Criminogenic Asymmetries in Cyberspace: A Comparative Analysis of Two Tor Marketplaces

Diana S. Dolliver – University of Alabama

Katherine L. Love – University of Alabama

CRIMINOGENIC ASYMMETRIES IN CYBERSPACE: A COMPARATIVE ANALYSIS OF TWO TOR MARKETPLACES

Diana S. Dolliver and Katherine L. Love

Cyberspace presents a unique medium in which criminogenic asymmetries propagate, fueled by globalization processes that contribute to various forms of transnational criminality. The cyber domain challenges traditional criminological concepts related to the connection of 'space' and 'time', allowing offenders and victims to virtually interact despite their geographical locales. Further, structural discrepancies differentially impact cybercrime rates, as connectivity to the Internet remains restricted or inaccessible in many countries. This study conducted a descriptive assessment of criminality on two marketplaces housed on the Tor Network within the broader context of these cyber-structural discrepancies and asymmetries. Data were collected from Evolution and Silk Road 2 during August and September 2014 using webcrawling software. This study found illegal or criminally concerning items to be abundant on Evolution and modest on Silk Road 2, largely sold from a core group of culturally Western countries. Yet, an abundance of other countries were found to engage differentially in specific markets, though in smaller percentages.

Keywords: *criminogenic asymmetries, cybercrime, globalization.*

Introduction

Cyberspace presents unique opportunities for offenders to transfer activities from the physical world into the virtual, challenging many of the traditional criminological concepts related to the connection of 'space' and 'time'. The global community is becoming increasingly interconnected through the process of time-space compression (Appadurai 1996; Harvey 1990) in which the growing speed of communication and movement of capital is 'resulting in the "shrinking" of space and the shortening of time' (Aas 2007: 7). Offenders no longer need to be within close geographical proximity to their victims or customers; they can target potential victims for robbery or conduct illegal transactions while remaining thousands of miles away (Aas 2007). Further, within cyberspace a single person has the ability and potential power to be a credible threat to nation-states' security. These criminogenic 'asymmetries contribute in complex ways to the absence of adequate controls. In some cases there are simply no controls at all' (Passas 1999: 403). Indeed, law enforcement officials around the world have struggled to adapt to the pervasiveness of cybercrimes that often traverse jurisdictional borders, as criminal activities on the Internet have continued to increase since the 1990s with sharp escalations reported in more recent years (FBI IC3 2013).

Structural discrepancies by way of simple global access to the Internet also impact crime in the cyber domain. As of 2014, roughly 42 per cent of the world's population

was connected to cyberspace (IWS 2015). As this percentage continues to increase each year, opportunities likewise expand to trade goods and services online easily and without pause for national boundaries. Elements of various cultures, both tangible and otherwise, are being diffused around the world as cyber-related glocalization (Robertson 1995) continues to become more pervasive. That is, the local is coming to terms with the global, and the global is becoming more expressed within the local. However, this trend is not uniformly impacting every region. While North America, Europe, and Oceania experience Internet connectivity rates ranging between 71 per cent (Europe) to 88 per cent (North America), only roughly of 33 per cent of populations in Africa, Asia, and the Middle East have routine online access (IWS 2015). This Internet connectivity balance is reflective of resource dispersion among countries, in addition to political approaches to cyberspace. Modern Western democracies not only have the resources necessary to build the infrastructure required to provide universal Internet access, but these countries also do not restrict their citizens' access to content on the Internet.[1]

However, scholars have yet to understand how these global cyber-structural discrepancies and asymmetries impact or are reflected in various macro-level trends in cybercrime markets. The majority of past studies on Internet-driven crimes have focused on cyber victimization related to cyber-stalking and online harassment (*e.g.*, Halder and Jaishankar 2011), malicious software infections (*e.g.*, Bossler and Holt 2009), and identity theft (*e.g.,* Reyns 2013) from largely micro-level theoretical perspectives (Broadhurst *et al.* 2014; Lipton 2011; Navarro and Jasinski 2012; Ngo and Paternoster 2011; Pratt, Holtfreter, and Reisig 2010; Reyns *et al*. 2011). Additionally, the vast majority of previous cybercrime-related research has been limited to the 'clearnet' (*i.e.*, the open Internet). Few studies have investigated criminality on other corners of the Internet (*e.g.*, the Tor Network) that provide users with additional security protections, allowing them to browse, shop, and host businesses online with seemingly complete anonymity. Importantly, these networks such as Tor are accessible even to those residing in countries with the strictest government-imposed Internet limitations.[2]

As such, this study sought to conduct a descriptive assessment of the scope of criminality on two popular online marketplaces housed on the Tor Network within the broader context of these cyber-structural discrepancies and asymmetries. These marketplaces, Evolution and Silk Road 2, were analyzed comparatively in terms of the types and volumes of items sold in addition to geographic patterns among countries of origin. At the time of this writing, both Tor marketplaces have since been dismantled and are no longer in operation, but were until recently[3] Tor sites that attracted a variety of vendors advertising and selling broad ranges of items (*e.g.*, drugs, software, stolen data, weapons) originating from over fifty countries combined. This in depth comparative analysis will significantly contribute to the related literature by advancing the understanding of the global availability of illicit goods and services on an online network that defies governmental controls but remains impacted by cyber-structural discrepancies and asymmetries.

The Tor Network and its Marketplaces

The Tor Network is accessible only once the free Tor anonymizing software has been downloaded. A series of rendezvous points set up by Tor nodes inside the Tor Network

ensures Tor users' identities are kept untraceable and unidentifiable (Christin 2012).[4] The U.S. Naval Research Laboratory originally deployed the Tor Network in 2010 as a third-generation onion routing project with the 'primary purpose of protecting government communications' (Tor Project 2014a: 1). To-date, the Tor Project (2014a) notes that their network provides secure Internet access to individuals living in oppressed nations, it allows journalists to 'communicate more safely with whistleblowers and dissidents' (1), and it enables law enforcement officials to covertly gather intelligence. The enhanced levels of secure, anonymous access provided by the Tor Network have enticed these new users to join Tor (Aldridge and Decary-Hetu 2014); yet, a portion of these users operate outside of the legal realm.

