Conflict Management in Illicit Drug Cryptomarkets

Document Version
Accepted author manuscript

[Link to publication record in Manchester Research Explorer](#)

Citing this paper
Please note that where the full-text provided on Manchester Research Explorer is the Author Accepted Manuscript or Proof version this may differ from the final Published version. If citing, it is advised that you check and use the publisher's definitive version.

Conflict Management in Illicit Drug Cryptomarkets

Authors and affiliations

Carlo Morselli*, Université de Montréal
David Décary-Hétu, Université de Montréal
Masarah Paquet-Clouston, Université de Montréal
Judith Aldridge, University of Manchester

* Centre international de criminologie comparée / School of Criminology
Université de Montréal
C.P. 6128, succursale Centre-ville
Montreal, Quebec
H3C-3J7
Tel: (514) 343-5676
Fax: (514) 343-5650
carlo.morselli@umontreal.ca

Abstract

Illegal drug markets have been described as 'stateless' systems. Drug dealers, moreover, are commonly considered to have a predilection toward the use of violence to resolve disputes arising from dealing activities. While some studies have undermined this popular perception, new trends surrounding the distribution of illegal drugs via online channels (drug cryptomarkets) have shifted the transactional setting from the physical to virtual realm, thus decreasing the likelihood of violent resolution outcomes even further. This article examines conflict management strategies within cryptomarkets by coding discussion forums between vendors and buyers. Violence, as expected, is absent. Strategies more likely reflect alternatives that have been recognized in conflict management research within and beyond illegal market settings: tolerance; avoidance; ostracism; third party intervention; monetary sanctions; negotiation; and threats. The overall setting from which such resolutions emerge is clearly not subject to formal regulations, but our analyses illustrate the multitude of informal social control mechanisms that are consistently at play and which underlie the self-regulatory and communal processes that are firmly in place.

Introduction

Illegal drug markets, in keeping with illegal markets more generally, have been described as 'stateless' settings (Wilkins 2001), leaving participants to resolve their problems and disputes without the benefit of formal mediating agents and guidelines (Reuter 1983; Cooney 1998; Jacques 2010). Without legally binding contractual arrangements afforded by the state, illegal drug markets have been argued to go hand-in-hand with violence. In his tripartite framework, Goldstein (1985, 1997) remains explicit in regard to this association: "violence is intrinsic to involvement with any illicit substance" (Goldstein 1985: 497). This drug-violence nexus is designed around psychopharmacological (violence due to the effects of a drug), economic compulsive (violence enacted when stealing to buy drugs), and systemic (violence because of extra-legal transactional issues) features. While support for the nexus has been found when focusing on the experiences of consumers (see Copes, Hochstetler, and Sandberg 2015), the prevalence and consistency of violence has been less clear-cut when examining the supply side of illegal drug trafficking settings.

Some researchers construe violence as a social phenomenon, even before considering the selling of drugs specifically. Violence, in this sense, pervades all spheres of a drug dealer's life. Sommers and Baskin (1997) consider that the violence of drug sellers stems not from the distribution of drugs, but rather from the drug underworld that provides a context that favours the use of violence within a larger social environment. Pearson and Hobbs (2001: 41) concur: "many of those featuring prominently in middle market drug dealing networks bring with them prior reputations for violent action", with some drug trade participants predisposed to violence even before becoming involved in drug selling. Support for this perspective is demonstrated by the finding that certain drug markets, such as those dealing in cocaine or crack, are more violent than other illegal drug markets (Fagan and Chin, 1990; Johnson, Golub and Fagan, 1995), suggesting that it is not marketplace illegality *per se* that deterministically creates violence. Moreover, we find considerable variation in violence connected to drug trafficking across countries, with recent increases (e.g. Mexico) and decreases (e.g. Colombia) in violence not simply linked to the existence and persistence of trafficking in these locations (Duran-Martinez 2015).

For others, the place of violence in illegal drug settings has been largely overstated. Reuter (2009) has stressed that illegal drug markets are relatively peaceful. Violence has been found to be a last resort, with general consensus identifying the importance of the multiple alternatives to violence employed by drug market actors (Meeson and Morselli, 2012). Contrary to the leading assumption underlying Goldstein's framework, Jacques and Wright (2008: 222-223) argue that violence "is not an invariant or inevitable feature of drug markets; many such markets experience little or no serious violence, and even the most violent drug markets are peaceful most of the time". Dickinson (2017) also provides similar evidence on the importance of avoiding violence in drug dealing settings, with first-hand examples of dealers practicing prevention by offering free drugs to clients so as to avoid snitching and eventual enforcement (see also Dickinson and Wright 2015). Dickinson's dealers were more likely to threaten clients with avoidance than violence. Such assertions are also supported by Coomber (2006) who also describes drug dealing experiences that, in general, indicate that the claim that violence is systematic or systemic in illegal drug markets is largely overstated.

Ethnographic research also supports such an appraisal. Taylor's (2007) study of drug dealing disputes illustrates that outcomes are generally influenced by the seriousness of the dispute and the relational features uniting participants in conflict. Most drug dealing

conflicts were found to present little harm and ill intent. For those that were more serious, the likelihood of violence was largely dependent on a preceding enemy link between conflicting parties; friends and long-standing business partners were more likely to find non-violent resolutions. However, and as Jacques' (2008) critique of Taylor's book also makes apparent, there is much more to this resolution setting than a clear-cut dichotomy between violence and non-violence. Jacques' point touches on a crucial fallacy emerging from many past drug market settings: the focus on violence in illegal drug markets has generally been approached from a simplistic outlook, lacking the comparison with nonviolence or the even more nuanced assessment that would integrate specific forms of nonviolent outcomes. Much of past research on violence in illegal drug markets (and illegal markets in general) has been tainted by a self-fulfilling prophecy that has us searching for violence and only violence. This fallacy suggests that, if we look for violence in illegal drug settings, we will find it, but this does not allow us to generalize such observations to a market as a whole. Essentially, violence is but one form of conflict management and scenes of violence must therefore be situated within a wider repertoire of conflict management and resolution alternatives. The importance of such alternatives is best expressed by one of the drug dealers who shared his experience and despair with having to resolve a dispute in Jacques and Wright's (2008) study: *"I mean, what am I going to do: shoot him?"*If questions remain in regard to the prevalence and situating of violence in illegal drug markets, the issue becomes even more salient when we shift the focus away from the physical interactions underlying these traditional markets and toward online channels for illegal drug transactions. Within the last decade, we have witnessed an increasing use of the Internet to facilitate the buying and selling of illicit goods and services, including stolen credit card information (Fallman et al 2010), sex work (Holt and Blevins 2007), and drugs (Walsh 2011). The step-change for Internet-facilitated drug sales was showcased in the online e-Bay-style marketplace that was Silk Road, shut down by the FBI in October 2013, and the many marketplaces that have proliferated since. Referred to as 'cryptomarkets' (Aldridge and Décary-Hétu 2014; Martin 2014a; Christin 2013), these hidden online marketplaces capitalise on the anonymity mechanisms afforded by the Tor network, which hides the IP address (the unique identifier of actors online) of the cryptomarket participants and the servers hosting the cryptomarkets themselves. Cryptomarkets also make use of the cryptocurrency Bitcoin, which also allows for anonymous, international and instant payments.

