JONATHAN LUSTHAUS

Honour Among (Cyber)thieves?

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 has emerged. The purpose of this paper is to address this puzzle in relation to profit-driven cybercrime. It draws on a collection of interviews with former cybercriminals 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.

THIS PAPER addresses the increasing degree of cooperation among profit-driven cybercriminals. The early hackers of the 1960s, whose central motivation was intellectual curiosity, have now been joined in large numbers by those seeking profit. Among these financially motivated cybercriminals, business is thriving [EC3 2014: 11]. They are professional and organised, leaving behind the stereotype of the lone teenage hacker as the fundamental model of a cybercriminal [Ablon, Libicki, and Golay 2014: ix; EC3 2014: 19]. Illicit enterprises now range enormously in scope from identity theft and fraud to blackmail and extortion to intellectual property violations and spam among others. The offenders involved in cybercrime are increasingly specialised [Ablon, Libicki, and Golay 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

Jonathan LUSTHAUS, University of Oxford [jonathan.lusthaus@sociology.ox.ac.uk]

European Journal of Sociology, 59, 2 (2018), pp. 191–223—0003-9756/18/0000-900$07.50per art + $0.10 per page
©*European Journal of Sociology* 2018. doi: 10.1017/S0003975618000115

https://doi.org/10.1017/S0003975618000115 Published online by Cambridge University Press

shelf" malware, "social engineer" victims and provide "cashing out" services that can convert virtual loot into offline funds.

While some collaborations are fleeting, others are entrenched and last for a number of years. In some parts of the globe "cybercriminal businesses" have even emerged, operating out of physical office space with pseudo-corporate structures [Lusthaus 2014]. Some of the largest known cybercriminal enterprises have included the St Petersburg hosting provider, the Russian Business Network, and the 50-employee company, Liberty Reserve, which operated a virtual currency widely used by cybercriminals out of a business park in Costa Rica [Graham 2009: ch. 5; Halpern 2015]. Beyond persistent cybercriminal teams and businesses, forums are another structure that commonly lasts for a period of years. These 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 or stolen credit card data, and offer their services for hire, such as hacking or renting out a "botnet"[1] [Holt and Lampke 2010; Décary-Hétu and Dupont 2013]. These marketplaces play an important role in the underground economy, by providing online hubs around which disparate actors coalesce, and where they can trade, network and learn.

A sociological approach is well suited to the study of cooperation among cybercriminals. 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: the profiles of cybercriminals, how they are organised, and how they operate. While still at the niche level, there is now a growing social science literature on the subject [see, for example, Grabosky 2001; Wall 2007; Décary-Hétu and Dupont 2012; Hutchings 2014]. But a number of issues still require greater study, not least how cybercriminals cooperate with each other in the anonymous, and inherently low-trust, environment of online crime, which has found only rare mention in the literature [Dupont 2014; Yip, Webber and Shadbolt 2013; Dupont *et al.* 2016; Hardy and Norgaard 2016]. This subject is important not only to comprehending the still somewhat mysterious world of cybercrime but should also be

[1] 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.

https://doi.org/10.1017/S0003975618000115 Published online by Cambridge University Press

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.

For cybercriminals the anonymity of the Internet creates further challenges on top of those facing conventional criminals, who must partner with other criminals outside the state's enforcement systems. In an online setting, the cooperation problem becomes more acute. It is difficult to assess trustworthiness and enforce agreements when one does not even have physical interactions, which would normally indicate the identity of partners. Furthermore, even if one did manage to identify one's 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 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, Clayton and Anderson 2009]. The fieldwork on which this article is based further confirmed the industrial nature of cybercrime, with a strong degree of specialisation and professionalization, along with the presence of firm-like structures and mature markets.

The purpose of this paper is to address this puzzle of how profit-driven cybercriminals have managed to overcome their trust problem in order to achieve fairly wide-scale cooperation. In so doing, it will apply established theory on trust and cooperation to cybercrime, an approach that has not been widely employed in the existing literature. The focus of the paper is on profit-driven cybercrime. The first section of the article will introduce the key theory necessary to address this question. The second section addresses the approach and methods employed in this study. Emerging from the discussion of theory, the following four sections will each address one mechanism that enhances cooperation and explain how it applies to profit-driven cybercriminals. The seventh section will address the role that offline interactions may play in cybercriminal cooperation. This is a somewhat counterintuitive aspect of cybercrime and is often overlooked in many studies. However, it may provide a vital piece of the puzzle. The final section addresses failures of cooperation.

https://doi.org/10.1017/S0003975618000115 Published online by Cambridge University Press

Theoretical Background

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; they often do not have access to reliable information on goods and services; they find it difficult to freely advertise illicit wares; and they 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 the way in which 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, 2009; Varese 2001; Skarbek 2011; Levi 2008; Reuter 1983; Wang 2011].