The popularity of the Tor Network has undoubtedly grown since its inception in 2010. Since this time, individuals have created thousands of websites (*i.e.*, 'marketplaces') using the *.onion* domain that have been likened to 'e-Bay' and Amazon (Barratt 2012), where vendors post legal and illegal goods and services for sale while customers browse and shop at their leisure in a free-market environment. The network experienced a peak in user-connectivity in October 2013 following the U.S. federal arrest of Ross Ulbricht,[5] owner and operator of the largest and most popular marketplace on Tor at the time, Silk Road (Grossman and Newton-Small 2013). This high profile arrest received international media attention, temporarily spiking the number of directly connected users on Tor from 900,000 to 5.6 million (Dolliver 2015a); the number of daily users has since reverted to a new mean of approximately 2.3 million. While the number of daily Tor users is much fewer than average number of daily open Internet users worldwide (estimated in 2014 at 3 billion), past research has indicated the concealment of identities afforded to Tor users provide additional motivation for some individuals to use this network in place of the clearnet to engage in criminal activities (*e.g.*, Barratt *et al.* 2014; van Hout and Bingham 2013a, 2014).

Supporters of Ulbricht and his marketplace's business model later developed the successor to the Silk Road, aptly named Silk Road 2. Other popular sites were also created (*e.g.*, Agora, the Farmers Market, the Outlaw Market, the Armory, Blue Sky, and Pandora), including Evolution, which was launched on January 14th, 2014. These marketplaces grew and evolved throughout 2014, offering a diverse array of items for sale including everything from drugs to weapons, stolen data, and clothing items. Evolution came to replace the original Silk Road as one of the largest and most popular marketplaces, though Silk Road 2 enjoyed hosting a smaller vendor-base loyal to its namesake (Dolliver 2015a, 2015b). However, this increase in marketplace activity also attracted the attention of law enforcement agencies worldwide. On November 5th, 2014 U.S. and European federal law enforcement agencies shut down Silk Road 2, seizing the site's servers and arresting Blake Benthall, the marketplace's 26-year-old alleged operator (FBI 2014a). Pursuant to U.S. federal forfeiture laws, the arrest of Benthall led law enforcement to seize additional servers hosting over 400 *.onion* domain names (FBI 2014b). These particular sites included dozens of other marketplaces (*e.g.*, Hydra, Executive Outcomes, Blue Sky, and Cloud Nine); however, Evolution as not shut down in this operation. The site did, though, go offline on March 18th, 2015 and remains down. It has been assumed that the Tor site's operators shutdown the website without warning in an apparent exit scam, robbing vendors of allegedly million worth of Bitcoin (Fox-

Brewster 2015). Nonetheless, this research sought to study criminal activity that was present on Evolution and Silk Road 2 while the sites were functioning in 2014. Both sites were identified for use in the study by their former popularity on Tor, and data were collected while the sites were operational.

Criminogenic Asymmetries and Cyberspace

Criminogenic asymmetries, defined as 'structural discrepancies, mismatches, and inequalities' in various realms including law, politics, culture (Passas 1999: 402), are also present in the cyber domain. These asymmetries are intensified by globalization processes (Passas 1999) and can lead to crime:

(1) By fuelling the demand for illegal goods and services;

(2) By generating incentives for people and organizations to engage in illegal practices; and

(3) By reducing the ability of authorities to control crime (*Ibid.*: 402).

In the late 1990s, Passas observed the impact that globalization had on such asymmetries in the physical realm. That is, globalization 'reinforce[d] inequalities of power and wealth both within nation-states and among them' (*Ibid.*: 406). This tendency towards universalism (whereby cultural identities become 'disembedded' [*Ibid.*: 405] as a result of globalization) is often countered with varying degrees of resurgences in nationalism and emphasizing ethnic identities (Harvey 1990; Passas 1999). This, in turn, created conflicts and contradictions between the local, national, and global perceptions of universal cultural goals. Nations experiencing heightened structural and cultural contradictions, Passas (1999) surmised, would subsequently encounter increasing volatility of asymmetries and likelihood for transnational crime.

Cyberspace, which contains an 'integral part of the transnational threat landscape' (McCusker 2006) by way of cybercrime, has since spurred on the rate at which national borders continue to disintegrate as contact among previously isolated groups increases. Indeed, the cyber realm is one in which scholars have already begun to observe aspects of criminogenic asymmetries in the form of robust demand for illegal goods and services (*e.g.*, drugs sold via illegal online pharmacies [FDA 2012; Mackey and Liang 2011a] and stolen electronic data [Dolliver 2015a]). The cyber domain also offers new opportunities for individuals to engage in illegal practices, such as cyber stalking and harassment (Halder and Jaishankar 2011) and identity theft (Reyns 2013), which are not restricted by traditional notions of 'space' and 'time'.

Indeed, the ability to browse and shop online encapsulates the time-space compression (Appadurai 1996) as consumers can now buy directly from their sources while remaining thousands of miles away. Online drug sales have undoubtedly received the most attention from scholars (*e.g.*, Aldridge and Decary-Hetu 2014; Barratt *et al.* 2014; DEA 2005; Mackey and Liang 2011a, 2011b; Molnar *et al.* 2010; Walsh 2011). Marijuana was reportedly one of the first items ever to be sold online via the ARPANET in the early 1970s (Markoff 2005; Walsh 2011) and continues to be a main drug of choice for online consumers (Christin 2012). However, a recent study highlighted the increasing demand for stimulants, other hallucinogens, and narcotics in an online Tor venue (Dolliver 2015a). Particularly on the Tor Network, researchers have consistently noted a clear bias toward vendors representing and shipping these drugs from English speaking

countries (*e.g.*, the United States, the United Kingdom, Canada, and Australia) to users worldwide (*e.g.*, Christin 2012; Dolliver 2015a).

Studies have also shown that the cyber domain, and in particular, the Tor Network, has generated added incentives for people and criminal organizations to use this network in place of clearnet websites or traditional offline methods (Barratt *et al.* 2014; Martin 2014; van Hout and Bingham 2013b, 2014). Both self-proclaimed 'drug connoisseurs' and vendors touted anonymity to be the chief motivating factor behind their preference for Tor, in addition to the ease and security of transactions on Tor marketplaces such as Silk Road (van Hout and Bingham 2014). These online marketplaces in general offer customers user-friendly features and added security that reduce the likelihood of detection by law enforcement. Further, the cyber domain enables individuals to use cryptonyms, decentralized exchange networks, and encrypted cryptocurrencies to further conceal user identities (Martin 2014). These generate added incentives to conduct illegal operations in the cyber realm that have resulted in an expansive online pharmacopeia and ever-increasing rates of cyber victimizations (*e.g.*, Hunt 2011; Pyrooz *et al.* 2015; Reyns 2013).

