress trust. But in this case compromising information rather than people are exchanged, which improves cooperation by giving each individual the power to incriminate the other if there is a defection (Schelling, 1980: 43-44). In the context of cybercrime forums, some similar processes have been observed. DarkMarket,
required those who wished to join to submit the details of 100 compromised credit cards. These would be verified by two reviewers, who would provide reports on their legitimacy (Davies, 2010). Nonetheless, the primary, and strongest, application of information hostages appears to be with regard to offline relationships. Gambetta (2009) outlines how paedophiles sharing child pornography online require various tests of commitment, along with proof that one is not a law enforcement agent, to join their groups. One such test, similar to the DarkMarket approach, was the provision of ten thousand original images. But a stricter test was that certain members travelled to other countries to vet would be recruits face to face. The primary significance of this was that when “identification is at a premium and must be kept secret, just showing one’s face is itself like giving a hostage, namely the knowledge of one’s key sign of identity” (pp. 62-63).

Some profit-driven cybercriminals also appear to vet potential collaborators they have met online face to face. Akmal, a Southeast Asian hacker who was involved in low-level cybercrime in his younger days, met a collaborator on a website and eventually arranged to sell hacked website data to him after a relatively long online relationship. Akmal and his partner chose to exchange the money for data in a café, each time they transacted. In hindsight Akmal acknowledged the risks involved in meeting a stranger in person for a criminal deal. But his main concern at the time was that he felt it was riskier to carry out the transaction online, where it couldn’t be directly monitored and it might leave a digital trail (Author, 2014a).

The enforcement mechanism might also apply to cybercriminal groupings that evolve out of existing offline relationships. For similar reasons that kinship could act as an effective information hostage (Campana and Varese 2013), working with known
people could also enhance cooperation. The more one knows about a collaborator, the
closer they are bound together and the easier to enforce agreements. By interacting
offline, cybercriminals open up (and open themselves up to) traditional tools of
physical enforcement among criminals: threats; destruction of property; harassment;
beatings; torture; death. Such enforcement mechanisms coupled with a knowledge of
offline identities is likely to lower the risk associated with defections in cybercriminal
dealings. Offline groupings have been suggested in a number of cases, including that
of Max Butler, the elite hacker and carding forum administrator. Butler’s key partner,
and the only person to fully know of the link between Butler and his online identity
Iceman, was a fraudster called Chris Aragon who had met Butler offline through a
mutual (criminal) acquaintance. While their relationship was not one of perfect trust,
they were effectively bound to each other and engaged in extensive criminal activity
together, until Aragon was arrested and turned Butler in (Poulsen, 2011).

The issue of physical enforcement links to a further question that is vital to
understanding cybercriminal cooperation: whether traditional organised crime groups
are playing a key role in cybercrime. While there are widespread claims in the media
that the Russian mafia and other such groups taking over cybercrime, there is very
little empirical evidence provided on this point. The issue is not dealt with in a much
better fashion by the academic literature with a distinct lack of data and a number of
loose claims (as argued by Wall, 2014; McCusker, 2006). This lack of knowledge is
unfortunate as the issue of potential organised crime involvement is very theoretically
significant. If the claims are true it could mean that the very same groups that govern
a number of conventional criminal activities are carrying out a key part of

10 On the issue of whether online cybercriminal groupings could classify as organised crime groups see
cybercriminal governance. Cybercrime would not offer much novel here, but may be a broader part of the existing criminal landscape in this regard.

As McCusker (2006) notes, there is a theoretical tension over whether traditional organised crime groups are likely to involve themselves in cybercrime. On the one hand, if there were new opportunities to make money, one would expect traditional organised crime groups to take advantage of them. On the other hand, these groups may be satisfied by sufficient opportunities in their existing activities and do not need to engage in cybercrime, or else there is a technical barrier which may prevent them from doing so (p. 257). This technical barrier is an important point. Despite popular perceptions of global criminal masterminds, many mafia members are “street guys” who specialise in violence and toughness and are far from worldly, often having tight links to their local neighbourhoods (Pistone, 1987). While technology is becoming increasingly widespread and is now likely being used by certain organised crime members (especially the younger generations), the inherently localised nature of much organised crime should not be forgotten (Reuter, 1983; Varese, 2011).

As a result, rather than a broad takeover, it would be expected that organised crime might be involved in cybercrime in quite specific ways that match its existing nature: 1) Organised crime groups might provide protection to local cybercriminals who operate on their turf. Like any other criminals, if cybercriminals make large sums of money they may become vulnerable to theft/extortion. If they are collaborating in their enterprises with other local (cyber)criminals, they may also require arrangements to be enforced by a “trustworthy” local mobster. 2) Organised crime groups might invest in certain cybercriminal schemes. 3) They may also use their traditional expertise in money laundering and their ability to physically enforce group
arrangements as service providers to, or partners of, broader cybercrime operations. The money side of cybercrime often requires offline groups of people to collect/withdraw/send money or buy merchandise with stolen proceeds, which benefits from monitoring. 4) Such organised crime groups may also get involved as the guiding hand of scams, by hiring those with technical skills to carry out certain jobs, such as the Citibank hack or the Sumitomo bank heist (Jordan and Taylor, 1998: 3-4; Bowcott, 2009). These last two alternatives are really two sides of the same coin, depending on whether those with technical skills approach the organised crime groups to assist with “cashing out”, or whether the organised crime groups look to bring in technical talent for their own scam. Sometimes it may be difficult to tell which is the case.

