Money Laundering and Technology Enabled Crime: A Cultural Analysis

Full papers

Gurpreet Dhillon
Virginia Commonwealth University
gdhillon@vcu.edu

Abstract

Over the past decade or so, aided by information and communication technologies, money laundering has seen a sharp increase. While traditionally money laundering was associated with drug cartels and warlords, increasingly the focus has shifted towards white-collar crime and terrorist financing. It is therefore important to understand why money laundering (and hence white-collar crime) comes into being and sustains over a period of time. This paper, while exploring the antecedents of technology enabled white-collar crime, undertakes a cultural analysis of the Silk Road case. The cultural analysis helps in understanding patterns of behavior associated with technology enabled white-collar crimes.

Keywords: Money Laundering; White Collar Crime; Technology Enabled Crime; Cultural Analysis

Introduction

Over the past few decades, money-laundering activities have become sophisticated. And hence there has been a sharp increase in the amount of laundered money. While estimating the amount of money laundering is problematic because it is a concealed activity, some researchers have put forward efforts to quantify money laundering. Schneider (2010) estimates that money-laundering turnover on a global scale was $595 billion in 2001 and rose to $790 billion in 2006. Agarawal and Agarawal (2006) state that the amount of globally laundered money in 2005 was more than $2.0 to $2.5 trillion, which was about 5-6% of the world GDP; this increased dramatically between 2005 to 2009 by about 33% (Scheider, 2013). A 2015 report notes that an estimated $2 trillion illicit capital finds its way into various financial institutions (Lam, 2015).

In recent years crypto currencies have redefined the landscape for money laundering. This is because of lack of regulation and the democratized trust enabled through block chain technologies. Peer-to-peer currency systems are fast evolving and offer an alternative to the more traditional Fiat money, which is backed by nation states. Yet, because of the distributed nature of the currencies, there are concerns that money launderers use them systematically. Poland is perhaps among the earlier countries to adopt a peer-to-peer payment systems – Billon where the exchange rate between Polish zloty and Billon has been fixed at 1:1 ratio.

The paper is organized into four sections. The first section explores the nature of white-collar crime, particularly emphasizing the focus on individual and the role of institutions. We draw attention to the evolving normative structures that provide a backdrop for many of the criminal activities. Second we focus on the recent Silk Road case. While Silk Road is non-existent now, it provides an interesting context where businesses have been created, largely with the aid of advanced information technologies to trade stolen property and be compensated by crypto currencies. In the third section we undertake a normative analysis of the Silk Road case and draw out cultural manifestations of the changes. Finally we draw lessons of managing money laundering and technology enables crimes.
Understanding the Context of White-Collar Crimes

Money laundering is a form of white-collar crime. However in the literature the definition of white-collar crimes has remained elusive. This is because new revelations and emergent challenges have surpassed traditional boundaries (e.g. see Box 1981). The concept has often been related to abuse of power, drug trafficking, fraud, exploitation, concealment, financial and psychological damage. And it has become difficult to demarcate mafia like organized crimes from political and economic corruption. This has resulted in spill over between the “good” and the “bad” guys.

The Bank of Credit and Commerce International (BCCI) epitomized how white-collar crime and money laundering could be carried about publically without any significant intervention from the regulators. BCCI was founded in 1972. It was registered in Luxembourg and had head quarters in London and Karachi. It operated in 78 countries and had assets in excess of $20 billion. In 1991 regulators from seven countries finally raided and locked down the offices. Investigators found that BCCI was deliberately founded to avoid centralized regulatory review. BCCI was known to have laundered money for people like Saddam Hussein, Manuel Noriega, among others.

The criminology literature has largely tried to understand white-collar crime by abstracting the individual from the context and labeling such people as “deviant”. Such individuals have been characterized as greedy who typically lack self-control (Morrison, 1995; Price and Norris, 2009). An exclusive focus on individuals unfortunately draws attention away from institutional and normative structures that provide an opportunity. The prospect may emerge from the fallacies of the modern economic system or the manner in which the monetary system has evolved, or the innovations abetted by modern technologies.