Further, the cyber domain itself by its very nature reduces the ability of authorities to control crime in this medium. The international community, therefore, is experiencing a state of dysnomie with regards to combating cybercrime worldwide. 'Dysnomie', meaning 'difficulty to govern', occurs when three conditions are present (Passas 2000: 37): 'a lack of a global norm-making mechanism, inconsistent enforcement of existing international rules, and the existence of a regulatory patchwork of diverse and conflicting legal traditions and practices'. Among the 82 countries that have enacted some form of cybercrime initiative, laws governing cyberspace consist of national, regional, and international legal systems that interact and diverge at multiple levels (UNODC 2013). Many countries struggle with providing legal guidance for online behaviors, and in some cases, countries have not addressed legality in cyberspace at all (*Ibid.*). Internationally, some goods and services sold online are outlawed in some countries, but not others (*e.g.*, rocket launchers, marijuana); some online practices are illegal in some countries, but not others (*e.g.*, operating an online pharmacy). Tangible items purchased online must be shipped via national or international parcel carriers, thus further reducing the likelihood of detection and interception. These elements taken together create legal contradictions that compound jurisdictional problems for law enforcement entities worldwide.

Passas (1999, 2000) concluded that countries experiencing increasing levels of these legal and cultural contradictions that produce dysnomie likely lead to higher levels of transnational criminal activity. Cyberspace and its various dark corners present a unique platform in which to investigate such criminality within this broader context of asymmetries; that is, the cyber domain greatly facilitates (legal and illegal) global commerce and communication, further compressing and altering traditional notions of 'time' and 'space'. Yet, access to this domain is restricted structurally (IWS 2015). This, in turn, differentially impacts the ability to interact within this particular venue. Given this theoretical context, this study sought to comparatively analyze the scope of criminality (measured as the level of geographic engagement by vendors selling crimi-

nally concerning items) on two popular online marketplaces housed on one corner of the Internet that provides additional security-related incentives for users: the Tor Network.

Methods

The Tor marketplaces selected for this comparative analysis were based largely on popularity of use (determined through sites including Reddit and TorChat) in order to capture a broad range of vendors advertising and selling a large variety of items for sale. The specific data collection methods employed in this study were similar to those used by Dolliver (2015a, 2015b) and others (*e.g.*, Aldridge and Decary-Hetu 2014; Christin 2012). A free webcrawling software program was used to collect publically available, self-reported data from both Tor sites. This software assembles the downloaded or 'mirrored' websites by the original site's link structure (*i.e*., the internal assembly of the website that includes the various paths to content connected by links) and allows browsing of the mirrored site by opening a static copy of the page as if viewing the site online. The software is also fully configurable, allowing for filtering (*i.e*., inclusion and exclusion) of content. In this study, the software program was instructed to capture HTML text only, omitting the mirroring of images as this substantially slows down the progress of the crawling software.

In order to ensure the precision of the webcrawler (*i.e.*, confirming the software was accurately mirroring every page of the website without skipping or missing pages), a series of daily partial and full 'test crawls' were conducted on Evolution and Silk Road 2 beginning in early August 2014. This step was labor intensive since each Tor site had a different link-structure. As a result, HTTrack had to be reconfigured for each site to accurately capture each webpage. After each test crawl, additional measures were taken to further ensure the webcrawling software was performing properly (*e.g.*, logging on to the live website, clicking page by page to ensure continuity with the mirrored pages). In early September 2014, Silk Road 2 was mirrored for use in this study, taking approximately 7 hours and 18 minutes. The Evolution marketplace took much longer to crawl, requiring 14 hours and 42 minutes to complete in mid-September 2014.

Items advertised (along with the advertisement's associated information on vendors, shipping methods, *etc*.) on Silk Road 2 and Evolution were sorted based on their respective categories (*e.g.*, 'drugs', 'erotica', 'hallucinogens', and 'guides') given on each Tor marketplace. That is, website operators on both Evolution and Silk Road 2 provided separate categories to house advertised items for sale; vendors then selected which category to list their items under when creating a new advertisement. However, the categories were not mutually exclusive (*e.g.*, 'weed' was a separate category from 'cannabis') and many vendors did not select the category that accurately reflected the item they were selling (*e.g*., stolen credit card information for sale was listed for sale under 'alcohol' category). As such, the data required additional cleaning and coding to accurately represent the scope and depth of each marketplace.

This study coded all items for sale on both Silk Road 2 and Evolution into twelve categories: drugs (excluding tobacco and alcohol), drug paraphernalia, weapons, ebooks (*e.g.*, digital 'how to' manuals), erotica, software (excluding hacking software), hardware, custom (an anonymous category in which the vendor does not identify anything specific for sale, but instead lists only 'custom order' and a price), counterfeit or stolen

data (including real and fake ID cards, passports, and stolen personal information including credit card numbers, emails, names, and addresses), hacking software, tobacco and alcohol, and other (including apparel, children's toys, and other miscellaneous items).

Results

This study sought to investigate criminality on two Tor marketplaces within the broader context of global criminogenic asymmetries. The first set of results discuss the comparative analyses of the volume and range of items actively advertised and sold on Silk Road 2 and Evolution. Next, the geographic analysis of the two marketplaces' is presented, providing a global context for the various criminally concerning items advertised and sold.

Item Analysis: Silk Road 2 and Evolution

While Evolution and Silk Road 2 were touted as two popular illicit marketplaces on the Tor Network, Evolution proved a much larger site than Silk Road 2 in terms of the volume, quality, and range of items for sale. Silk Road 2's site and its operators reported over 12,000 available drug items for sale (*e.g.*, 1,322 listings for stimulants, 1,676 for psychedelics, and 3,319 for prescription items in Figure 1) (FBI 2014a); however, Silk Road 2 totaled only 1,834 active, publically available listings on the date the data were mirrored (Dolliver 2015a, 2015b).[6] Comparatively, this study found 16,054 active listings on Evolution at the time of data collection, indicating Evolution to be a much larger, active marketplace (Figure 2).