While evidence may exist for the other three roles, interviews with former cybercriminals have provided some support for the fourth category. In his later life as a security professional, Akmal has been approached by a number of people seeking his services, which he regularly turns down. In one case a local drug dealer connected to a major syndicate was interested in hiring him to gather intelligence on specific individuals (most likely competitors) by hacking them (Author, 2014a). Casper, a Western European hacker, was convicted for his activities and later released. Not long afterwards, he was approached by what he called “real criminals, very big criminals”. The criminals flew in to meet Casper and treated him very well in the hopes of wooing him to become involved in their criminal activities, including a major jewellery heist in Europe, where he was to hack the alarm system of the target site. Casper politely declined the proposal (Author, 2014b). Elsewhere in Western Europe, a similar story was recounted by former hacker Jeremy who was approached by a woman seeking his services for a job, but who he suspected may have been an
undercover agent of one kind or another (Author, 2011b).

While these examples provide some evidence for the involvement of traditional organised crime in cybercrime (or at least the recruitment of cybercriminals into organised crime activities), one must remain cautious. A number of other former cybercriminals and hackers maintained that in many cases of cybercrime there is no clear involvement of traditional organised crime groups (Author, 2011a; Author, 2012a; Author, 2015a; Author, 2015b; Author, 2012b) As noted above, there is also a lack of strong evidence in the existing literature. New data may emerge and/or the role traditional organised crime plays in cybercrime may increase, but at this stage it is important not to overstate the phenomenon as a complete “takeover” of any kind.

**Conclusion: Is There Honour Among (Cyber)thieves?**

This paper has outlined the role that four key mechanisms play in enhancing cooperation among cybercriminals: reputation; appearance; performance; enforcement. Each finds support in the literature and interviews in making an important contribution to cybercriminal collaboration. But some elements appear to hold a more significant place in the cybercriminal underground than others. In online interactions, reputation finds the most support as a meaningful mechanism. It is mentioned time and again by interview subjects (Author, 2012a; Author, 2015-2016; Author, 2015b; Author, 2015a). In offline interactions, enforcement appears to be the key mechanism, as increased opportunities for monitoring and threatening physical violence become available. In fact, this enhanced enforcement mechanism helps explain the curiosity of why certain cybercriminals might engage in offline activities and not capitalise on the advantages of anonymity online.
But even with the successes of these mechanisms, it is important not to overstate their role. They certainly reduce the risk associated with various interactions and transactions, but some risk will always remain (Author, 2016; Author, 2015c). As noted in the introduction, this is true for conventional offline criminals (Gambetta, 2009; Reuter, 1983; Campana and Varese, 2013), as it is for all members of society. It is not surprising that these mechanisms do not entirely solve the cooperation problem for cybercriminals. For instance, online, the reputation mechanism is susceptible to one major flaw: those who build up a good reputation for a long period of time, but then wait to commit a scam so large that it justifies burning that nickname (Author, 2015a). It would also be naïve to assume that forum officers are intrinsically beyond repute. Some administrators might act in petty ways or “turn bad” and become corrupt, accepting money in return for certain members breaking rules (Author, 2015b). The offline dimension will also not lead to complete trust. For instance, in cases where traditional (organised) criminals work with technical actors, a key monitoring challenge will emerge. It would seem that there would be plenty of opportunities for electronic fraud by a technically skilled operator. In the reverse direction, talented but naïve computer technicians might find themselves in a vulnerable position when dealing with hardened street criminals.

Ultimately, mechanisms can improve the situation, but some risk always remains. Nonetheless, cybercriminals continue to operate. The simple reason for this is that they can still make money, even accounting for the downsides of the industry. Scott believed that the “bottom line is you are always taking a bit of a risk or gamble, but when you do finally get a good team together, you keep it as long as you can” (Author, 2015b). Lance was a little more forthright: “you got ripped off…? Guess what, you’re in the business of stealing money, you’re going to get ripped off. Suck it
up and carry on with your business” (Author, 2015a). As long as the risks are managed to an acceptable level and the potential gains are deemed to outweigh the danger, cybercriminal cooperation will continue and there will remain some honour among thieves.
Bibliography


Author. (2011a) Interview with Former Western European Cybercriminal 1.
Author. (2011b) Interview with Former Western European Hacker 1.
Author. (2012a) Interview with Former Expatriate Cybercriminal Based in Southeast Asia 1.
Author. (2014a) Interview with Former Southeast Asian Cybercriminal 1.
Author. (2014b) Interview with Former Western European Cybercriminal 2.
Author. (2015a) Interview with Former North American Cybercriminal 2.


Lusthaus J. (2013a) Call Me i$Hm@eL. *Pacific Standard* (Nov/Dec).