Fiat money invokes a level of trust between the individual and the banking system. In many countries, currency bills note, for example the Hong Kong Dollar bills, “The Hong Kong and Shanghai Banking Corporation Limited promises to the pay the bearer on demand at its offices here Twenty Hong Kong Dollars”. Such a demand could be made because the currency was linked to either gold or silver. In the US the currency bills note something to the effect, “this note is legal tender for all debts, public and private”. Today however the gold standard does not exist and most exchanges are based on the trust we place in the current banking systems and nation states. The emergence of democratized trust orchestrated by Bitcoin and block chain technologies challenges the Fiat currencies. Yet the lack of regulation poses interesting challenges in terms of white-collar crime, money laundering and the role of centralized clearance houses. It can be argued that much of the increased incidents of cyber crime, white collar crime and money laundering are a result of changing nature of capitalism, where increasingly profits are generated from speculation, insider trading, circumventing exchange controls (Mitchell et al 1996). Coupled with this is the general erosion of moral values – the Enron fiasco was a case in point where majority of the executives where business graduates from elite schools.

Undertaking a Cultural Analysis

In this study we use Hall’s (1959) taxonomy of behavioral patterns to interpret money laundering consequences and cultural manifestations. Hall classifies culture into streams that interact with each other to exhibit patterns of behavior – the silent messages. These streams form the primary message systems. Hall identifies ten different cultural streams, which interact with each other to produce 100 different cultural settings. The framework helps in interpreting the cultural consequences of white-collar crime that are likely to cause trouble if not perceived in time. A brief description of Hall’s ten cultural streams is presented below.

- **Interaction**: Interaction lies at the hub of the “universe of culture” and everything grows from it. This interaction occurs both at the formal and informal levels.
- **Association**: Hall uses the analogy of bodies of complex organisms as being societies of cells and association begins when two cells join.
- **Subsistence**: Subsistence relates to the physical livelihood, eating, excretion and income, working for a living.
- **Bisexuality**: This refers to differentiation of sexes, marriage, and family.
- **Territoriality**: refers to division of space, where things go, where to do things and ownership.
An important question that arises relates to the value of undertaking a cultural analysis. Clearly a good understanding of the values and assumptions of various stakeholder groups helps in being responsive to the nuances. Halls’ culture map is a systematic interpretation of the theory to present a broad understanding of the various facets of culture.

Silk Road - a case in point

Silk Road was an online black market, which was operated by Ross William Ulbricht. The marketplace was used to sell illegal drugs and other stolen materials anonymously. Also, digital goods like hack tools, pirated software, etc. and forgeries of passports, social security numbers, fake licenses were all available for interested customers. Using the browser Tor, people involved in Silk Road were protected from getting caught. IP address is hidden by this service which makes it highly impossible to catch the culprits operating such website by making them anonymous. The buying and selling of goods was done with Bitcoin. Silk Road used the service, tumbler, again making it impractical to trace back a culprit through block chains. The transactions were obfuscated to avoid tracking. There were around 957,079 users registered with this website till 2013. There were 1,367 transactions taking place on a daily basis at $976 and revenue was around 1.2 billion USD.

Silk Road was created in 2011. In January of the same year, a user called altoid posted about the website Silk Road in some forums - bitcointalk.org and shroomery.org. He posted the same post on both forums asking for programming help. He even revealed the address for Silk Road website. In 2011 on June 18, an update was performed to the forum posting by the administrator where he declared that he wanted a false identity. Then in 2012 on February 5th, he wrote that Dead Pirate Robert (DPR) would be his new identity. FBI was able to find this information largely because on 23rd July 2013 they were able to take an image of the Silk Road server.