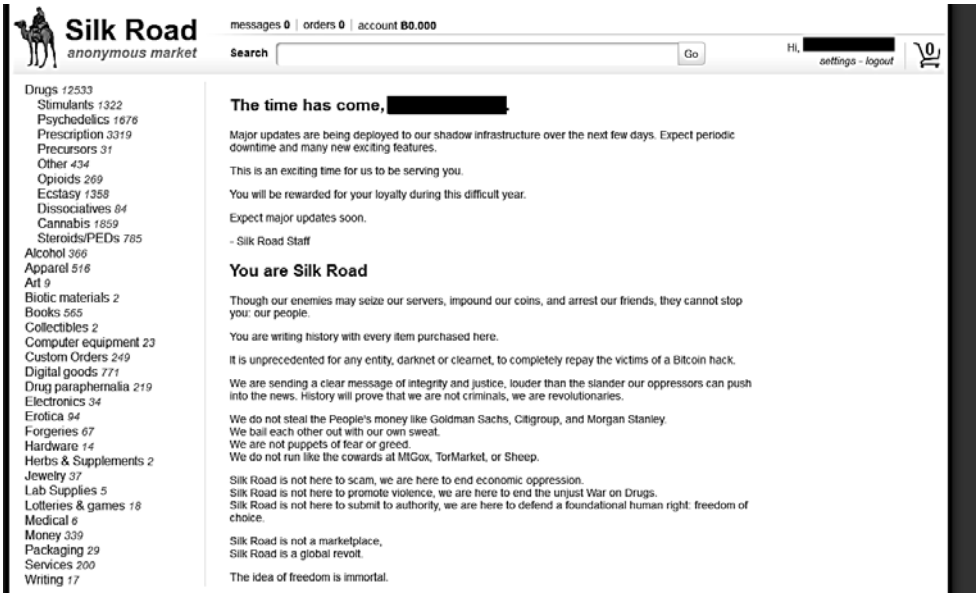

Fig. 1. Screenshot of Silk Road 2, 2014

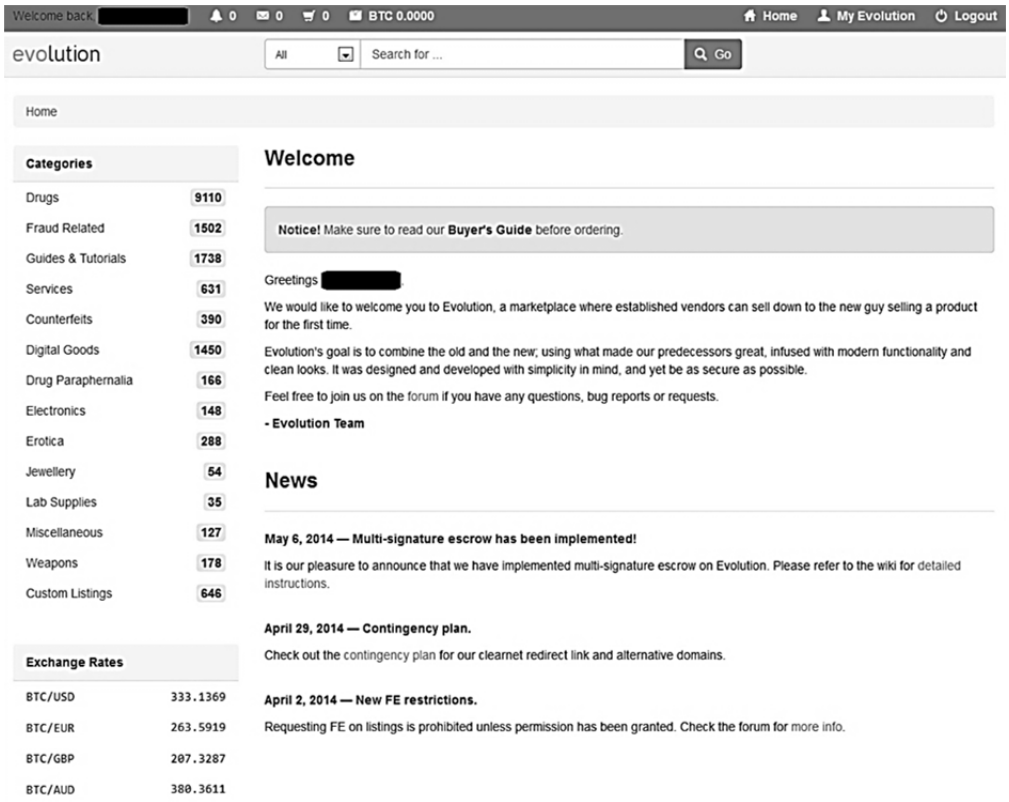

Fig. 2. Screenshot of Evolution, 2014

Table 1 provides a breakdown of the number and percent of total active items by category available on Silk Road 2. Of the twelve categories of coded items on this site, the 'other' category (consisting of miscellaneous items, such as wristwatches, clothing articles, and 'Facebook photo likes') comprised the majority of items for sale with 482 item listings. The second most popular category was ebooks (mostly 'how to' manuals and other digital downloads), followed by drug items, and counterfeit or stolen data (*e.g.*, forged passports, driver's licenses, and other forms of identification, counterfeit money, and databases containing stolen identities and financial accounts). The number of items for each of the remaining categories significantly drops off.

Table 1

Silk Road 2

Category of Item for Sale	# of Active Items	% Total Active Items
1	2	3
Other	482	26.28
eBooks	368	20.07
Drugs	348	18.97
Counterfeit or Stolen Data	328	17.88
Hacking Software	86	4.69
Custom	61	3.33
Drug Paraphernalia	38	2.07

1	2	3
Other Software	34	1.85
Hardware	31	1.69
Tobacco/Alcohol	29	1.58
Erotica	27	1.47
Weapons	2	0.11
Total:	1,834	

Providing a similar breakdown of the numbers and percentages of items by category, Table 2 indicates that in contrast to Silk Road 2, drugs were the vastly dominant category of item for sale on Evolution with over half (53 per cent) of the active listings. Trailing significantly as the second most popular category was ebooks, followed by counterfeit or stolen data, 'other' miscellaneous items, and custom listings. Each of the remaining seven categories accounted for less than 2 per cent of the active listings indicating that, at the point of data collection Evolution was a vibrant drug marketplace.