Drawing inspiration from these approaches, this section outlines some relevant theory on trust and cooperation that would be equally useful in making sense of cybercrime. Coming out of this tradition, it seems 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 choice of action when that action must be chosen before one can *monitor* the actions of those others" [51]. In a similarly influential formulation Coleman [1990] sees the phenomenon as:

> 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 [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 better assess trustworthiness, 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. 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

https://doi.org/10.1017/S0003975618000115 Published online by Cambridge University Press

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 that have not been 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 or not to trust them. For instance, if a certain cybercriminal's reputation is tarnished, the cybercriminal in question can abandon his/her nickname and use a different handle. In addition, physical enforcement becomes very difficult when dealing with unknown parties, who may also be operating from a distant jurisdiction.

https://doi.org/10.1017/S0003975618000115 Published online by Cambridge University Press

Following the methods section, the remainder of this paper examines the mechanisms cybercriminals employ to address these challenges and enhance cooperation. Mechanisms, in this case, are those processes that reduce the risks for cybercriminals in collaborating with each other. In terms of assessing trustworthiness, there are three conventional mechanisms that likely apply: *reputation, appearance* and *performance* [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 next 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.

Approach and Methods

The approach undertaken in this paper is exploratory and qualitative. It is best viewed as a pilot study attempting to make sense of a topic on which reliable data is extremely scarce. It does not seek to present a formal model or hypotheses to be tested. It does not provide definitive statements and tightly wound deductive reasoning. Instead, it is hoped that it will improve comprehension of the subject and provide groundwork for future studies to be carried out in this area. Much of cybercrime remains uncharted from an academic perspective. It is also a vast world in and of itself. This makes it challenging to identify topics that might warrant investigation and the research design and data that would be appropriate in each case. The contribution of this article should be read as a preliminary, rather than final, statement on cybercriminal cooperation. Without first

https://doi.org/10.1017/S0003975618000115 Published online by Cambridge University Press

shining light on this topic and making small steps forward, further research in either the deductive/explanatory or inductive/interpretivist traditions is much more difficult.

In order to address the research question, a core addition to this body of knowledge will be a collection of semi-structured interviews with former cybercriminals (and one hacker) 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. For instance, analysing data from cybercriminal forums is very much in vogue, but this largely provides only the most outward facing and public interactions of cybercriminals, rather than their individual insights. The interviewed participants include both arrested/convicted and self-identified cybercriminals, and span a variety of jurisdictions. They also range from low-level offenders to the highest echelons. Some are technical offenders with significant hacking or coding ability; others conform more to a fraudster profile and played an important role in "cashing out". Most were involved in popular forms of financially motivated cybercrime, such as credit card fraud or compromising bank accounts, along with data theft and spam. Table 1 summarises these interview subjects.

Given the sensitivity of some of the topics and participants involved in this study, anonymity and confidentiality were also fundamental. All the names of participants in this study have been replaced with pseudonyms. I have also attempted to provide only the most essential information about subjects, as cybercrime is still a relatively tight community; some seemingly innocuous details can have a bearing on revealing possible identities.

These subjects were interviewed as part of a larger research project carried out between 2011 and 2017. This study, itself an exploratory investigation, involved fieldwork in 20 countries and included research in key cybercriminal "hotspots" such as Russia, Ukraine, Romania, China, Nigeria, Brazil and the United States. It also included interviews with over 200 law enforcement agents, security professionals and others with a knowledge of cybercrime. While some of the insights contained in this paper are influenced by this fieldwork, for the purpose of brevity, the focus of this paper is on the most valuable of the collected data: interviews with former offenders. Almost all of these participants were accessed over the course of the study through purposive sampling. Considerable time and effort was required to identify and then locate/contact these former offenders through open source information. While a number of interviews were collected

https://doi.org/10.1017/S0003975618000115 Published online by Cambridge University Press

Table I
Interviews of Former Cybercriminals

No.	Alias	Description	Type/min.sec
I-1	Jeremy	Former Western European Hacker 1	In Person/38.56
I-2	Sean	Former Western European Cybercriminal 1	In Person/73.01 and Written Communication
I-3	Dave	Former Expatriate Cybercriminal Based in Southeast Asia 1	In Person/68.22
I-4	Noah	Former North American Cybercriminal 1	In Person/37.25
I-5	Ahmed	Former Southeast Asian Cybercriminal 1	Phone/Unrecorded Interview
I-6	Casper	Former Western European Cybercriminal 2	In Person/43.56
I-7	Scott	Former North American Cybercriminal 2	Written Communication
I-8	Claudiu	Former Eastern European Cybercriminal 1	In Person/Informal Discussion
I-9	Lance	Former North American Cybercriminal 3	Phone/50.47
I-10	Don	Former North American Cybercriminal 4	Written Communication
I-11	Andrey	Former Eastern European Cybercriminal 2	Written Communication
I-12	Jim	Former North American Cybercriminal 5	Written Communication

(Continued)

https://doi.org/10.1017/S0003975618000115 Published online by Cambridge University Press

Table I (Continued)

No.	Alias	Description	Type/min.sec
I-13	Ivan	Former Eastern European Cybercriminal 3	Written Communication
I-14	Mohammed	Former Middle East and North African Cybercriminal 1	Written Communication
I-15	Tan	Former Southeast Asian Cybercriminal 2	Written Communication
I-16	Thiago	Former South American Cybercriminal 1	In Person/ Unrecorded Interview

through field visits, some interviews were carried out by phone (or online equivalents), or through written communications (letters, emails and other messaging platforms). The paper also draws on existing empirical studies, which often rely on data from online cybercriminal trading forums, along with legal documents and other open source materials.