This study aims to address two inter-related research questions regarding violence and conflict management within online illegal drug markets. First, to what extent do drug cryptomarkets create self-regulating state-like mechanisms to resolve disputes over transactions? Second, what are the various conflict settlement strategies used by their participants, notably taking into account their resort to threats of violence, or lack thereof. The conflict management strategies analyzed here are based on Black's (1993) and Meeson and Morselli's (2012) past works and model conflict as a process in which its determinants can actualize through four channels and eight strategies.

Situating Violence and Other Forms of Conflict Management

Conflict can be conceptualized as a process where two or more parties argue around a point of contention. In illegal drug markets, such conflicts may arise for several reasons: merchandise problems; debt collection; competition with other suppliers; theft of money or goods; or threats of informants. The resolution of such conflicts may take on several violent and non-violent forms, with the latter often surpassing the former. This understanding is in line with a well-established perspective. Black (1984) argues that some groups may be stateless even though living under the jurisdiction of a state. For

3

example, Black (1976) argues that the system of social control used by the state and regulated by law is developed among the integrated, the conventional, the wealthy, and the respectable, as well as among members of cultural majorities. However, marginal, unconventional and poor individuals, as well as members of cultural minorities, often occupy relatively stateless locations within modern state societies. Consequently, they are more likely to resolve their conflicts using self-help or retaliatory methods (Black, 1984). Cooney (1997) identifies such stateless spaces within the state as virtual locations. Shakur (1993) maintains that the internal features of these virtual locations and people therein result in rare uses of the law, hostile relations with legal authorities, and little assistance or satisfaction when authorities are called upon to resolve conflicts.

Illegal drug markets are such virtual locations, as individuals engaging in drug dealing have practically no means of legal redress, leading them to find their own conflict resolution strategies. As discussed by Reuter (1984), illegal market participants must establish their own rules in addition to securing the cooperation of others willing to enforce their lifestyles and interpretation of justice.

Black's (1993) work on conflict management distinguishes self-help strategies that are employed by individuals in their personal experiences (e.g., vengeance, discipline and rebellion, avoidance, negotiation, settlement, and tolerance) from third-party interventions that are introduced across various scenes of conflict. Both general forms of conflict management are relevant in illegal drug settings, with more specific management strategies emerging as well (e.g., ostracism and threats). Building on Black's typology, Meeson and Morselli (2012) propose a six-point typology of conflict management that differentiates between non-violent (negotiations, preventive measures, third-party intervention, no resolution) and violent (assault, retaliation) conflict management strategies.

Thus, whether in the form of self-help or third-party strategies, there are many alternatives for drug dealers to turn to when confronted with conflict. Most importantly, several other studies in addition to Jacques and Wright (2008), Taylor (2007), and Meeson and Morselli (2012) show that drug dealers, at all levels of selling, try to avoid violence or generally turn to violence as a last resort (Morselli 2005; Pearson and Hobbs 2001; Dorn, Oette and White 1998; Adler 1985; Reuter 1983, 1984).

Online Illegal Drug Distribution Settings

The conflict management strategies of drug market participants were traditionally constrained by the physical setting in which they operated. Since 2011, however, drug market participants have had the opportunity to transact through online *cryptomarkets* (Martin 2014a; Christin 2013). Cryptomarkets have been defined (see Barratt and Aldridge 2016) as online platforms bringing together multiple sellers or 'vendors', and offering strong anonymity properties to their participants through the use of anonymous Internet connections (using the Tor network) and anonymous payments (using one of the available cryptocurrencies, most commonly Bitcoin). These technologies help to protect cryptomarket participants even in the occurrences of law enforcement operations that take down these marketplaces (Décary-Hétu and Giommoni, forthcoming).

Aside from the rarity in auctions, cryptomarkets operate on the same model as eBay or Amazon, in which vendors build virtual shops that buyers can browse through; purchases are sent through the mail. Most items sold on these platforms are related to drugs (Aldridge and Décary-Hétu 2016a) with 70% of all transactions in 2015 related to

cannabis, MDMA (ecstasy) and cocaine-related products (Soska and Christin, 2015). Cryptomarkets are international platforms as they bring together actors from around the world. To purchase drugs, a buyer needs to add Bitcoins to an account, purchase a product, and wait for the vendor to ship it through the mail. In most cases, payments are held in escrow, which means the money is kept in a third-party's or market administrator's custody until the product is received. This process, combined with automated feedback systems, ensure a high degree of successful transactions.

Cryptomarket buyers report that transactions are more convenient, professional, and safe since meeting face-to-face with a dealer is no longer necessary (Barratt et al. 2013; Van Hout and Bingham 2013a; Van Hout and Bingham 2013b). Vendors agree that transactions are more convenient and pleasant and appreciate the professionalism of cryptomarkets and the ease with which a vendor's shop can be set up (Van Hout and Bingham, 2014). A key feature of cryptomarkets is the harm reduction ethos of their participants (Van Hout and Bingham, 2014; Van Hout and Bingham, 2013). This ethos is centred on active participation in forums to give harm reduction advices, promote informed consumerism, and support other members of the community (Van Hout and Bingham, 2014).

Of particular significance to our research aims is the suggestion that cryptomarkets may reduce transaction-related drug market violence, even if conflicts manifest themselves in other ways (Aldridge and Décary-Hétu 2016a; Martin 2014b). Importantly, recent survey research suggests that cryptomarket purchasing is associated with less self-reported experience of threats and violence compared to users' reports of these experiences in their purchasing in offline markets, including through social supply (friendship) networks (Barratt et al, 2016).

Cryptomarkets appear to be settings with relatively low levels of conflict. Indeed, feedbacks left by buyers are almost exclusively positive, with upwards of 95% of feedbacks being positive (Christin, 2013). These numbers are impressive but hide a reality where an array of determinants can generate conflicts. We conceive these as falling into six types, listed in Table 1.

INSERT TABLE 1 ABOUT HERE

Transaction failures include any deficiency in the prospective flow of transactions. These failures can arise from the actors themselves when the drugs shipped are of lower than expected quality. They can also arise from outside factors such as interception by border officials or postal service delays. By dealing online, cryptomarket participants are also subject to scams by other participants. Scams are intentional activities that increase an actor's profits to the detriment of others. The most common scams are thefts by vendors (when lying about having shipped the drugs) and buyers (when lying about not having received the drugs). Another problem is phishing, which takes on many forms but is intended to lead to the takeover of a participant's account to steal bitcoins or access funds held in escrow. Bad management by cryptomarket administrators has been blamed for allowing such scams to take place. Indeed, participants have complained about administrators that react too slowly to problems, thereby allowing a faulty vendor to scam even more buyers. This platform mismanagement may also lead to late third-party approval of escrow payments and to software bugs that compromise the operational

security of cryptomarkets and their participants. In more lax settings, vendors may be able to adopt unfair competitive practices. Such practices aim to disrupt competitors' activities through ostracizing on public forums or making purchases from competitors with the purpose of leaving negative feedback, thereby damaging a competitor's reputations. Attacks of this nature may be particularly effective as most cryptomarket vendors have a near-perfect reputation score; buyers may therefore be put-off when planning a purchase from a vendor with a less-than-perfect feedback metric. Buyers and vendors routinely interact on official cryptomarket forums and these social interactions may result in conflicts among cryptomarket participants. Misunderstandings, disagreements, or rumours can upset participants and generate social conflicts. Finally, law enforcement agencies have tried to destabilize cryptomarkets since the take down of Silk Road in 2013 (Aldridge and Décary-Hétu 2014). For this purpose, they may undertake various activities such as the use of informants, market obstruction practices, arrests, and even marketplace take-downs. Such activities may lead to mistrust and paranoia that generate conflict among cryptomarket participants.