Table 2

Evolution

Category of Item for Sale	# of Active Items	% Total Active Items
Drugs	8,577	53.43
eBooks	2,254	14.04
Counterfeit or Stolen Data	1,902	11.85
Other	1,094	6.81
Custom	702	4.37
Other Software	312	1.94
Erotica	306	1.91
Drug Paraphernalia	244	1.52
Hacking Software	222	1.38
Weapons	208	1.3
Tobacco/Alcohol	140	0.87
Hardware	93	0.58
Total:	16,054	

Both Tor sites offered ample opportunities for customers to purchase a wide variety of illegal goods and services; however, criminal opportunities in this particular sales form were found to be more limited on Silk Road 2's website when compared to Evolution. That is, the top two categories on Silk Road 2 (*i.e.*, 'other' and ebooks) mostly consisted of items that could be legally purchased and were readily available on clearnet sites and/or found in brick and mortar stores. For instance, items in the 'other' category mostly included replicas of Canada Goose men's and women's clothing, Cartier jewelry, Chanel sunglasses, and Dior products, while items in the 'ebooks' category were downloadable 'how-to' guides on anything imaginable – from how to identify hallucinogenic plants to versions of the anarchist cookbook. While themes of these guidebooks included additional arguably concerning topics like bomb making, evading police detection, and how to hack various types of networks, all of these *.pdf* files were also available for purchase (or free to download) in other online venues. Further, sales or downloads of

these items may not have been specifically illegal depending on the country's legal context.

Evolution, on the other hand, provided ample opportunities to purchase illicit items, as evidenced by the overwhelming amount of drug-related items for sale. While not the case in many European countries, in the United States, the simple act of advertising the sale of a controlled substance violates federal law in addition to the transaction itself (Ryan... 2008). Additionally, the majority of drug items for sale consisted of stimulants (*e.g.*, cocaine, methamphetamine) and hallucinogens[7] (*e.g.*, research chemicals, inhalants, LSD, Ketamine), illustrating a 'harder' drug market than was found on the original Silk Road (Christin 2012). Yet, similarly to Silk Road 2, the 'ebooks' category was well represented among historic transactions on Evolution, containing largely legitimate items sold.

However, criminal potential lies not only within the legality of items sold, but also within the criminal prospects inherent in the items once they are sold. That is, some items (whether legally or illegally sold) may facilitate future criminal behavior more so than others. For instance, it is not illegal to sell used Soviet-era rocket launchers in some countries (*e.g.*, Poland), liquid mercury, or uranium ore (see Figure 3); however, these items have a high probability of being employed for criminal or deviant purposes following the sale. Criminality in this form was also found to be more substantial on Evolution than Silk Road 2. Weapons for sale abounded on Evolution, including STEN MKII 9mm fully automatic submachine guns, 16" AR-15 kits, magnesium fuses, and grenade launcher ROS shrapnel. AK-47 30 round magazines were available by the hundreds for purchase, as were software programs for 3-D printable guns (tested as functional, according to the vendor), steel iron knuckles, iPhone tasers, and various forms of explosives (*e.g.*, Delova Rana 75mm, Zink Bodenblitz 751–1). Comparably, Silk Road 2 only offered concealable body armor. While the vast majority of these items are legal for purchase (given varying restrictions in various countries), the range of legitimate purposes is questionable.

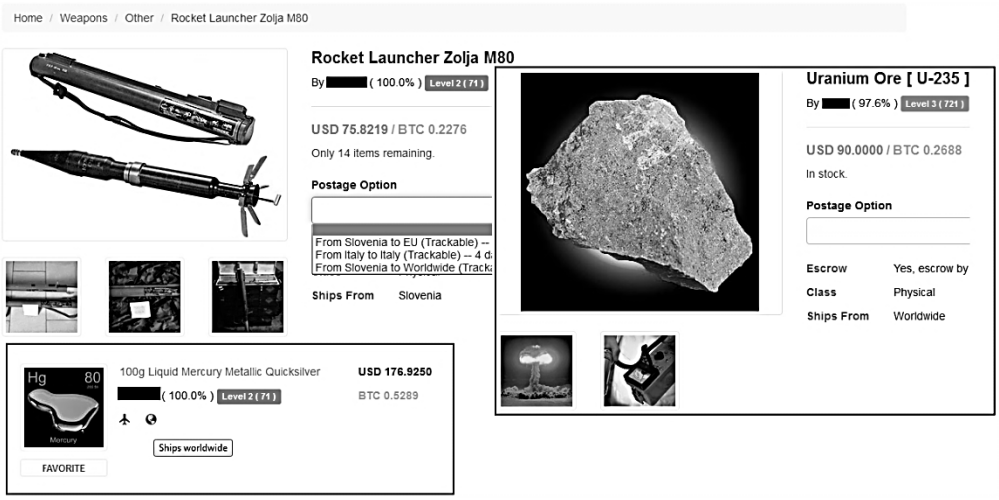

Fig. 3. Screenshots from Evolution, 2014

Apart from drugs and weaponry, Evolution also offered 'NSA email contacts megalists' for sale, in addition to counterfeit passports from a broad range of countries and sales of large data dumps containing stolen social security numbers, full names, dates of births, phone numbers, and addresses for many thousands of people. Silk Road 2 offered fake drivers licenses and passports from many countries and U.S. states, but other than lower-grade pyrotechnics, this Tor site's 'criminally concerning' inventory did not match that of Evolution's in depth or scope.

The findings of this item-based analysis offer support for the advancement of the time-space compression (Appadurai 1996) through the facilitation of global commerce of a broad range of illegal (or legal, yet criminally concerning) items advertised and sold on Evolution, and to a lesser degree, Silk Road 2. Customers can indeed browse and shop directly from their sources in a virtual environment that offers added protections against discovery of users' identities and/or law enforcement interdiction. This further challenges traditional notions of 'time' and 'space', in which criminal transactions can occur without the necessity of close spatial proximity.

Geographic Analysis: Silk Road 2 and Evolution

Of particular interest to this study are the global geographical representations for illegal and/or criminally concerning items sold on Evolution and Silk Road 2. According to Passas (1999, 2000), a higher degree of 'structural discrepancies, mismatches, and inequalities' (Passas 1997: 402) experienced by various countries should subsequently lead to higher levels of transnational criminal activity in these locations. While these asymmetries also impact criminal activity in the cyber domain, structural barriers preface individuals' access to the Internet in various countries. Within this context, this analysis compared and contrasted criminal activity based on the countries of origin (identified by the vendors themselves) for all advertised items on both Tor sites, followed by an item-based geographical breakdown.[8]

Twenty-four separate countries were identified as points of origin for all items advertised on Silk Road 2. Items advertised on Evolution originated from 46 distinct countries. Tables 3 and 4 below display the top 10 countries of origin for each site's currently advertised and historically sold items, in addition to 'undeclared' and 'worldwide' categories. These latter source designations given by vendors accounted for between 40 and 48 per cent of all points of origin on both Tor marketplaces – a significant amount of listings on both sites. However, electronically delivered items (*e.g.*, eBooks, stolen data, and software) accounted for the majority of the items listed as shipping from an 'undeclared' source (see Appendices B and C). Interestingly, there does appear to be an over-representation of English-speaking countries in line with past Tor marketplace research (Christin 2012; Dolliver 2015a). Indeed, the vast majority of listings on both Tor sites were in English, though other languages (*e.g.*, German, French, and Dutch) were also present. The United States, the United Kingdom, Canada, and Australia are well represented on both marketplaces as locations of origin. However, China (including Hong Kong[9]) was also found to have a moderate-to-strong presence on Evolution and Silk Road 2 despite an estimated 46 per cent connectivity rate (IWS 2015) and high levels of governmental control over China's Internet. This indicates that a substantial percentage of citizens in China are accessing and using the Tor Network despite the Chinese government's Internet-based restrictions to participate in these marketplaces.