Reputation

The next four sections address the key mechanisms identified in the theory section: reputation, appearance, performance, and enforcement. To begin with reputation, it is clear that it is central to how cybercriminals assess trustworthiness and engage in cooperation. As one senior security firm officer and former hacker has 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 [I-3].

https://doi.org/10.1017/S0003975618000115 Published online by Cambridge University Press

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 [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 [75]. This suggests that a number of 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: "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" [I-7]. Writing about his dealings with collaborators, former Eastern European cybercriminal Ivan addressed matters in a Schelling-like way:

> After first couple of deals are done, that is where the trust is beginning to grow. So, if you have done successful deals with a person in the past, then it is unlikely that he will disappear after another one—it is just not in his best interest; it will not going to make any sense, because he will make more money by continuing doing business with you, than by ripping you off. So, growth of trust is based on analysis of a person's egoistic motives [I-13].

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

https://doi.org/10.1017/S0003975618000115 Published online by Cambridge University Press

anonymous), but to their online nickname or handle. As another former Eastern European cybercriminal Audrey wrote:

> For many nickname is a "brand," so when you choose it, it means a lot. It is even more so, if one elects to promote his services or sell proceeds of his activity. In such case his fame, reputation and standing relation is all dependent on his nickname [I-11].

As a brand, 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 they can to reduce security threats [I-11]. At the other are individuals who value their reputation over any risk, keeping the same handle for their entire career. 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" [I-3]. 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 [I-2, I-6].

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: 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

https://doi.org/10.1017/S0003975618000115 Published online by Cambridge University Press

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" [I-7]. To help the referral process, cybercriminals also list potential referees when introducing themselves on forums and elsewhere to allow others to vet them. 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 [I-7].

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 is 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 (perhaps indicative of interest in doing business). In his case, Ivan talked about the strong importance of such reputation measures in choosing a programmer to work on a project for him [I-13].

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]. 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 have formal ranks, such as "trusted members" among others, if users prove their "criminal credentials to the administrator

https://doi.org/10.1017/S0003975618000115 Published online by Cambridge University Press

and moderators".[2] 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 [I-7, I-14]. 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 in lowering 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 reputation systems [Dellarocas 2003; Resnick and Zeckhauser 2002; Diekmann, Jann and Wyder 2009]. But there are also parallels between reputational systems on forums and offline historical examples from entirely different contexts [Milgrom, North and Weingast 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; before engaging in a deal, traders would enquire with a private judge about their potential partner's reputation [Milgrom, North and Weingast 1990]. Cybercriminal forum reputational mechanisms like reviews, naming and shaming sections, and numerical indices 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:

[2] *R v. Kelly and Others* [Case Summary], Southwark Crown Court, 2011: 35.

https://doi.org/10.1017/S0003975618000115 Published online by Cambridge University Press

> 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 easier… [I-2].

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 cannot be changed (or can be changed only with difficulty), 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, and time spent online.[3]

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 who 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 PMs etc."[4] 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 else untoward was going on [I-7]. 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

[3] While beyond the scope of this paper, it is possible to view issues of cybercriminal appearance through a signaling theory framework: Lusthaus 2012; Décary-Hétu and Leppänen 2013.

[4] "PM" is short for private message.

https://doi.org/10.1017/S0003975618000115 Published online by Cambridge University Press

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 [I-7, I-9, I-11]. However, 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 [I-2].

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. Some cybercriminals might even pretend to be from Eastern Europe, trying to appropriate their good reputation in the industry [I-7]. This was the case with Albert, 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 accidently happen upon. A user who is present in one

https://doi.org/10.1017/S0003975618000115 Published online by Cambridge University Press

of these places has to have at least some degree of knowledge and connections to be there in the first place [I-3].

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 and attached to a specific nickname or profile, the more time one has invested. The greater the investment of time, the less likely one is to jeopardise it, and so the more trustworthy that person appears [I-13]. A number of forums list the starting date for each user on their profile, which demonstrates how long they have been around. Another more abstruse 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" [I-2]. 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

https://doi.org/10.1017/S0003975618000115 Published online by Cambridge University Press

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 [I-9, I-13, I-14]. 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, Webber and Shadbolt 2013: 528]. Some might also advertise their verified status from other forums that they might be on, as a means of attracting more business.

Some of the performance checks employed by cybercriminals do not 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. 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). In such cases, it was important to ask a suitable "verification question". This 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 [I-7].

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. Don, who was a leading player in the underground, wrote:

https://doi.org/10.1017/S0003975618000115 Published online by Cambridge University Press

> The only consistent manner of uncovering American law enforcement is to get them to do something that they and their turned individuals cannot do. Usually in the USA this means getting them to hack a site, or abuse some piece of information that you know is an innocent third-party. I have often seen undercovers pretend to provide dumps in or other resources but those were actually bogus accounts set up as part of an agreement with the bank, so the account was really not owned by a person, and therefor didn't break laws—they were giving away their own credit cards, basically [I-10].

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 have only limited enforcement options available when operating independently of online institutions like forums. In contrast to 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 by 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].