Conflict Management in Illicit Drug Cryptomarkets

Many scholars have examined the variety of sources and resolution options for conflict in illegal drug markets. As the several demonstrations of non-violent conflict management options from past research have illustrated, there are key shortcomings to the typical appraisal of what it means to be an illegal drug market participant and how violence is not necessarily the trigger response to a problem as often believed in mainstream criminological circles. This contention is pushed even further when examining violence in contemporary online and, more specifically, anonymous drug market settings. Indeed, the limitations of Goldstein's (1985) framework on the systemic violence dimension of drug markets become most apparent when applied to cryptomarkets. The social distance between buyers and sellers and the underlying access conditions that precede an actor's inclusion in a cryptomarket decrease and largely eliminate the harmful features that Goldstein associated with traditional drug markets. The spatial extensions offered by online vending minimize territorial disputes. Dealing hierarchies are less of an issue, which should minimise assaults and homicides between competitors or within firms. The transaction costs associated with robberies, burns, and physical retaliation are too challenging, largely because participants' identities are concealed. This relative anonymity should also lead to a radical reduction in the violence that traditionally extended from the elimination of informants. Cryptomarket regulations should thus shift punishment for bad transactions and rip-offs away from violence.

In the age of the Internet and with the rise of illegal drug cryptomarkets, the dominant concepts, frameworks, and theories that have helped us understand and explain illegal drug market conflicts have reached their limits. By making the crucial break with physical interactions, online drug distribution settings avoid the heated and impulsive violent reactions in times of transactional conflict. The social and geographical distances between buyers and sellers that converge in these setting not only reduce the likelihood of violence at the situational level, but also limit the capacity of participants to follow through on such ill intents over an extended period.

Hence, whereas researchers have questioned for quite some time the popular association between illegal drug markets and violence within traditional drug supply settings (Coomber, 2006; Jacques and Wright, 2008; Reuter, 2009; Meeson and Morselli, 2012), this study investigates the various mechanisms that provide regulations on cryptomarkets, mechanisms that are traditionally assumed to be absent in stateless locations that characterize offline drug markets. This includes conflict settlement

strategies used by participants and their resort to violence or lack thereof. To do so, we focus on the strategies that cryptomarket participants use to settle conflicts. Extending from Black's (1993) typology, we identified six strategies that could be used by cryptomarket participants to resolve disputes: tolerance; avoidance; ostracism; third party intervention; negotiation; and threats.

Figure 1 provides an illustration of how resolution of the six determinants of conflict we have identified on cryptomarkets (see Table 1) may be achieved: via four available channels though which disputes can be settled, alongside the six conflict resolution strategies available to cryptomarket customers.

INSERT FIGURE 1 ABOUT HERE

When conflicts arise, four channels are available to cryptomarket participants through which resolution may be achieved. Participants can first initiate direct contact though dialogue with a conflictual party through built-in marketplace messaging systems. A second channel, offered on many but not all cryptomarkets, is the formal support ticket system. Support tickets allow participants to ask for assistance when they have issues with money withdrawal or order resolution. When these tickets are related to conflictual situations, they lead to third-party mediation by cryptomarket administrators who seek to settle the conflict. A more public alternative to support tickets is the use of forums posts. Participants can post publicly about a conflict and discuss the issue with other participants. Some markets also offer specific scam discussion forum sections where participants can post about the perceived mistreatment or injustice. The last channel for conflict management is automatic feedback systems. Participants who feel they have not had their fair share in a transaction can leave a negative feedback to the vendor associated to the transaction. Negative feedbacks allow customers to express their discontent in a transaction and manage the conflict quickly by affecting the vendor's reputation. Of course, cryptomarket participants could seek to settle conflicts outside of the marketplace via confrontation in real life. For this to happen however, the participant would first need to have information about the other person's identity and location.

Of the four channels available for conflict resolution, direct contacts and support tickets are private interactions that can only be accessed by cryptomarket participants and administrators, and so are unavailable for public viewing. This leaves two channels open and accessible to researchers to understand conflict settlement, the public forums and the automatic feedback systems. This article focuses on the former, as the latter provides little in the way of interactions and the feedbacks' qualitative comments typically amount to little more than a few words, which is far from enough to discern the nature of conflicts and the strategy used to settle it.

By examining publicly observable conflict and its resolution on drug cryptomarkets on the public forums, we are unable to observe real-world violence that may be enacted in this connection, but can observe threats of violence. In accordance with Jacques and Wright (2008) and Meeson and Morselli (2012), we do not expect to find that threats of violence will be a dominant strategy to settle conflict on cryptomarkets. Rather, we expect that the remaining strategies will play a much larger role in the settlement of conflicts, with third party intervention by marketplace administrators taking on a key role. The online nature of cryptomarkets should make particularly available the use

ostracism as a conflict resolution strategy, since customers are able via discussion forums to publicly identify vendors with whom they have disputes to warn other users and encourage marketplace administrators to intervene.

Data and Method

We used two sources of data to address our research aims. Most cryptomarkets post rules of engagement in the form of conventional statements "agreement and conditions". Using the 'Dark Net Market Comparison Chart' published by Deepdotweb (2016), we selected the top 10 marketplaces in the list and then accessed each marketplace to obtain their rules of engagement. All of these marketplaces had rules of engagement that were visible to non-vendors (although two additionally made reference to additional rules only available to those registered as vendors). The marketplaces included: Alphabay, Dream Market, Valhalla, Hansa, Python, Acropolis, Tochka, Cryptomarket, Outlaw and Nucleus and included the markets with the most listings at the time of writing.

Our second data source was obtained from a cryptomarket discussion forum. The online forum we selected is the official forum of one of the largest cryptomarkets at the time of writing. More specifically, we analyzed 200 discussion threads from the scam reports section of the forum. Normally, this channel would be the third or fourth choice used to settle conflicts after direct contact and support tickets. In this cryptomarket's case however, market administrators redirected scam victims to this section of the forum rather than the official support ticket system. This section is therefore the preferred channel to settle conflicts on this particular cryptomarket that is publicly available. We examined all interactions that took place between September and November 2015, but excluded those explicitly referring to non-drug purchases. In doing so, we obtained 679 interactions between buyers, vendors and market administrators that ensued from the 200 forum discussions.