Table 3

Frequency of Items for Sale on Silk Road 2 by Top 10 Countries of Origin

Country of Origin	# of Active Items	% Total Active Items
Belgium	309	16.85
China	185	10.09
United States	166	9.05
United Kingdom	113	6.16
Hong Kong, China	102	5.56
Australia	67	3.65
Germany	61	3.33
Canada	26	1.42
Netherlands	22	1.2
Switzerland	8	0.44
*Undeclared**	*740*	*40.35*
Total	1,834	

Table 4

Frequency of Items for Sale on Evolution by Top 10 Countries of Origin

Country of Origin	# of Active Items	% Total Active Items
United States	2,293	14.28
United Kingdom	1,207	7.52
Netherlands	1,094	6.81
Germany	1,008	6.28
Canada	561	3.49
Australia	457	2.85
China	298	1.86
Hong Kong, China	279	1.74
Poland	166	1.03
France	158	0.98
Worldwide	*7,756*	*48.31*
Blank	*4*	*0.02*
Total	16,054	

When the separate categories of items advertised and sold on Evolution and Silk Road 2 were analyzed based on their country of origin (as identified by each vendor), interesting patterns emerged. Among the drug listings for both sites, 19 countries were identified as countries of origin for vendors on Silk Road 2 and 41 countries of origin were identified on Evolution (Appendix A). The U.S., the U.K., Germany, the Netherlands, Canada, and Australia composed the majority of self-identified sources for drugs on both Tor marketplaces. This overlap in country-representation and participation in the drug markets on both Silk Road 2 and Evolution is particularly interesting given that Silk Road 2 overall was not primarily a drug market as Evolution was found to be (*i.e.*, Tables 1 and 2). On Silk Road 2, a small percentage of vendors identified origins including India, Bulgaria, Slovenia, Denmark, and Spain for active drug listings. Even more significant was the broad range of countries of origin identified on Evolution that

have substantial ties to traditional drug trafficking operations (UNODC 2010), including Guatemala, Mexico, Columbia, Malaysia, Cambodia, Singapore, and Thailand. While combined these latter countries only accounted for a small percentage of active listings on Evolution, these countries were nevertheless found to have an active presence in the drug market on this particular Tor site at the time of data collection.

Smaller ranges of countries were found for the remaining categories of items advertised and sold on both Silk Road 2 and Evolution. For instance, regarding ebooks Belgium and the United States were the only two separate countries identified by vendors as countries of origin on Silk Road 2 (21 per cent and 3.8 per cent, respectively, of active listings for this category) (Appendix B). On Evolution, the U.S. and the U.K. were the top countries of origin for this category (3.8 per cent and 4.2 per cent, respectively), with Australia, Columbia, China, India, Italy, and the Netherlands represented by much smaller percentages of listings (all less than 1 per cent). It should be noted, though, that the nondescript 'worldwide' (on Evolution) and 'undeclared' (on Silk Road 2) points of origin composed 91 per cent and 75 per cent of active listings for ebooks, respectively. This failure of vendors to identify a separate country of origin was most likely due to the nature of the items for sale in this category; that is, these digital 'how-to' manuals were instant digital downloads for little or no cost.

For items in the 'counterfeit and stolen data' category, 16 separate countries of origin were identified for Evolution while only 5 were identified for Silk Road 2 (Appendix C). On Evolution, the U.S., U.K., and Australia were the countries found to be engaging the most in this particular category (between 1–4 per cent of active listings for this category). Smaller percentages of listings (less than 1 per cent of active listings) also included Columbia, Argentina, Germany, China, Bosnia, Canada, Malaysia, and Romania. The 'worldwide' point of origin composed 91 per cent of the active listings for this category of items on Evolution, again most likely due to the digital nature of the items for sale. On Silk Road 2, 'undeclared' origins composed 58 per cent of active listings for counterfeit and stolen data, in addition to Belgium, the U.S., Canada, Australia, and Poland.

Weapons and hacking software-related items are of particular concern for their potential to be used in the commission of a crime. Though these two categories did not compose more than 5 per cent of active or historic listings on either site, their countries of origin were further investigated. Weapons listings on Evolution originated from ten different countries, including the U.S., Austria, Germany, Sweden, and China. The 'worldwide' point of origin accounted for 50 per cent of active weapons listings, most likely selected by the vendors to further conceal their identities from law enforcement detection. Only two weapons listings were found on Silk Road 2 at the point of data collection, originating from Israel and 'undefined'. Hacking software originated from four separate countries on Evolution: the U.K., U.S., Australia, and Columbia; however, 'worldwide' accounted for 95 per cent of active hacking software-related listings. The market for such software on Silk Road 2 was much smaller, with only vendors from Belgium and the U.S. identifying these countries as points of origin. Vendors listed 'undeclared' origins in 71 per cent of active listings for this category.

The 'other' category, containing largely non-criminally concerning miscellaneous items (*e.g.*, clothing, Facebook 'likes', and sunglasses) originated from 13 countries on

Evolution and 10 separate countries on Silk Road 2 (Appendix D). Unlike the other categories, China (including Hong Kong) was the main points of distribution on both Tor marketplaces (roughly between 24–36 per cent of listings on the sites for this category). Belgium, the U.S., U.K., Australia, Canada, and the Netherlands were also represented in smaller percentages (each under 11 per cent of active 'other' listings) on Silk Road 2 and Evolution. Evolution also saw limited market engagement (less than 1 per cent of 'other' listings) from vendors in Thailand, Germany, Spain, Columbia, Ghana, and Poland.