Other forms of cybercriminal enforcement have also been 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

https://doi.org/10.1017/S0003975618000115 Published online by Cambridge University Press

most treasured possession of any self-respecting cybercriminal. Scott provided an example of a leading cash out expert who miscalculated by underpaying his supplier. This led to his being banned from his IRC channel and a link going up that published his picture, name, address, phone number, and account numbers. He was arrested shortly after this occurred. The seriousness of this form of punishment is clear: not only does it lead to embarrassment/violation, it also allows other actors online to make use of the posted information and engage in further violations against the target. 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 professional doxing services also exist [I-7]. "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 underway [Krebs 2013].

Forums formalise and extend aspects of the enforcement mechanism to keep cybercriminals in line. One former cybercriminal, Mohammed, even described the way forums enforce rules as a "state of legit hackers" [I-14]. In these settings, 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; I-2]. 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].[5] 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 [I-7, I-11, I-12, I-14]. As a result of this process, punishments are meted out, with exclusion being relatively common [Holt and Lampke 2010: 44].

Finally, forums also make use of escrow to directly enforce agreements [I-9, I-10, I-15]. 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.

[5] See also *US v. Andrew Mantovani and Others*, United States District Court, New Jersey, 2004 [indictment].

https://doi.org/10.1017/S0003975618000115 Published online by Cambridge University Press

Guarantors can require payment, often in the form of a percentage, but do not always do so [Yip, Webber and Shadbolt 2013: 14; Holt 2013a: 173].

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 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 [I-7].[6]

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" [I-9]. 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. A relatively large number of cybercriminals appear to have significant offline

[6] One weakness that may have become apparent to cybercriminals in recent years is that even administrators with a good reputation may become vulnerable to arrest by law enforcement and turn undercover informant. With thanks to Benoit Dupont on this point.

https://doi.org/10.1017/S0003975618000115 Published online by Cambridge University Press

interactions and operations in running their business [see also Lusthaus and Varese 2017; Leukfeldt *et al.* 2017]. For instance, Albert had a number of associates that he operated with in person, both for business and socialising. One of their main activities was driving past or positioning themselves near the WIFI signals of major "big box" stores in order to access their networks and steal credit card information [Verini 2010]. Two former Eastern European cybercriminals I interviewed suggested that there have been cybercrime "teams" physically working together on specific projects within the region [I-11, I-13]. While some teams are short-lived, certain groups can last for a number of years, particularly when built around a founder and a geographical hub [I-11]. The most obvious case of an offline organisation that has developed with the rise of cybercrime is the cash out crew. By virtue of the physical nature of the work, often involving making purchases from shops with counterfeit cards or withdrawing money from ATMs, it is not surprising that a number of such offenders are known to each other [I-10]. But, as noted in the introduction, some examples begin to approximate illicit technology companies, even with physical office space. This has been observed with regard to malware exploitation groups [Ragan 2012], spam operations [Krebs 2014], virtual currencies used by cybercriminals,[7] and bulletproof hosting providers [Graham 2009: ch. 5]. In the Romanian town of Râmnicu Vâlcea, online fraud has become somewhat of an offline local industry [Bhattacharjee 2011; Lusthaus and Varese 2017].

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 [I-9]. 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 [I-2, I-5, I-7, I-9, I-11, I-15, I-16]. Generally it was considered sensible to meet only with partners one was quite sure were not law enforcement agents [I-9]. The most famous offline meetings between cybercriminals 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].

[7] *US v. Liberty Reserve S.A. and Others*, United States District Court, Southern District of New York, 2013 [indictment].

https://doi.org/10.1017/S0003975618000115 Published online by Cambridge University Press

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, 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 was the provision of 10,000 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" [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

https://doi.org/10.1017/S0003975618000115 Published online by Cambridge University Press

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 could not be directly monitored and it might leave a digital trail [I-5]. For the former South American cybercriminal, Thiago, the process of meeting online partners in person was a gradual one. Collaborators first get to know each other online. Then they begin to share personal information and, when trust has developed, money might become involved. Thiago's description of eventually meeting in the flesh closely matched the concept of hostage exchange: if there is a betrayal, "he goes to gaol too" [I-16].

The enforcement mechanism might also apply to cybercriminal groupings that evolve out of existing offline relationships. Just as kinship could act as an effective information hostage [Campana and Varese 2013], working with known people could also enhance co-operation. 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, and death. Such enforcement mechanisms coupled with a knowledge of offline identities is likely to lower the risk associated with defections in cybercriminal dealings. Such 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 [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, where there is a distinct lack of data and a number of loose claims [as argued by Wall 2014; McCusker 2006; Lavorgna 2015; for a rare empirical study see Leukfeldt *et al*. 2016].[8] This lack of knowledge is unfortunate as the issue of the potential involvement of organised crime is very

[8] On the issue of whether online cybercriminal groupings could classify as organised crime groups, see Lusthaus 2013.

https://doi.org/10.1017/S0003975618000115 Published online by Cambridge University Press

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 cybercriminal governance. Cybercrime would not offer much that is 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 without seeing the need to engage in cybercrime, or else there is a technical barrier which may prevent them from doing so [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 against theft, extortion or disputes to local cybercriminals who operate on their turf. 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) Organised crime groups may also get involved as the guiding hand of schemes, 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: 759-760; Bowcott 2009]. These last two alternatives are really two sides of the same coin: either those with technical skills approach the organised crime groups to assist with "cashing out", or the organised crime groups look to bring in technical talent for their own scams. Sometimes it may be difficult to tell which is the case.

https://doi.org/10.1017/S0003975618000115 Published online by Cambridge University Press

While evidence may exist for the other three roles, interviews with former cybercriminals have primarily provided 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 [I-5]. Casper, a Western European cybercriminal, became publicly known as a talented hacker. He was then 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 [I-6]. 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 [I-1].