However, the story took a new turn. FBI recorded a conversation which took place between DPR and FriendlyChemist, a vendor on Silk Road. On March 13, 2013, DPR is threatened by a vendor (FriendlyChemist) saying that he would leak the client’s information if he does not get paid $500,000. Then, on March 15, some information is sent by FriendlyChemist to DPR as proof that he would be releasing the information and DPR believes FriendlyChemist and asks him to make his suppliers contact him so that he can come up with something. So, on March 20, DPR gets a message from the username redandwhite stating that he was told to contact DPR. Then, DPR replies to him offering a deal that he can do business with him and offers him to be a vendor to sell illegal things on Silk Road. To this redandwhite responds that if DPR pays him FriendlyChemist’s debt, he will try to do business with Silk Road. On March 27th, DPR sends a message to redandwhite saying that FriendlyChemist is just an obstacle, and there won’t be any if FriendlyChemist was executed. On March 29, FriendlyChemist threatens DPR stating again that he would leak details of some vendors and 5000 users if he were not paid by him. As soon as DPR receives this message he writes to redandwhite asking how much he would want to find FriendlyChemist. To this, redandwhite replies that he would want anywhere between $150,000 and $300,000. DPR requests redandwhite to do the operation with $80k and asks him to do it as soon as possible. Finally, they both make a deal in Bitcoins worth 1,670 which is $1,50,000 approximately. After receiving the payment from DPR, redandwhite acknowledges DPR and assures him that his work will be done. Later on March 31st, redandwhite sends DPR a message that FriendlyChemist has been killed and states that FriendlyChemist won’t threaten him again. After getting this message, DPR replies that he needed a proof to believe what redandwhite was saying. Redandwhite sends DPR a photograph, which relieves DPR. However, there are no records with the authorities that redandwhite received any name...
from DPR. Making this case even more mysterious, there has been no record of any homicide on the day when redandwhite give the proof to DPR that they killed FriendlyChemist in British Columbia. There was also no proof that FriendlyChemist was killed by redandwhite.

Thereafter FBI was able to link Ross Ulbricht to posts on YouTube, Google+ and his log history. In many ways Ross Ulbricht gave himself up by accessing his social media accounts and his posts on public forums. While at times Ross used fictitious names, simple investigations revealed linkages to same parent account. Eventually Ross Ulbricht was arrested. Nearly $4 million were seized by the FBI. Estimates suggest the Ross profited nearly $200 million from his illegal activities.

**Normative Analysis of the Silk Road Case**

The Silk Road online black market web site allowed buyers and sellers to meet anonymously, trade securely and receive goods via local mail and courier systems (Backman, 2013; Baratt et al, 2014). The benefits of ease of use coupled with the security, provided a platform to build trust relations and thereby allow for growth beyond the local neighborhood community. It is in the matter of trust and reputation that requires the inclusion of Edward T. Hall’s (1959) use of ten Cultural Stream analysis as the methodology to understand the underlying structure of this online community and potential means to disrupt its use. As noted previously Silk Road was established by Ross Ulbricht and ran from 2011 until October 20, 2013 when FBI agents arrest and eventual successfully prosecuted him and shut down the original site from use. However, subsequent sites emerged with similar design and use indicating a usefulness and demand for such platforms. The Silk Road site had specific features which were: a focus on “soft drugs” (Dolliver, 2015) consumer level drug trading between suppliers, dealers and users; political agenda; use of encryption methods to provide secure access for both parties; and most importantly an Ebay style of vendor rating allowing for a feedback system of user experience (Johnson, 2014).

Hall’s proposes ten cultural streams that interact with each other to provide a rich description of the cultural settings. Using Hall’s intercommunication amongst different streams, relationships of the Silk Road can be understood in the contexts socio-technical communities. The analysis of the Silk Road case is presented in Table 1 below.