For each posted conflict, we coded which among the seven conflict resolution strategies (described above) were employed. An interaction could be coded as employing multiple strategies. Our analyses focus on the interactions among the different conflict settlement techniques. In keeping with the emerging literature on ethical conduct in research using digital traces, we paraphrase quotations so that users' online identities cannot be ascertained through searching (Bancroft, 2016) and do not name the cryptomarket from which we collected data (Décary-Hétu and Aldridge, 2015).

Self-Regulation in Marketplaces

All of the marketplaces had guidelines that could be broadly characterized as having the objective of reducing harm, particularly third-party harm. Nine of the ten marketplaces we examined prohibited particular products and services from being listed by vendors for sale. The remaining marketplace referred to rules only accessible to registered vendors, which we were not able to observe. Most typically, these included child pornography, assassination services, and banned weapons or particular subsets of weapons (e.g. weapons of mass destruction, including bombs and poisons). One marketplace stated that its policy on prohibited items was developed following a vote by marketplace participants on the forum. Another marketplace was overtly ideological in banning products and services that involved what it referred to as 'discrimination, religion, and politics', although what products and services might be included under this heading were not provided. In most cases, cryptomarket administrators stated that posting listings for prohibited products and services would result in taking down the associated listings.

Seven of the ten marketplaces listed rules related to security and trust activities either required or prohibited. Five marketplaces did not allow the practice of vendors requesting that customers 'finalize early' (i.e. circumventing the escrow of payments while drugs are in transit) in order to bypass the buyer protection that escrow systems provide, or allowed the 'finalize early' option only to approved for vendors with a track record. To discourage scamming, two marketplaces stated that too many customer-initiated 'scam reports' (thus only accusations not necessarily verified) could result in a vendor account being revoked. Although most marketplace rules were geared towards regulating the activities of vendors, one marketplace described its infrastructure that had been designed to prevent exit scams by marketplace administrators.

Two marketplaces stated that vendors threatening, blackmailing, or 'doxing' customers (revealing personal information) were prohibited. Three marketplaces encouraged participants to follow good security and encryption practice; one marketplace stated that not doing so could result in marketplace dispute adjudication services being made unavailable to them.

Conflict Resolution Strategies used by Cryptomarket Participants

Of our six determinants of conflict listed in Figure 1, most of the conflicts we observed in our sample of forum discussions concerned transactions failures or scams. The main complaints raised focused on the non-delivery of a purchase ("*Never received my drugs*"); lack of communication following a direct contact initiated by a buyer with a vendor, or vice versa ("*Never received, never responded, nothing*"); or less than expected product quality ("*I loaded my shot, slammed it, and my first observation was that it SUCKED ASS*"). Some conflicts were also related to administrator inactivity where questions were raised about the trustworthiness of specific vendors (*"I'm pissed at admins for being so slow banning the vendor"* or "*WILL ADMIN PLEASE FINALLY WEIGH IN ON THIS, FFS!*"). All forms of resolutions strategies that were listed above emerged in our fieldwork.

Tolerance

Black (1993) defines toleration as "inaction when a grievance might otherwise be handled" (p.88). Such inaction is a sign of patience once dissatisfaction with a situation has been raised. Buyers registering dissatisfaction in the forum were often encouraged to wait longer for their purchase to arrive, just as a vendor might be asked for patience in waiting for a customer to finalise a transaction. A typical response to a buyer reporting that a purchase had not been received when expected was "*wait a little more*" or "*be a little more patient and report back*". A buyer screaming 'scam' too quickly could result in other forum participants encouraging tolerance: "*I understand your frustration but take it from me, he is not a scammer. I have been doing business with [vendor name] since he started and he has delivered 100%*"; [Response:} "*Take it easy, he's a good guy".* The purchaser generally concurred with these other participants: *"Okay, I'll be patient a while longer.*"

We also observed evidence of tolerance as a conflict resolution strategy when buyers were encouraged to extend their patience while marketplace administrators investigated vendors under review for possible scam activity: "*Can I get my money back? [Response:]* "*Not possible until a moderator resolves the issue*" and after a vendor scam accusation: "*I'll wait to see his side of the story*." This type of interaction can simultaneously be understood as third party intervention, discussed further below.

Avoidance

The avoidance strategy, in contrast, occurs when actors manage a conflict by "the curtailment of an interaction" (Black 1993: p.79). We found evidence of market administrators and other forum participants using avoidance techniques when there was no response to a complaint brought to the forum, as well as via the explicit rejoinder "*no response*" to a forum complaint, with no further discussion to follow. We cannot ascertain with our data how often dissatisfied marketplace participants avoided conflict by not registering the problem on the forum to begin with. Assuming that such a strategy of avoidance in dealing with conflict did occur, we can surmise that avoidance may have been even more common than we found. The avoidance strategies we did observe, however, suggest that market actors witnessing complaints but not responding to them and where no complainant follow-up discussion ensues both model avoidance by refusing to intervene and encourage avoidance by the complainant—and, in some cases, to the obvious frustration of the complainant: "*IS ANYBODY LISTENING HERE?*". Evidence of vendor avoidance in dealing with conflict was evident when buyers referred to having privately messaged vendors with a complaint to no effect, as this interaction illustrates: "*He sent bad quality bars, but will not deal with the matter.*" Discussions initiated by buyers that referred to private communications with vendors going unanswered in this way were particularly prevalent on the forum.

Ostracism

While Black did not explicitly include ostracism as a specific form of conflict management (he included it as a form of avoidance), the prevalence of cases falling within this category was important enough to warrant its inclusion in this study. Ostracising as a conflict resolution strategy on the cryptomarket forum occurred when buyers attempted to call attention to vendors with whom they were dissatisfied by identifying them with a "scam". The aim of such action is to exclude someone from the group. This was commonly employed by marketplace participants to manage conflict: "*Believe what you like, but this fucking bastard [vendor name] scammed me*" or "[vendor name] *IS A SCAMMER, NO QUESTION*!" Such statements were often explicitly warning other potential buyers: "*Do not do business with [vendor name]. He is a selective scammer[1]*". The outcome of disputes often involved not only calling attention to misconduct in this way, but was evident when interactions indicated the possibility of banning of participants outright: "*Thanks for letting us know. [Vendor name] is under review. We should be in a position to enforce a ban within 24 hours after further investigation*". This strategy was also evidenced with the common statement *"[Vendor name]'s been banned"* by marketplace administrators following conflict discussion interchanges.