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), it is necessary to 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 [I-2, I-3, I-4, I-7, I-9, I-13, I-16]. Audrey believed that there were some connections between organised crime and cybercrime in Eastern Europe, but that this was often just part of life in the region:

> All the relations between traditional mafia and gangs are eventual and personal, so there's no more connections than in any other industry or enterprise. Some individuals do, and if they do, they use it. Others don't. There are various individuals with different backgrounds, some came from "IT" world to carding, other from world of crime. Of course, regular criminals show interest in certain aspects of cybercrime, but they show interest in many other things. More advanced carders and hackers, however, usually show strong disgust to "traditional" criminals and usually join whatever cause there might be on temporary basis. In turn, "traditional" criminals often regard cybercriminals as "milk cows" and nerds [I-11].

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. Instead, while beyond the scope of this article, it is possible that cybercrime connections to corruption rather than organised crime may prove a more fruitful angle for future research in this area.

https://doi.org/10.1017/S0003975618000115 Published online by Cambridge University Press

Failures of Cooperation

Before concluding, one final point is worthy of addressing. If one wishes to study the presence of a phenomenon—in this case cybercriminal cooperation—one should also examine instances where that phenomenon is absent—failures of cooperation.[9] The mechanisms discussed in this paper certainly reduce the risk associated with various interactions and transactions, but some risk will always remain [I-9, I-12]. Given that some degree of defection still takes place in largely transparent societies, 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 [I-9]. 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 [I-7]. 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 many 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.

Nonetheless, many failures of cooperation support rather than challenge the framework discussed in this paper. Breaches of trust often occur when one side fails to adequately assess risk and take steps to reduce it. For instance, Scott was scammed when he did not appropriately monitor and keep logs on a previously trusted partner. As such, he could not prove the malfeasance to anyone [I-7]. Ivan, a leading Eastern European cybercriminal involved in developing malware suggested that his failure in dealing with offline partners was due to the "Incompetence and unreliability of people. Or, better to say, my inability to detect them" [I-13]. Such instances are not a failure of the mechanisms, but rather a failure in their application; the framework itself is not challenged. In fact, in some ways these failures compound the importance of these mechanisms.

[9] Some might regard this as avoiding selection on the dependent variable (see King, Keohane, and Verba 1994: 129-137).

https://doi.org/10.1017/S0003975618000115 Published online by Cambridge University Press

Despite occasional miscalculations, cybercriminals will continue to operate as long as they can still make money from the business. Former cybercriminal Jim wrote a very simple and direct answer to the question of why cybercriminals engage in the business when facing risks of scams or arrest: "$, Greed." While noting that it was "not a very trusting business," he suggested that "I guess what most people do is try to find a few people they can work with and just stick with them" [I-12]. Lance was equally 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" [I-9]. 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.

Summary and Conclusion

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 interviews and broader literature 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. In offline interactions, enforcement appears to be a more important mechanism, as increased opportunities for monitoring and threatening physical violence become available. In fact, this enhanced enforcement mechanism helps explain the curious phenomenon of why certain cybercriminals might engage in offline activities and not capitalise on the advantages of anonymity online.

Table 2 below summarises the presence of these various points in the interviews. In this case, as it cannot be cited directly, the one informal discussion has been removed from the sample to make a total of 15. The first four elements relate only to online activity, with the offline code providing a distinct point of comparison for that component.

While the table appears to confirm the pre-eminence of reputation and the widespread role that the offline dimension plays in cybercrime, some riders should be noted. The data are exploratory semi-structured interviews and therefore largely suggestive. As this is not

https://doi.org/10.1017/S0003975618000115 Published online by Cambridge University Press

TABLE 2
Data Summary

Codes	*Number of Interviews*
Trustworthiness	
Reputation	14
Appearance	7
Performance	10
Enforcement	11
Offline	12

a standardised survey, both the questions and responses in each interview can vary, often requiring some interpretation as to which categories the data supports. In addition, just because an element was not mentioned in an interview does not mean it might still not have been present in that case. This table also does not account for the relative importance that each participant placed on each category, but merely captures the relevance (or not) of each element to their own past activities or to other cybercriminals that they were aware of. Nonetheless, it is broadly supportive of the claims made throughout this paper.

As to the conclusion of this article, one might wonder if there is much difference between the way in which cybercriminal cooperation functions compared to traditional crime. One might even wonder if there is much difference between cybercriminal cooperation and non-criminal cooperation. This is not a limitation in the findings of this article, but rather one of its primary outcomes. Cybercrime is perhaps not as mysterious and unknowable as it sometimes appears—a myth that some perpetuate. The fact that this case does not challenge major sociological assumptions suggests that it might be comprehended through existing frameworks (both with regard to cooperation and broader topics). Ultimately, cybercriminals are people and they are susceptible to being studied. Technical elements in their activities should not deter social scientists from the important role they need to play in comprehending these actors and their organisation. This paper suggests that sociologists and others do not need to reinvent the wheel in order to do this. While new data and methods may add something to the analysis, the discipline should not forget that it already has numerous theoretical and methodological tools at its disposal to undertake this task and further uncover this hidden world. As a preliminary study, this paper has merely scratched the surface of

https://doi.org/10.1017/S0003975618000115 Published online by Cambridge University Press

cybercriminal cooperation. Further studies could assemble a much larger pool of interview data on cybercrime offenders to confirm or dispel particular suppositions. They could also investigate, for instance, the level of variation as to when some cybercriminals choose to use particular mechanisms, or if the use of particular mechanisms varies by nationality or by role in the industry. Beyond cybercriminal cooperation, an almost endless domain of research topics awaits curious scholars.