<table>
<thead>
<tr>
<th>Stream</th>
<th>Interrelations with other streams</th>
<th>Information Security Implications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interaction: Buyers, sellers, and the administrators of Silk Road seemed to have minimal contact with each other, aside from questions about transactions or products.</td>
<td>Interactions between buyers and sellers may have been influenced by the reviews provided by other buyers and sellers; the more reputable, the more likely someone would transact with another person.</td>
<td>eBay is able to collect and associate names, addresses, and other personally identifiable information to buyer and seller profiles. None of this exists on Silk Road, making it virtually impossible for recourse, if a seller or buyer is conned.</td>
</tr>
<tr>
<td>Association: From an organizational perspective, no hierarchy existed within Silk Road; only the written agreement that all transactions would be charged a facilitator’s fee.</td>
<td>Ironically, the less the interaction a Silk Road user had with a buyer or seller, the more they had to trust that a transaction would go as planned.</td>
<td>Large and legitimate online marketplaces have an array of policies and procedures that can deal with a number of issues. On Silk Road, if problems arise, the user has no option but to absorb the loss.</td>
</tr>
<tr>
<td>Subsistence: Silk Road had one administrator, imposed minimal rules, and was unregulated, creating a safe haven for illegal activity.</td>
<td>A consistent and long-standing presence on Silk Road required that at a minimum, buyers and sellers delivered on their transactions, and earned ratings that helped recruit and retain new and existing customers.</td>
<td>Silk Road encouraged selfishness and encouraged accomplishing “business objectives” by any means necessary, including, perhaps, taking advantage of the platform’s technical vulnerabilities.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Bisexuality: Because Silk Road emphasized anonymity, profiles had no personally identifiable information including gender or sexual preference.</td>
<td>Because identity was not an issue, buyers and sellers could focus on the transaction without accounting for any pre-existing expectations or biases.</td>
<td>This system may be the one redeeming quality of Silk Road, in that it helped buyers and sellers focus more on products, and less on finding ideal buyers or sellers.</td>
</tr>
<tr>
<td>Territoriality: In the physical world, territories exist where sellers can freely sell their product, and where no other sellers can. Silk Road, a virtual environment, removed those boundaries.</td>
<td>Nonexistent physical boundaries may motivate sellers to offer products that are superior and makes buyers keep coming back.</td>
<td>Sellers may be able to see the potential this marketplace creates and could exploit its very lax environment with little to no governance, regulation, or technical controls. All this in an environment that’s hidden from the visible and commercial space of the internet.</td>
</tr>
<tr>
<td>Temporality: Silk Road took advantage of the power of the Internet, such as the ability to bridge the gap between buyers and sellers of illegal products or services, transacting and paying or accepting payments anonymously, all while withholding personally identifiable information on their profile.</td>
<td>Buyers and sellers were more likely to interact with those they didn’t know, since Silk Road removed both the barriers to entering the drug trade and risk in terms of physical harm.</td>
<td>With some foundational programming skills, and a few Google searches, copycats to the Silk Road market may become commonplace, as old ones are seized by law enforcement. These types of marketplaces are too convenient and a lot of criminal opportunities to be had for one or more Silk Road copycats not to exist.</td>
</tr>
<tr>
<td>Learning: Silk Road was not publicly accessible, so a technical learning curve may have existed for some users. However, once in the marketplace, any user who had created an eBay or Amazon account probably found Silk Road to be intuitive.</td>
<td>Accounts in Silk Road were similarly set up to its legitimate counterparts such as eBay or Amazon, which led to increased transactions based on positive reviews of both buyers and sellers.</td>
<td>Those who were first time users of Silk Road may have been taken advantage of in several ways. One method would be phishing, where a buyer may have legitimately asked around for information about Silk Road, but may have been sent a bogus email with malware or link to a bogus website.</td>
</tr>
</tbody>
</table>
Recreation and Humor: Some sellers and buyers may have tried out the Silk Road platform to see what type of business could be generated, so from a recreation perspective, it was just another market to sell in. In terms of humor, seller’s storefronts may have used this to attract, engage, and maintain its customer base.

For some legitimate sellers, Silk Road may be the only place where they can find an audience and market for their product or service.

Users who found that they could only buy or sell legitimate products on Silk Road may have been taking on too much of a risk, where they were conducting legitimate transactions next to illegal ones, unintentionally implicating themselves later.

Defense: A Tor browser allowed all users of Silk Road to help keep their location anonymous and keep Silk Road on the darknet; Bitcoin users to pay and be paid anonymously; and Silk Road didn’t require personal information to be tied into user accounts.

To keep all parts of Silk Road operating, the administrators should have split the business into different marketplaces, i.e., when they branched out the purchasing and selling of weapons to another website.