Third-party Intervention

Banning by marketplace administrators is a form of third-party intervention and was a common form of conflict resolution on the forum. We observed third-party mediation in two ways. First, buyers often explicitly requested the intervention of administrators with interactions following the description of a dispute with statements like: *"Need help of admin or moderator please"* and *"Scamwatch, can you talk to him please?"* Second, after a

---

[1] Selective scammers are vendors or customers that scam only occasionally so that their fraudulent actions (not sending goods, or claiming goods have not been received) are more likely to be believed to be shipment interception or loss, both of which are accepted as inevitable when posting illegal drugs.

customer raised a concern or dispute on the forum, marketplace administrators themselves monitoring the forum might offer to intervene either by asking to be added to private message exchanges with the vendor ("*Please add me to those conversations that you're having with the vendor. If allegations are confirmed, I'll fuck the vendor up*") or by requesting specific evidence of vendor wrongdoing ("*If [vendor name] asked you to FE, please supply evidence and we'll investigate*"; "*Shut up or show the proof I asked you to!*"). Others participating in these interactions would recommend to the buyer or vendor posting their dissatisfaction to employ the third-party facilities provided by the marketplace: "*Just explain your case to the mod in charge.*" and "*Scamwatch, can you advise this guy?*"

In line with third-party interventions, monetary sanctions were observed when vendors agreed to refund lost shipments after having raised the dispute on the forum, often after intervention by administrators or the Scamwatch team, as evidenced by interactions ending with "*That's been resolved in your favour*" and "*I've been refunded now, thanks.*" Where vendors had been banned or were unwilling to provide refunds, the marketplace administrators could intervene to make payment redress to participants deemed to have suffered loss, although this was observed only rarely and in connection to funds being available to do so. This administrator, in response to a buyer's scam allegation, illustrated how banned vendors' assets could be shared by injured parties: "*There's [bitcoin value] remaining in [vendor name]'s account. We'll divide this up and distribute once everyone's provided evidence for their losses, but there obviously isn't much to go around.*" This vendor, aware that monetary sanctions could be applied, taunted his victims: "*Don't worry guys there is [trivial bitcoin value] available in my account for refunds*". Monetary sanctions of this kind were likely a 'last resort' conflict management option, because vendors banned for scamming often had few bitcoins left in their accounts. Monetary sanctions were typically employed following ostracism and third-party intervention.

Negotiation

Negotiation is a conflict management option where conflicting parties show a willingness to discuss a resolution strategy to accommodate losses. It is likely that most negotiation interactions will have taken place in private communications between vendors and buyers, and so will not be observable in our data. Nevertheless, we saw considerable evidence of negotiation used to resolve conflicts. Even where buyers were concerned about the possibility of having been scammed, a common opener discussion posting indicated a willingness to negotiate: "*I'm not calling scam here, but want to discuss my options since [vendor name] hasn't yet responded to me*" and "*I don't want to dispute, but I haven't received my package. Can anyone advise? I don't want to name the vendor.*" One buyer explicitly offered to negotiate after receiving notification indicating a package had been seized and confiscated by customs authorities, but was asked by administrators to "*Provide proof please*". Some conflicts were satisfactorily resolved after negotiation: "*[Vendor name] provided me a tracking number the same day my order showed up. Everything looks good, and I can find no breakage. I have to retract anything negative I may have said, sorry [Vendor name]*". This buyer, after having first accused the vendor of scamming, closed the interaction with: "*I've received the package, [Vendor name] is a good seller, I will continue buying from him. Cheers.*" Vendors also demonstrated a willingness to negotiate or refund, as this response following a scam accusation illustrates: "*You're acting like babies. If I confirm your shipment hasn't been received, you'll get you a refund*"

Threats were evident on the forum. Comments like this were illustrative and typical: "*If [vendor name] doesn't address this, I won't finalise so he doesn't get paid AND will leave bad feedback.*" These commonly found threats have much in common with behaviour associated with dissatisfaction associated to transactions in legal markets. The remaining two threats we encountered may be more unique in the online drug trade (doxing), or traditionally considered to be typical of drug markets more generally (threats of violence). We observed these only rarely, but describe each instance in some detail here.

Threats of blackmail via doxing were found in in only two of all the interactions we analysed. In the first instance, a buyer initiated a complaint about a dox threat made by a vendor, and retaliated with a counter-threat: "*I'll go public on Reddit with this*". Given the conflict had escalated to the stage of making threats, a negotiated solution was achieved in this case, by way of a partial refund, and this occurred without third-party intervention by administrators. In the second instance, a vendor complained of being doxed by a buyer: "*Please help me. I got doxed*". An administrator intervened to request evidence: "*If he's threatening you, please add me to the conversation.*" Another forum participant jumped in to defend the buyer: "*He's OK*", followed by a final response from the administrator justifying the decision to ban the buyer: "*He breached rules and was dealt with accordingly.*"

Threats of violence were rare, but did occur. In a first case, two buyers involved in an exchange disclosed threats of violence from the same vendor. An administrator intervened, asking for evidence of the threats from the buyer who started the interchange. A second buyer added a similar experience with the same vendor: "*[Vendor name] scammed me too, but I got my money back through arbitration. He also threatened to get me saying he has my address, but it was a drop [not home address] so I don't care.*" The original complainant then claimed to have deleted the messages since receiving a refund after dispute resolution, but described the content of the threat from memory: "*He said – don't forget, I have your address – nothing personal, just business.*" In both cases, these threats took the form of pointing out to victims that their locations were known, with the threat of violence not made explicit. In a second case, a buyer reported that an agreed negotiation following dispute to split the losses incurred was not followed through by the vendor. The message ended with a warning to others not to deal with the vendor (that is, ostracising him). The vendor responded: "*Cancer is in your future*". The buyer replied: "*Gang rape is in your future!*" In a third and last case, a buyer accused a vendor of having scammed him, and twice contributed to the exchange with variations on the message: "*I WILL KILL YOU MY FRIEND. DON'T WORRY, THE WORLD IS A SMALL PLACE, AND YOU DON'T KNOW WHO I AM :)*" The vendor replied in a taunting fashion, suggesting that a ban would not hurt him because of multiple vendor accounts. No administrators intervened in the exchange. These threats of violence appear fairly innocuous, intended perhaps to convey outrage, perhaps even with comic (albeit dark comic) effect. Such snippets of conversation could also be the result of trolls, which are provocative posts to intentionally upset participants and that aim to cause disturbance and within a forum. As Barratt and Maddox (2016) described via their own personal experience, distinguishing between a real and fake threat is an important challenge in internet interactions. In Barratt and Maddox's specific case, the threat was dismissed once no real consequences emerged over time. In our case, the presence of trolls that make such no-consequence offensive statements is also a strong likelihood.

Standard Operating Conflict Management Procedure

The most common conflict management options undertaken by participants in forums are ostracism, third-party mediation, tolerance, and avoidance. Negotiation and threats were more scarce options and violence was completely absent. Conflict management is also a process and, therefore, many options were subsequently pursued according to the status of the conflict. We found conflict management patterns that were quite common through the analyses of the discussion threads. A common trait of almost every thread was that participants started their thread by calling out the other party involved in the conflictual situation a scammer: "*he is a selective scammer fucker*". This is far from surprising as scam forums are built in part so that people may warn about others.