Acknowledgements

This paper could not have been written without the participants generously sharing their time and knowledge. The author thanks Paolo Campana, Heather Hamill, Alice Hutchings and Benoit Dupont for their helpful comments on various iterations of this article. This paper derives from doctoral research in the Department of Sociology at the University of Oxford, which was only possible through the support of the Clarendon Fund and Nuffield College. The John Fell Fund and Nuffield College also provided funding for various field trips that were required as part of the study. The broader support of the Commonwealth Bank of Australia for the Human Cybercriminal Project is also sincerely acknowledged. Finally, Federico Varese provided expert supervision for this research, and it has been greatly enhanced by his insights and commitment.

BIBLIOGRAPHY

Ablon Lillian, Martin C. Libicki and Andrea A. Golay, 2014. *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar* (Santa Monica, Rand).

Abreu Dilip, 1988. "On the Theory of Infinitely Repeated Games with Discounting", *Econometrica*, 56 (2): 383-396.

Axelrod Robert, 2006. *The Evolution of Cooperation* (New York, Basic Books).

Bhattacharjee Yudhijit, 2011. "Welcome to Hackerville: The Romanian Cybercriminal Hotspot", *Wired*, Last Modified Febr. 7 2011, accessed January 12 2016. http://www.wired.co.uk/magazine/archive/2011/03/features/welcome-to-hackerville.

Bowcott Owen, 2009. "International bank raiders foiled by form-filling", *The Guardian*, Last Modified March 4, accessed April 3. http://www.theguardian.com/uk/2009/mar/04/sumitomo-fraud-attempt.

Campana Paolo and Federico Varese, 2013. "Cooperation in Criminal Organizations: Kinship and Violence as Credible Commitments", *Rationality and Society*, 25 (3): 263-289.

Coleman James, 1990. *Foundations of Social Theory* (Cambridge, Mass and London, Belknap Press of Harvard University Press).

Cook Karen, Chris Snijders, Vincent Buskens and Coye Cheshire, eds. 2009. *eTrust: Forming Relationships in the Online World* (New York, Russell Sage Foundation).

Dasgupta Partha, 1988. "Trust as a Commodity", *in* D. Gambetta, ed., *Trust: Making and Breaking Cooperative Relations* (Oxford, Basil Blackwell: 49-72).

Davies Caroline, 2010. "Welcome to DarkMarket—Global One-Stop Shop for Cybercrime and Banking Fraud", *The Guardian*, Last Modified January 14 2010, accessed August 1 2011. http://www.guardian.co.uk/technology/2010/jan/14/darkmarket-online-fraud-trial-wembley.

Décary-Hétu David and Benoit Dupont, 2012. "The Social Network of Hackers", *Global Crime*, 13 (3): 160-175.

—, 2013. "Reputation in a Dark Network of Online Criminals", *Global Crime*, 14 (2-3): 175-196.

Dellarocas Chrysanthos, 2003. "The Digitization of Word-of-Mouth: Promise and Challenges of Online Feedback Mechanisms", *Management Science*, 49 (10): 1407-1424.

Diekmann Andreas, Ben Jann and David Wyder, 2009. "Trust and Reputation in Internet Auctions", *in* K. Cook, C. Snijders, V. Buskens and C. Cheshire, *eTrust: Forming Relationships in the Online World* (New York, Russell Sage Foundation: 139-165).

Dixit Avinash, 2004. *Lawlessness and Economics: Alternative Modes of Governance* (Princeton and Oxford, Princeton University Press).

Drömer Jan and Dirk Kollberg, 2012. *The Koobface Malware Gang Exposed* (Abingdon, Sophos).

Dupont Benoit, 2014. "Skills and Trust: A Tour Inside the Hard Drives of Computer Hackers", *in* C. Morselli, ed., *Crime and Networks* (New York, Routledge: 195-217).

Dupont Benoît, Anne-Marie Côté, Claire Savine and David Décary-Hétu, 2016. "The Ecology of Trust among Hackers", *Global Crime*, 17: 129-151.

EC3, 2014. *The Internet Organised Crime Threat Assessment* (The Hague, Europol).

Gambetta Diego, 1993. *The Sicilian Mafia: The Business of Private Protection* (Cambridge and London, Harvard University Press).

—, 2009. *Codes of the Underworld: How Criminals Communicate* (Princeton and Oxford, Princeton University Press).

Gibbons Robert, 2001. "Trust in Social Structures: Hobbes and Coase Meet Repeated Games", *in* K. Cook, *Trust in Society* (New York, Russell Sage Foundation).

Glenny Misha, 2011. *DarkMarket: CyberThieves, CyberCops and You* (London, Bodley Head).