Using multiple layers of tools to prevent the identities, locations, and administrators of Silk Road pose a security challenge in that there is no control in place to hold users accountable for their actions. For example, if one user steals from another, there is no option for remediation.

Exploitation: When Silk Road existed, it had two distinct advantages over other online marketplaces: its ability to keep users anonymous, and for the marketplace to remain hidden from an otherwise publicly available Internet.

Silk Road may have been a place where buyers and sellers alike were exploited numerous times, perhaps most often when dealing with first time users.

Aside from a few rules about what can be sold or bought, Silk Road fostered marketplace where buyers and sellers transact at their own risk; holding no one, not even the marketplace’s administrator accountable.

<table>
<thead>
<tr>
<th>Table 1, A Cultural Analysis</th>
</tr>
</thead>
</table>

**Discussion**

The Internet has provided a method by which large distances and time (Territorial, Temporarily) are eliminated with the low cost of entry for access and are used to connect and relate with dispersed individuals (Backman, 2013). In the context of Silk Road this made it possible for drug subculture members to meet and arrange exchanges of goods, independent of geographical constraints to local neighborhoods and regions. In turn the low cost of communication amplified the positive feedback loop of buyers and sellers thereby increasing word of mouth and increasing the use of the site. When talking of the Silk Road subculture in the context of territorial analysis the area in use was what is known as the “deep web” (Johnson, 2014) since it includes all of the addressing space and websites not listed on commercial search engines such as Google and Yahoo. These deep web sites are cryptically named and while accessible to data packets may need special routing and encryption for users to see the relevant data. This was the case with Silk Road in that membership required a willingness to overcome legal and technological barriers in order to participate and thus provided exclusiveness into the Silk Road subculture. The sense of group was amplified by its founder Ross Ulbricht using the justification of libertarian political values to justify the illicit activities. Using the Silk Road site as his political and philosophical platform allowed for control over the membership personal views as his alternate world
view took hold and was reflected in member postings expressing similar views and support (Backman, 2013). This amplification falls under the cultural stream of “association” as well as incorporating “recreation” in the form of relaying usage stories, personal and political views.

The makeup of the Silk Road subculture was predominately white young males between 18 to 24 years of age and from the English speaking areas of the United States, England and Australia (Barratt, et al 2014). This category falls under the heading of “bisexuality” as it is focused on the gender issues for what is permitted between them. In this context the majority male group is supportive in methods of transport as well as use of drugs and while there appears to be black market trading in weapons the bulk of the transactions are narcotics found in club and disco settings. As such the cultural stream of “subsistence”, which embraces attitudes and ideas of what constitutes basic needs in life, is seen here in the aspect of drug use. The defining activity for the young male members of the Silk Road community exclude age related health problems and possible adverse reproductive issues of women and thereby allow for justification and mutual support for the consuming and trading activities. The processes used to provide for the subsistence beliefs are created within the Silk Road web site. This is shown by the interviews in which members detailed that community provided a wider range of drugs, better quality, more convenience and trusted sellers (Barratt, et al 2014).

Looking at the four aspects of range, quality, convenience and trust an understanding of the technical aspects to provide them is necessary. The Silk Road community would not exist without anonymity anymore than local criminal activities can occur in public spaces. Therefore, the “territoriality” and “temporality” benefits alone do not allow for criminal activity and rather the use of the cultural stream of “exploitation”, “defense”, and “learning”. In the context of exploitation two technologies, besides the low cost of communication, are the ability to hide location and destination of the internet traffic used in the Silk Road community (Tor) and pay for goods via an untraceable currency (Bitcoin). The Onion Router project or Tor was a construction from the Department of the US Navy as a means of providing oppressed groups around the world access to secure communications independent of the host country’s government (Backman, 2013). The Tor network works by providing host based encryption software and a list of access/exit route sites, which then encrypt each hop-by-hop route across the Internet independent of the underlying Internet routing. This then gives layers encryption (hence the idea of an onion) to each packet as it moves through the Tor network. The only known method to halt such use is to block the dynamically changing exit points from Tor on edge points to a service provider’s network (Johnson, et al. 2014; Dolliver, 2015). In order to pay for goods a virtual currency is desired, as it is not tied to any one nation state and thereby, allows for the bypassing of money laundering controls with banks. The Silk Road community used the Bitcoin currency as it was established and allowed for exchange into local currencies (Johnson, et al. 2014; Dolliver, 2015). These two combined tools for anonymity were then supported and taught to the community members as the methods to bypass law authorities and fall under the understanding of “learning” within the context of the cultural stream methodology (Backman, 2013). These technical tools become the target of control and disruption by authorities as they seek to know the identities of the participants.