Hence, most conflicts started with calls for ostracism, from which other management techniques were undertaken by participants, depending on the context. The most prevalent pattern of conflict management among participants was from ostracising to third party intervention to banishment. A participant would write: "*Long story short, ordered 1kg. [...] Do not order from [vendor name], obviously he is a selective scammer*" and then an administrator would respond: "*Add me to those conversations.*" From there, a great number of conflict management scenes would result in the banishment of a participant with a message of "*Vendor is banned*" or "*Vendor is taken care of*". This pattern was often observed in the conversation and seemed to be the most common way to manage conflict.

Two other less common but still important conflict management patterns were observed in cryptomarkets. The first started with ostracism and then moved to tolerance. Often, participants would first ostracise: "*[...] [Vendor name] is a scammer! I have not received my order and, after 24 hours, still no reply to my PM [private message].*" A subsequent comment called for tolerance: "*I can help you. Just wait for some more time*" and "*[Vendor name] is legit. I did many orders on Agora with him. Don't see him scamming - maybe just a big misunderstanding.*" Often, conflicts management scenes that shift from ostracism to tolerance would resolve quickly, with one participant in the discussion reporting that the conflict had been resolved. Shifts from ostracism to avoidance also represented important conflict management patterns within the scam forums. A participant would start by ostracising someone and no response would follow the first comment. Most comments with no reply were either poorly written, unclear, or excessively abrasive in tone.

Stateless? Regulating and Enforcing Cryptomarkets

Illegal markets have been typically understood to be 'stateless', leaving participants to resolve their problems and disputes without the benefits of formal mediating agents and guidelines (Reuter 1983; Black 1984; Cooney 1998; Wilkins 2001; Jacques 2010). When William Ross Ulbricht was sentenced to life in prison for his role in setting up the first and best known cryptomarket, Silk Road, Judge Forrest proclaimed: "*In the world you create over time, democracy didn't exist*". What we observed in this study was that cryptomarkets were far from anarchic or a world ruled by dictators. Official rules were posted publicly on these marketplaces. These rules primarily took two forms. First we discerned 'moral/ethical' rules banning the listing for sale of particular items (most typically child pornography and weapons), with one marketplace having agreed on a list of prohibited items after a democratic vote on its marketplace forum. Second, functional rules were necessary to achieve effective marketplace functioning through regulation. In particular, these rules were designed to prevent thefts and scams that might undermine the trust required for on-going trade in a drug trade that is otherwise uncertain and risky. Particularly when these rules have 'teeth' when backed up by effective

13

enforcement, they can be understood as functioning to create self-regulation or nodal governance mechanisms that mirror those provided by traditional agencies of the state for markets in legal goods and services (Martin 2014b). This leads us to ask: how effective are these rules of engagement in preventing market discord?

Clearly the self-regulating mechanisms of cryptomarkets do not completely prevent vendors from scamming their customers (or customers scamming vendors), nor do they prevent marketplace administrators from absconding with the funds of both, as a number of high profile 'exit scams' have demonstrated (e.g. Woolf 2015). As Branwen's research shows, more marketplaces have closed due to inside hacks or scams than as a result of law enforcement take downs (Branwen 2015). That one of the ten marketplaces we examined for rules of engagement described how its platform was designed to reduce or eliminate vendor scams or administrator exit scams suggests that on-going innovations in cryptomarkets are aimed precisely at creating effective marketplace function and, hence, longevity.

Our analysis of conflict resolution on the cryptomarket we studied demonstrated that marketplace administrators, alongside a dedicated 'scamwatch' team of cryptomarket community members, sought to enforce rules. Participants had access to multiple channels to settle private and public conflicts. These channels give options to cryptomarket participants when conflicts emerge and allow them to have a voice in the decisions made. However, administrators always have the last word when settling conflict and not all conflicts will have resulted in a resolution that satisfies all parties to the conflict. Munksgaard and Demant's (2016) analysis of political sentiments in marketplace discussion forums between October 2013 and March 2015 identified the presence of a hegemonic libertarian discourse that declined after the closure of Silk Road 1, leading the authors to identify a decrease in political discussion in these marketplaces. Maddox et al. (2016), on the other hand, found that opportunities for open yet anonymous exchange on cryptomarkets encouraged discussions on politically sensitive subjects, such as drug prohibition. Our results suggest that, beyond such discussions, there is real political participation within cryptomarkets that takes the form of policy-in-action through enforcing regulations. By using these conflict management channels, participants actively engage in the construction of a trustable market ecosystem.

Violence and Threats: A Lesser Strategy?

Taken together, the establishment and enforcement of rules, the presence of administrators as 'capable guardians' (Cohen and Felson 1979), alongside the inbuilt conflict reduction mechanisms common to all cryptomarkets (dark net online location, escrow, and customer feedback) reduce the need for cryptomarket participants to settle on their own those conflicts that may still arise and to adopt retaliatory strategies to do so. As seen in Black (1984) and Meeson and Morselli (2012), drug market participants can choose among an array of conflict settlement conflicts and violence is even more the exception than the norm in the case of cryptomarket participants. We saw in our review of scam report threads that most participants would, in many cases, opt to ostracize, be tolerant, and/or ask for third-party intervention rather than resort to the threat of violence. Through the process of conflict management, multiple options would be employed in different order, with almost all interactions beginning with the complainant ostracising the perceived offender in the conflict.

Although scenes of violence appear to be rare in the cryptomarket setting, comparing cases in which violence does emerge to the many in which alternative options are used to resolve a conflict contributes to Jacques' (2010) quest to further develop a theory of

retaliation in illegal drug market settings. The main challenge set forward by Jacques was a data gathering issue. While we no longer find ourselves within the confines of a physical drug market context, this challenge is conveniently overcome when orienting our fieldwork on the dark web and the accessible discussion forums that are accessible.

Taylor's (2007) study on drug dealing disputes illustrated that the outcome of a dispute depends on its seriousness and the relational features uniting conflicting participants. As we cannot say anything about the seriousness of a dispute, which depends on the subjectivity of both parties, we can assume that online relationships of cryptomarket participants are mostly economic and, therefore, that the features uniting both parties are quite limited. Considering that relationships mostly have economic exchange as their purpose and that there are several channels and conflict management strategies to resolve conflicts, the absence of violence or threat is not surprising. Even in offline drug markets, this method is often a last resort (Meeson and Morselli 2012). Its use may be less required and effective in the context of Internet. Much more effective is the targeting of reputation. Establishing credibility and trustworthiness on online illicit markets is a challenge and requires long-term investments (Décary-Hétu and Dupont, 2013). Reputation is very often the most prized capital of cryptomarket participants and the ostracizing we observed most frequently attacks it directly. Doing so poses a serious risk to the business of a participant and may have more of an impact than making threats against a vendor that may be thousands of miles away. Where threats were made, these most often took the form of monetary threats or making threats to reputation via customer feedback or further ostracising, strategies not unusual in markets for legal goods and services.