Grabosky Peter, 2001. "Virtual Criminality: Old Wine in New Bottles?", *Social & Legal Studies*, 10 (2): 243-249.

Graham James, ed. 2009. *Cyber Fraud: Tactics, Techniques, and Procedures* (Boca Raton, CRC Press).

Granovetter Mark, 1985. "Economic Action and Social Structure: The Problem of Embeddedness", *American Journal of Sociology*, 91 (3): 481-510.

Greif Avner, 1989. "Reputation and Coalitions in Medieval Trade: Evidence on the Maghribi Traders", *Journal of Economic History*, 49 (4): 857-882.

Halpern Jake, 2015. "Bank of the Underworld", *The Atlantic*, accessed May 15 2017. http://www.theatlantic.com/magazine/archive/2015/05/bank-of-the-underworld/389555/. Date?

Hardin Russell, 2001. "Conceptions and Explanations of Trust", *in* K. Cook, *Trust in Society* (New York, Russell Sage Foundation: 3-39).

Hardy Robert and Julia Norgaard, 2016. "Reputation in the Internet Black Market: An Empirical and Theoretical Analysis of the Deep Web", *Journal of Institutional Economics*, 12 (3): 515-539.

Holt Thomas, 2013a. "Examining the Forces Shaping Cybercrime Markets Online", *Social Science Computer Review*, 31 (2): 165-177.

—, 2013b. "Exploring the Social Organisation and Structure of Stolen Data Markets", *Global Crime*, 14 (2-3): 155-174.

Holt Thomas and Eric Lampke, 2010. "Exploring Stolen Data Markets Online: Products and Market Forces", *Criminal Justice Studies*, 23 (1): 33-50.

Hutchings Alice, 2014. "Crime from the Keyboard: Organised Cybercrime, Co-offending, Initiation and Knowledge Transmission", *Crime, Law and Social Change*, 62 (1): 1-20.

Jordan Tim and Paul Taylor, 1998. "A Sociology of Hackers", *The Sociological Review*, 46 (4): 757-780.

King Gary, Robert Keohane and Sidney Verba, 1994. *Designing Social Inquiry: Scientific Inference in Qualitative Research* (Princeton, Princeton University Press).

Klein Benjamin and Keith Leffler, 1981. "The Role of Market Forces in Assuring

Contractual Performance", *Journal of Political Economy*, 89 (4): 615-641.

Krebs Brian, 2013. "The World Has No Room For Cowards", *KrebsonSecurity*, Last Modified March 15 2013, accessed September 22 2015. http://krebsonsecurity.com/2013/03/the-world-has-no-room-for-cowards/.

—, 2014. *Spam Nation: The Inside Story of Organized Cybercrime-from Global Epidemic to Your Front Door* (Naperville, Sourcebooks).

—, 2015. "Arrests Tied to Citadel, Dridex Malware", KrebsonSecurity, Last Modified September 7 2015, accessed November 8 2015. http://krebsonsecurity.com/2015/09/arrests-tied-to-citadel-dridex-malware/.

Kshetri Nir, 2010. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives* (Berlin, Springer).

Lavorgna Anita, 2015. "Organised crime goes online: realities and challenges", *Journal of Money Laundering Control*, 18 (2): 153-168.

Leukfeldt Rutger, Edward Kleemans and Wouter Stol, 2017. "Cybercriminal Networks, Social Ties and Online Forums: Social Ties Versus Digital Ties Within Phishing and Malware Networks", *British Journal of Criminology*, 57 (3): 704-722.

Leukfeldt Rutger, Anita Lavorgna and Edward Kleemans, 2016. "Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime", *European Journal on Criminal Policy and Research*, 23 (3): 287-300.

Levi Michael, 2008. *The Phantom Capitalists: The Organisation and Control of Long-Firm Fraud* (Aldershot, Ashgate).

Lusthaus Jonathan, 2012. "Trust in the World of Cybercrime", *Global Crime*, 13 (2): 71-94.

—, 2013. "How Organised is Organised Cybercrime?", *Global Crime*, 14 (1): 52-60.

—, 2014. "Electronic Ghosts", *Democracy*, Winter, no. 31.

Lusthaus Jonathan and Federico Varese, 2017. "Offline and Local: The Hidden Face of Cybercrime", *Policing: A Journal of Policy and Practice*, published online July 28, 2017.

Mccusker Rob, 2006. "Transnational Organised Cyber Crime: Distinguishing Threat from Reality", *Crime, Law and Social Change*, 46 (4-5): 257-273.

Mell Andrew, 2015. "Promoting Market Failure: Fighting Crime with Asymmetric Information", *Department of Economics Discussion Paper Series* (Oxford, University of Oxford).

Milgrom Paul, Douglass North and Barry Weingast, 1990. "The Role of Institutions in the Revival of Trade: The Law Merchant, Private Judges, and the Champagne Fairs", *Economics and Politics*, 2 (1): 1-23.

Moore Tyler, Richard Clayton and Ross Anderson, 2009. "The Economics of Online Crime", *The Journal of Economic Perspectives*, 23 (3): 3-20.

Motoyama Marti, Damon Mccoy, Kirill Levchenko, Stefan Savage and Geoffrey Voelker, 2011. "An Analysis of Underground Forums", *Internet Measurement Conference 2011*, Berlin, November 2.