Across these categories, whether the items were frequently advertised or otherwise, or whether the items were criminally concerning or not, patterns among countries emerged. Consistently, the United States, Canada, Australia, and the United Kingdom were identified as countries of origin for the majority of active listings, indicating high rates of market engagement from vendors in these countries. Indeed, the United States was listed as a country of origin for items in every category on Evolution, and in all but three categories on Silk Road 2 (*i.e.*, weapons, erotica, and other software). However, when categories of items were further examined in a geographical context, there was much more country variation and representation among drug listings, counterfeit and stolen data, and weapons (particularly on Evolution).

Discussion and Conclusion

Globalization processes advance the compression of time and space with the increasing speed of communication and movement of capital (Appadurai 1996); around the world, national borders become progressively fluid as contact with previously isolated groups increases. The rate of this resulting glocalization (Robertson 1995) has particularly been driven by the developments in and use of the cyber domain, and challenges traditional criminological concepts related to the connection of 'space' and 'time'. Criminals have found a new medium in which to operate, one that does not require them to be in the same geographical vicinity as their victim(s) or customer(s). This complicates law enforcement efforts to address and curb such activity, resulting in a dysnomic (*i.e.*, difficult to govern) environment (Passas 2000).

Additionally, access to cyberspace is not uniform across countries; instead, structural restrictions related to political control of the domain in addition to cyber-based infrastructural limitations in various countries inhibit more universal participation. These discrepancies and inequalities in law, politics, and culture (Passas 1999) define criminogenic asymmetries that exist in the cyber domain and have been surmised by past scholars (Passas 1999, 2000) to increase the likelihood for participation in such global criminal activities. However, researchers have yet to explore online criminality, a noted 'integral part of the transnational threat landscape' (McCusker 2006), from this perspective.[10] As such, this study sought to investigate criminality on two Tor Network marketplaces (Silk Road 2 and Evolution) within the broader context of these criminogenic asymmetrical elements. Criminality was measured as the level of geographic engagement of vendors advertising and selling criminally inclined items on each marketplace. That is, Evolution and Silk Road 2 were examined based on type of items sold on each site and then further analyzed for geographical patterns among the items to better un-

derstand levels of global distribution by vendors within the larger context of asymmetrical and structural variations.

Upon analysis, three notable sets of findings were uncovered in this study. First, this research found that criminally concerning items advertised and sold differed between the two Tor sites in terms of their volume and range. More specifically, at the point of data collection Evolution distributed mostly drug-related items (53 per cent), while Silk Road 2 advertised and sold mostly items coded as 'other' (*e.g.*, Facebook and YouTube 'likes', clothing items, perfumes) (26 per cent) and 'ebooks' (*e.g.*, *.pdf* 'how-to' manuals on countless topics) (20 per cent). These later items on Silk Road 2 contained limited concerning material (*e.g.*, bomb building and police evasion guides); however, the majority of items were readily available for purchase or download on clearnet sites and neither such transactions nor items were particularly criminal in nature. This was not the case on Evolution; a myriad of illicit drugs were advertised and sold, with the majority of drug-related items consisting of stimulants (*e.g.*, cocaine, methamphetamine) and synthetic hallucinogens (*e.g.*, research chemicals, inhalants, LSD, Ketamine). Evolution was also found to house more inventory with inherent criminal prospects than what was found on Silk Road 2. In other words, many more items (whether legally or illegally sold) on Evolution were found that had a high probability of facilitating future criminal behavior, including grenade launcher ROS shrapnel, uranium ore, stolen U.S. Social Security Numbers (SSNs), 16" AR-15 kits, stolen NSA employee information, and a range of various explosives.

The second notable finding of this study indicated that while in total, all items advertised originated from 46 countries on Evolution and 26 countries on Silk Road 2, much overlap was found among a smaller, 'core' group of countries representing a large percentage of the marketplaces. That is, the U.S., the U.K., Canada, and Australia comprised the majority of vendor-identified sources for items on both Tor marketplaces. These findings are particularly interesting given that Silk Road 2 was not primarily a drug market as Evolution was found to be; different dominant markets would suggest different global patterns to emerge specific to each market, yet this was not found to be the case in the majority of item-based categories[11] on both Tor sites.

This set of findings also illustrates a more pervasive English-speaking market on Evolution and Silk Road 2, which is consistent with past research (*e.g.*, Dolliver 2015a; 2015b); however, these findings are also congruent with larger structural Internet connectivity patterns. That is, connectivity rates as a percentage of the population in the U.S., the U.K., Germany, the Netherlands, Canada, and Australia ranged between 86 to 96 per cent in 2014 (IWS 2015), indicative of near universal access. The findings of this study might, then, appear to be based on simple opportunity and availability of the Internet. Yet, if this were the case, then one would also expect to find Qatar, Iceland, Denmark, Norway, Finland, and New Zealand more equally represented on these marketplaces, as each of these countries has cyber connectivity rates over 90 per cent (*Ibid.*). However, vendors from these countries were not found to engage regularly with the two Tor marketplaces.

Additionally, countries with high frequency participation in this study share similar political and legal stances towards net neutrality and access to information in cyberspace (UNODC 2013). Yet, between and within each of these countries rests legal and

cultural contradictions with regards to criminally concerning items identified in this study. For instance, as of 2008, in the United States it is a violation of federal law to advertise and/or sell any illegal substance in an online venue[12] (Ryan… 2008); this is, however, not the case in other Western nations. These contradictions lead to dysnomie, or an inability of the authorities to control crime within this cyber venue due to the conflicting country-specific laws, and perhaps intensified by jurisdictional complications and the anonymity that Tor provides for its users (*e.g.*, Barratt *et al.* 2014; Martin 2014; van Hout and Bingham 2014). This particularly dysnomic environment may spur additional incentives for vendors from these particular countries to engage in higher levels of criminal activity on Tor marketplaces than vendors from other countries with equally high internet connectivity rates and opportunities (*i.e.*, experiencing a similar lack of structural contradictions) for criminally-based market engagement (*e.g.*, Iceland, Denmark, Norway, Finland, and New Zealand). However, future research is needed to support this conclusion.

The third notable finding from this study illustrated that aside from the four core countries of origin on Evolution and Silk Road 2, an abundance of other countries were found to participate differentially in specific markets (*e.g.*, drugs, stolen data), though in smaller percentages. For instance, while the U.S. was the top country of origin for drugs on both marketplaces, smaller percentages of active listings originated from countries known to have substantial ties to traditional drug trafficking operations (UNODC 2010). These included Guatemala, Mexico, Columbia, Malaysia, Cambodia, and Singapore. Columbia and Malaysia were also countries of origin for a smaller percentage of listings on Evolution regarding counterfeit and stolen data, in addition to Italy, the Czech Republic, Austria, Argentina, Bosnia and Herzegovina, and Romania. Physical weapons and hacking software originated mainly from the U.S. (on both marketplaces), in addition to Austria, Germany, the U.K. (on Evolution), and Belgium (via Silk Road 2), though limited activity from Israel, Columbia, and China was also found. This broader range of country participation on both marketplaces is indicative of the reach of globalization processes, but also perhaps the structural restrictions limiting additional criminally related participation in the online markets.