The Public Nature of Conflicts

Our analysis demonstrated that conflicts on cryptomarkets can be settled publicly and with a range of marketplace participants often jumping to a conflict interaction to bolster the complainant with their own similar experiences or to defend the accused. With cryptomarkets viewed as mini-ecosystems that include their own forums for discussion by the cryptomarket community, ostracism becomes a particularly effective tool for dealing with conflict, not only generating a response to the particular grievance by marketplace administrators, but effectively warning others in the community about the allegations against a participant. Exposing conflicts thereby becomes a 'duty' for some participants to protect others in their community from a perceived scam. Our finding that participants in this illegal market denounced others thought to breach the pre-established rules implies a form of community social control. Illegal marketplaces facilitated by the Internet therefore challenge notions of the social disorganisation thought to characterise the disenfranchised communities that drug markets have been found to exacerbate (Martinez et al 2008). This mutual aid among participants, when a conflict emerges, shows how tight the cryptomarket community can be and how its participants are thereby made inter-dependent. Future research might consider examining questions around how online illegal marketplaces facilitate social cohesion, and, via community activated social control, create virtual locations that may reduce drug market-related harm.

Limitations and Suggestions for Future Research

Our data only included the 'public' discussion of conflicts and therefore exclude the private messages between buyer and sellers that also aimed at conflict resolution. Many messages posted to public forum were placed after these private (and therefore not available to us) attempts at conflict resolution have failed. For this reason, we suspect that the data we obtained will over-represent the more intransigent conflicts on the

marketplaces, and under-represent the more peaceable negotiated through private communications. That we still observe as much peaceable conflict resolution as we did perhaps suggests that cryptomarkets may be more effective in managing conflict than our results suggest. Conversely, it is possible that private communications may simultaneously be the location in which more threats, including threats of violence, take place. Future research might use surveys of cryptomarket users to further explore the nature, variety and extent of experiences of conflict, such as the approach employed effectively by Barratt et al (2016), although the samples obtained from surveys will lack the 'full market' picture that is a strength of digital traces (Décary-Hétu & Aldridge, 2015).

Our data do not allow us to know how many vendors or their customers may discretely accept situations that give risk to conflict, such as poor quality product or not receiving shipments or payments. However, research in connection with the first Silk Road has described vendors accepting a certain amount of loss as the costs of doing business "You have to factor in the increased chance of international packages being seized, and accept the risk to yourself of the loss of funds" (Décary-Hétu et al, 2016), suggesting that avoidance may occur more often than we observed it, with both drug buyers and vendors accepting this as a cost of illegal drug transactions.

We are unable to observe actual violence, and it is possible that some vendors will have held accurate identifying information about their buyers (names, addresses), and if distance was not prohibitive, might well have enacted violence. This is a limitation of our methodology, and one that survey approaches (albeit with their limitations noted as above) can go some way to remedying. Survey research by Barratt et al (2016) found that of the 3,794 Global Drug Survey respondents who reported cryptomarket drug purchasing, 1% reported experiences of violence associated with their transactions. This suggests that in spite of their online location, cryptomarkets do not prevent transactional violence. Moreover, as suggested by Aldridge and Décary-Hétu (2016b), cryptomarkets remain 'anchored' in offline drug markets "with vendors there purchasing drugs offline to sell online and stock-sourcing cryptomarket customers making their retail sales in offline markets. These anchors in offline drugs markets mean that cryptomarket users involved in drug supply activities may still be victims and perpetrators of violence connected to these face-to-face transactions."

We found that cryptomarkets created formal 'rules of engagement' as a form of self-regulation. Of particular interest was the marketplace that described an infrastructural design aimed at reducing or eliminating scams, and in particular, the marketplace exit scams that have hampered the longevity of the many cryptomarkets that have emerged and disappeared since the first, Silk Road. Whether this particular marketplace will prove immune to this threat remains to be seen. However, it is a truism that markets innovate and change in response to all kinds of threats, from within, and from without in the form of law enforcement interventions. While we cannot predict the nature of these innovations, this research provides a clue: drug cryptomarkets that are successful are likely to be those that help their participants manage conflict, that capitalise on technological innovations designed to maintain the trust required to buy and sell their illegal products, and that create socially cohesive communities with formal and informal social control mechanisms.

References

Adler, P. A. (1985). Wheeling and dealing: An ethnography of an upper-level drug dealing and smuggling community. New York: Columbia University Press.

Aldridge, J., and Décary-Hétu, D. (2016a). Cryptomarkets and the future of illicit drug markets. In EMCDDA (Ed.), Internet and Drug Markets, EMCDDA Insights (pp. 23-30). Luxembourg: Publications Office of the European Union.

Aldridge, J., and Décary-Hétu, D. (2016b). Hidden Wholesale: How drug cryptomarkets may transform traditional 'offline' drug markets. International Journal of Drug Policy.

Aldridge, J., and Décary-Hétu, D. (2014). Not an 'Ebay for Drugs': The Cryptomarket "Silk Road" as a Paradigm Shifting Criminal Innovation. Available at SSRN: http://ssrn.com/abstract=2436643.

Bancroft, A. (2016). Concepts of illicit drug quality: exploring purity, reliability, and judgement-making amongst darknet market users. International Journal of Drug Policy, 35, 42-49.

Barratt, M. J., Ferris, J. A., and Winstock, A. R. (2016). Safer scoring? Cryptomarkets, social supply and drug market violence. International Journal of Drug Policy, 35, 24-31.

Barratt, M. J and Aldridge, J. (2016). Everything you ever wanted to know about cryptomarkets (But were afraid to ask). International Journal of Drug Policy, 35, 1-6.

Barratt, M. J. and Maddox, A. (2016). Active engagement with stigmatised communities through digital ethnography. Qualitative Research, 16, 6, 701-719.

Barratt, M. J., Lenton, S., and Allen, M. (2013). Internet content regulation, public drug websites and the growth in hidden Internet services. Drugs: Education, Prevention, and Policy 20: 195–202.

Black, D. (1993). The social structure of right and wrong. San Diego: Academic Press.

Black, D. (1984). Crime as social control. In D. Black (Ed.), Toward a general theory of social control, volume 2: Selected problems. Cambridge: Academic Press.

Black, D. (1976). The behavior of law. New York: Academic Press.

Branwen, G. (2015). Black-Market Risks. Retrieved 12 March 2016 from https://www.gwern.net/Black-market%20survival.

Christin, Nicolas (2013). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. Paper presented at Proceedings of the 22nd International Conference on World Wide Web.

Cohen, L. E., and Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 588-608.

Coomber, R. (2006). Pusher Myths: Re-Situating the Drug Dealer. London: Free Association Books.

Cooney, M. (1998). Warriors and peacemakers: How third parties shape violence. New York: New York University Press.

Cooney, M. (1997). From Warre to tyranny: Lethal conflict and the state, American Sociological Review, 62: 316-338.

Copes, H., Hochstetler, A., and Sandberg, S. (2015). Using a Narrative Framework to Understand the Drugs and Violence Nexus. Criminal Justice Review, 40, 32-46.

Deepdotweb. Dark Net Markets Comparison Chart. Retrieved 24 February 2016 from https://www.deepdotweb.com/dark-net-market-comparison-chart/.

Décary-Hétu, D. and L. Giommoni. (forthcoming). "Do Police Crackdowns Disrupt Drug Cryptomarkets? A Longitudinal Analysis Of The Effects Of Operation Onymous." Crime, Law And Social Change.