Pistone Joseph, 1987. *Donnie Brasco: My Undercover Life in the Mafia* (London, Hodder).

Poulsen Kevin, 2011. *Kingpin* (New York, Crown Publishers).

Ragan Steve, 2012. "Eight Arrested in Moscow After Allegedly Stealing Millions Using Carberp Trojan", *Security Week*, Last Modified March 21 2012, accessed September 25 2015. http://www.securityweek.com/eight-arrested-moscow-after-allegedly-stealing-millions-using-carberp-trojan.

Resnick Paul and Rihard Zeckhauser, 2002. "Trust among Strangers in Internet Transactions: Empirical Analysis of eBay's Reputation System", *in* M. Baye, ed., *The Economics of the Internet and E-Commerce* (Amsterdam, Elsevier Science: 127-157).

Reuter Peter, 1983. *Disorganized Crime: The Economics of the Visible Hand* (Cambridge, Mass; London, MIT Press).

Schelling Thomas, 1980. *The Strategy of Conflict* (Cambridge, Harvard University Press).

Skarbek David, 2011. "Governance and Prison Gangs", *American Political Science Review*, 105 (4): 702-716.

Sztompka Piotr, 1999. *Trust: A Sociological Theory* (Cambridge, Cambridge University Press).

Varese Federico, 2001. *The Russian Mafia: Private Protection in a New Market Economy* (Oxford, Oxford University Press).

—, 2011. *Mafias on the Move* (Princeton and Oxford, Princeton University Press).

Verini James, 2010. "The Great Cyberheist", The New York Times, Last Modified November 10 2010, accessed September 3 2015. http://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html?_r=1.

https://doi.org/10.1017/S0003975618000115 Published online by Cambridge University Press

Wall David, 2007. *Cybercrime: The Transformation of Crime in the Information Age* (Cambridge, Polity).

—, 2014. "Internet Mafias? The Dis-Organisation of Crime on the Internet", *in* S. Caneppele and F. Calderoni, ed., *Organized Crime, Corruption and Crime Prevention* (Cham, Springer: 227-238).

Wang Peng, 2011. "The Chinese Mafia: Private Protection in a Socialist Market Economy", *Global Crime*, 12 (4): 290-311.

Yip Michael, Craig Webber and Nigel Shadbolt, 2013. "Trust Among Cybercriminals? Carding Forums, Uncertainty and Implications for Policing", *Policing and Society*, 23 (4): 516-539.

https://doi.org/10.1017/S0003975618000115 Published online by Cambridge University Press

Résumé

Il est bien connu que les criminels, qui agissent en dehors de la loi et de la protection de l'État, font face à des difficultés particulières pour coopérer, notamment en raison de l'impératif de secret mais également du manque de confiance. Pour les cybercriminels, l'anonymat d'Internet crée des défis supplémentaires, en compliquant tant l'évaluation de la fiabilité que la mise en œuvre des accords. Pourtant, contrairement aux attentes, la collaboration entre les cybercriminels est répandue et une industrie sophistiquée a vu le jour. L'objectif de cet article est de résoudre cette énigme à partir du cas de la cybercriminalité à but lucratif. Il s'appuie sur une série d'entretiens avec d'anciens cybercriminels qui fournissent des données importantes sur leurs micro-interactions le plus souvent secrètes. Il examine quatre mécanismes clés qui permettent d'améliorer la coopération : la réputation, l'apparence, la performance et l'exécution. Il aborde également le rôle rarement discuté, et quelque peu contre-intuitif, que les interactions hors ligne peuvent jouer dans le renforcement de l'action collective parmi les cybercriminels.

Mots-clés : Cybercriminalité ; Coopération ; Confiance ; Gouvernance extra-juridique ; Dimension hors connexion.

Zusammenfassung

Aufgrund der Geheimnispflicht und eines Vertrauensdefizites, arbeiten Kriminelle, die außerhalb der staatlichen Gesetze und deren Schutz handeln, allgemein weniger gern zusammen. Für Cyberkriminelle stellt die online Anonymität eine weitere Herausforderung dar, da sie die Bewertung der Vertrauenswürdigkeit sowie die Vertragsdurchsetzung erschwert. Entgegen aller Erwartungen ist die Zusammenarbeit zwischen Cyberkriminellen weit verbreitet und zu einer hochentwickelten Industrie geworden. Dieses Rätsel soll im Rahmen dieses Beitrags am Beispiel der gewinnbringenden Cyberkriminalität gelöst werden. Gespräche mit ehemaligen Cyberkriminellen liefern hier wichtige Informationen über die meist verschwiegenen Mikrointeraktionen. Vier Schlüsselmechanismen, die die Zusammenarbeit verbessern, werden untersucht: der Ruf, das Erscheinungsbild, die Leistung und die Ausführung. Es wird auch die selten erwähnte Rolle der offline Interaktionen kritisch diskutiert, die nicht intuitiv ist, aber die Zusammenarbeit der Cyberkriminellen fördert.

Schlüsselwörter : Cyberkriminalität; Zusammenarbeit; Vertrauen; außerlegale Führung; offline Elemente.

https://doi.org/10.1017/S0003975618000115 Published online by Cambridge University Press