The final element needed to provide a holistic understanding of the Silk Road subculture is that of trust as defined under the cultural streams of “interaction” and “association”. The security necessities of accessibility, confidentiality and integrity are provided for with the previously presented streams of “exploitation”, “defense”, “temporality” and “territoriality”. However, this does not explain the level of trust attained by Silk Road since anonymity does not in itself provide the buyer and seller with assurances that the transactions will compete fairly between both parties. In a physical market a seller will have personal contact with their community of buyers, participate in the local society and have a known location (Gregg and Scott, 2008). To provide a similar personal interaction to a diffuse population, eBay turned to the use of a rating system by which buyers and to a limited extend sellers could judge the quality of services, goods and buying experiences. All users benefit from the transparency seen, of not only their particular seller, but in general what is to be expected and asked for from buyers and sellers. This in turn allows for objective review of the process and removes the “anonymity” from the trust relation. This is unique as the participants are not known but their actions are and in providing this transparency trust is maintained. Such a system would be complicated and most likely inaccurate if placed into a physical form. The use of electronic technologies therefore allows for a new method of trust to form for non-trusting
participants. The success of such a rating system was seen in eBay research where there was an 80% probability of a repeat purchasing for those sellers with a high customer satisfaction rating (Gregg and Scott, 2008). The innovation that Silk Road brought to the online drug market was just such a rating system (Backman, 2013; Baratt et al, 2014), which allowed for now secured and anonymous users, buyers, and sellers to trust one another during their illicit activities.

Findings from the analysis using the cultural stream framework allow for the exposure of a potential method of disruption. Societies use technical tools and the sharing of such knowledge as a low societal changing impact, which modifies their culture over a period of time. As such the tools of Tor and Bitcoin allow for easy adoption by users wanting to participate with the online drug subculture and if such tools become unusable, other tools will be substituted. This leads to the insight that as the tools are compromised by authorities a pattern of cat and mouse will appear, with criminal parties moving to alternative methods or means to transact business. However, trust is necessary for any transaction to complete and it is in this culture stream of “interaction” that a method of disruption and reduction might be pursued. The Silk Road rating system provided the trust used in the community and as such any replacement site such as Sheep Market or Black Market Reloaded also needed some method of customer feedback. This feedback system did occur with the demise of Silk Road and manifested itself on these alternative sites with chat rooms dedicated to known good sellers of a particular product. Therefore as a method of compromise using the socio-technological approach of introducing a technology as a means to change the culture or in this instance reduce its use, the idea is to compromise the “trust” relationships of the subculture using the tools creating the trust. Leaving intact the technologies of anonymity the focus by authorities could focus on compromising the integrity of the seller rating system with disinformation leading to a “lack of trust”. Further, to disable the use of virtual currencies, in place of regulation, the use of injecting corrupting transactions, false profiteering scandals and publication of fabricated system breaches could be pursued as a means to discredit and attack the “trust” element found with users of the virtual currency. This disruption of trust could potentially lead illicit users to fall back onto traditional means of trust using traceable currencies, personal relationships and physical locations to transact business. Authorities would then be in a position to detect and prosecute using the current methods control.

Conclusion

It goes without saying that technology enabled white-collar crime is on the rise. In this paper we have undertaken a cultural and a normative analysis to understand the patterns of behavior associated with a criminal activity. It is important to understand these patterns since they provide a rich understanding of nuances related to how technology enabled crimes comes into existence and gets sustained over a period of time. Such an understanding is also useful in curtailing technology related criminal activities.

REFERENCES