Décary-Hétu, D., and Aldridge, J. (2015). Sifting Through The Net: Monitoring Of Online Offenders By Researchers. European Review of Organised Crime, 2, 122-141.

Décary-Hétu, D., and Dupont, B. (2013). Reputation in a dark network of online criminals. Global Crime, 14(2-3), 175-196.

Dickinson, T. (2017). Non-violent threats and promises among closed-market drug dealers. International Journal of Drug Policy, 42, 7-14.

Dickinson, T. and R. Wright (2015). Gossip, decision-making and deterrence in drug markets. British Journal of Criminology, 55, 1263-1281.

Dorn, N., Oette, L. and White, S. (1998). Drugs importation and the bifurcation of risk: Capitalization, cut outs and organized crime. British Journal of Criminology, 38, 4, 537-560.

Duran-Martinez, A. (2015). To Kill and Tell? State Power, Criminal Competition, and Drug Violence. Journal of Conflict Resolution, 59, 1377-1402.

Fagan, J. and Chin, K. (1990). Violence as regulation and social control in the distribution of crack. In M. De La Rosa, E. Y. Lambert and B. Gropper (Eds.), Drugs and violence: Causes, correlates, and consequences (pp. 8-43). Rockville, Maryland: NIDA Research Monograph 103.

Fallmann, Hanno, Gilbert Wondracek, and Christian Platzer. 2010. Covertly probing underground economy marketplaces. In Detection of Intrusions and Malware, and Vulnerability Assessment, edited by Christian Kreibich and Marko Jahnke. Berlin: Springer.

Goldstein, P. J. (1997). The relationship between drugs and violence in the United States of America (pp. 116-121). World Drug Report: United Nations Internal Drug Control Program.

Goldstein, P. J. (1985). The drugs/violence nexus: A tripartite conceptual framework. Journal of Drug Issues, 39, 4, 493-506.

Holt, Thomas J., and Kristie R. Blevins. 2007. Examining sex work from the client's perspective: assessing johns using on-line data. Deviant Behavior 28 (4):333-354.

Jacques, Scott (2010). The necessary conditions for retaliation: Toward a theory of non-violent and violent forms in drug markets. Justice Quarterly 27: 186-205.

Jacques, Scott (2008). Review of How Drug Dealers Settle Disputes: Violent and Nonviolent Outcomes by Angela P. Taylor. Criminal Justice Review 33(4):577–578.

Jacques, S. and R. Wright (2008). The Relevance of Peace to Studies of Drug Market Violence, Criminology, 46, 1, 221-253.

Johnson, B. D., Golub, A. and Fagan, J. (1995). Careers in crack, drug use, drug distribution, and nondrug criminality. Crime and Delinquency, 41, 3, 275-295.Martin, J. (2014a). Lost on the Silk Road: online drug distribution and the 'cryptomarket'', Criminology & Criminal Justice, 14, 3, 351-367.

Maddox, A., M.J. Barratt, M. Allen, and S. Lenton (2016). Constructive activism in the dark web: cryptomarkets and illicit drugs in the digital 'demimonde'. Information, Communication & Society, 19, 1, 111-126.

Martin, J. (2014b). Drugs on the dark net: how cryptomarkets are transforming the global trade in illicit drugs: Palgrave Macmillan.

Martínez, R., Rosenfeld, R., and Mares, D. (2008). Social Disorganization, Drug Market Activity, and Neighborhood Violent Crime. Urban Affairs Review.

Meeson, Julie-Soleil and Carlo Morselli (2012). "La violence et la résolution des conflits auprès des trafiquants de cocaïne", Criminologie 45: 213-241.

Munksgaard, Rasmus and Demant, Jakob (2016). Mixing politics and crime - the prevalence and decline of political discourse on the cryptomarket. International Journal of Drug Policy, 35, 77-83.

Pearson, G. and Hobbs, D. (2001). Middle market drug distribution. London: Home Office Research Study 227, Development and Statistics Directorate.

Reuter, P. (2009). Systemic violence in drug markets. Crime, Law and Social Change, 52(3), 275-284.

Reuter, P. (1984). Social control in illegal markets. In D. Black (Ed.), Toward a general theory of social control, volume 2: Selected problems (pp. 29-58). Cambridge, Massachusetts: Academic Press.

Reuter, P. (1983). Disorganized crime. Cambridge, Massachusetts: MIT Press.

Shakur, S. (1993). Monster: The autobiography of an L.A. gang member. New York: Penguin.

Sommers, I. and Baskin, D. R. (1997). Situational or generalized violence in drug dealing networks. Journal of Drug Issues, 27, 4, 833-849.

Soska, K., and Christin, N. (2015). Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. In USENIX Security '15 (pp. 33-48). Washington DC.

Taylor, A. P. (2007). How drug dealers settle disputes: Violent and nonviolent outcomes. Monsey: Criminal Justice Press.

Van Hout, M.C. and T. Bingham (2014). Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading, International Journal of Drug Policy 25: 183–189.

Van Hout, M. C. and Bingham, T. (2013a). 'Silk Road', the virtual drug marketplace: A single case study of user experiences. International Journal of Drug Policy 24: 385–391.

Van Hout, M. C. and Bingham, T. (2013b). 'Surfing the Silk Road': A study of users' experiences. International Journal of Drug Policy, http://dx.doi.org/10.1016/j. drugpo.2013.08.011 [Epub ahead of print; September 8].

Walsh, C. (2011). Drugs, the Internet and change. Journal of Psychoactive Drugs, 43, 55-63.

Wilkins, C. (2001). A "New Institutional Economics" Approach to the Reliability of Street-Level Drug Transactions. Contemporary Drug Problems, 28, 679-693.

Woolf, N. (2015) 'Bitcoin 'exit scam': deep-web market operators disappear with $12m', Guardian, Accessed 13 March 2016. http://www.theguardian.com/technology/2015/mar/18/bitcoin-deep-web-evolution-exit-scam-12-million-dollars

Décary-Hétu, D., & Aldridge, J. (2015). Sifting through the net: Monitoring of online offenders by researchers. European Review of Organised Crime, 2(2), 122-141.

Table 1: Summary of conflict determinants on cryptomarkets

Determinants of conflicts	Examples
Transaction failures	· Delay in shipping · Drug intercepted at borders
Scams by vendors	· Phishing links used to obtain account details · Theft of bitcoin payments
Bad market management	· Platform mismanagement · Marketplace scams
Unfair competitive practices	· Dissing other vendors · Buying from competitors and leaving bad feedback
Social interactions	· Rumors · Disagreements
Law enforcement activities	· Arrests · Take downs

Figure 1: Illustration of the conflict management process

DETERMINANTS OF CONFLICTS	CHANNELS	STRATEGIES
• Transaction failures • Scams • Bad market management • Unfair competitive practices • Social interactions • Law enforcement activities	• Direct contact • Support ticket • Public forum • Automatic feedback system	• Tolerance • Avoidance • Ostracism • Third-Party intervention • Negotiation • Threats