Taken together, this study found illegal or criminally concerning items to be abundant on Evolution and modest on Silk Road 2, largely sold from a core group of culturally Western countries. Yet, these and other countries are not engaging equally in these online marketplaces. Dysnomie caused by criminogenic asymmetries likely incentivizes (Passas 1999, 2000) individuals and groups to engage in criminal activities on Tor sites, leaving law enforcement entities multiple steps behind as criminologists and practitioners alike continue to adapt and adjust to the time-space compression (Appadurai 1996) of crime in the cyber domain. However, results from this study indicate that law enforcement agencies in the core countries (the U.S., the U.K., Canada, and Australia) can anticipate elevated levels of involvement in criminal activity on Tor from their respective citizens, regardless of the particular illicit market (*e.g.*, drugs, stolen data). As such, agencies in these countries (and elsewhere, in anticipation of potential future involvement) should seek to develop methods to better predict patterns in various transactions, as well as work closely with the national and international postal services responsible for delivering the majority of tangible criminally concerning items sold on Tor. By bet-

ter understanding the processes and differential impacts of globalization on cybercrime, researchers will be better equipped to conceptualize, monitor, and anticipate patterns in cyber-related criminal activities on all corners of the Internet.

NOTES

[1] For instance, China has a closed intranet system whereby the government restricts access to a series of websites and electronic content.

[2] This access is available as long as the individual can download the free Tor browser.

[3] November 2014 for Silk Road 2 and March 2015 for Evolution.

[4] For a more detailed explanation of how the Tor Network operates, please, see Tor Project (2014a).

[5] Also known by his online pseudonym Dread Pirate Roberts. Ulbricht was convicted on February 4, 2015 on all 7 charges, including drug trafficking, money laundering, and conspiracy, in a U.S. federal court.

[6] It should be noted that in the months leading up to its takedown, researchers including the authors observed erratic patterns in the number of items actively advertised. The data in this study were collected during these months; however, without having access to the seized servers hosting Silk Road 2, the causes for the fluctuations in listings were unable to be uncovered. Thus, the data were utilized as it was collected from the site. These fluctuations further underscore the dwindling significance of Silk Road 2 in comparison to Evolution, indicating that perhaps the site's operators were attempting to attract new business by inflating the number of advertised items.

[7] 'Hallucinogens' did not include cannabis or other THC products; cannabis was coded separately from THC products and edibles, and both categories were separated from general hallucinogens to discern differences between these drug forms.

[8] When a vendor created a new advertisement on either Silk Road 2 or Evolution, they were able to select a discrete country from a pull-down menu to indicate where the item(s) 'ships from'. If the vendor did not wish to indicate a specific country or has multiple countries of origin for the item, the vendor could select 'undeclared' on Silk Road 2 or 'worldwide' on Evolution. Vendors were also able to select the countries they were willing to ship the item(s) to. However, these potential destination locations were not included in this study because the percentage of sales to buyers in each country could not be determined from the data.

[9] Hong Kong was identified separately from China by users on both Tor sites and thus remained categorically separated in this study.

[10] The majority of past cybercrime-related research has taken a largely micro-level theoretical perspective, focusing on victimization related to (for instance) cyber stalking and online harassment and malicious software infections (*e.g.*, Broadhurst *et al*. 2014; Navarro and Jasinski 2012; Ngo and Paternoster 2011; Pratt *et al*. 2010).

[11] The exception to this regarded the item-based category labeled 'other' that was composed of clothing and other miscellaneous items. Here, vendors advertising items from China (including Hong Kong) were substantially found to be the most frequent on both Silk Road 2 and Evolution.

[12] With the exception of brick and mortar pharmacies (*i.e.*, pharmacies that exist in a physical location) that are registered with the U.S. Drug Enforcement Administration.

REFERENCES

Aas, K. F. 2007. *Globalization & Crime: Key Approaches to Criminology*. Thousand Oaks, CA: Sage Publications.

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 2436643.

Appadurai, A. 1996. *Modernity at Large: Cultural Dimensions of Globalization*. Minneapolis, PN: University of Minneapolis Press.

Barratt, M. J. 2012. Silk Road: Ebay for Drugs. *Addiction* 107: 683–684.

Barratt, M. J., Ferris, J. A., and Winstock, A. R. 2014. Use of Silk Road, the Online Drug Marketplace, in the United Kingdom, Australia and the United States. *Addiction* 109(5): 774–783.

Bossler, A. M., and Holt, T. J. 2009. On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory. *International Journal of Cyber Criminology* 3(1): 400–420.

Broadhurst, R. R., Grabosky, P. P., Alazab, M. M., and Chon, S. S. 2014. Organizations and Cybercrime: An Analysis of the Nature of Groups Engaged in Cybercrime. *International Journal of Cyber Criminology* 8(1): 1–20.

Christin, N. 2012, May. Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace. In *Proceedings of the 22nd International Conference on World Wide Web* (pp. 213–224). International World Wide Web Conferences Steering Committee.

DEA – Drug Enforcement Administration. 2005. *International Internet Drug Ring Shattered*. News release, April 20, 2005. Washington DC. URL: http://www.dea.gov/pubs/pressrel/pr042005p.html.

Dolliver, D. S. 2015a. Evaluating Drug Trafficking on the Tor Network: Silk Road 2, The Sequel. *The International Journal of Drug Policy* 26: 1113–1123.

Dolliver, D. S. 2015b. A Rejoinder to Authors: Data Collection on Tor. *The International Journal of Drug Policy* 26: 1128–1129.

FBI. 2014a. *Operator of Silk Road 2.0 Website Charged in Manhattan Federal Court.* New York Field Office Press Release. URL: http://www.fbi.gov/newyork/press-releases/2014/operator-of-silk-road-2.0-website-charged-in-manhat tan-federal-court.

FBI. 2014b. *Dozens of Online 'Dark Markets' Seized Pursuant to Forfeiture Complaint Filed in Manhattan Federal Court in Conjunction with Arrest of Operator of Silk Road 2.0.* New York Field Office Press Release. URL: http:// www.fbi.gov/newyork/press-releases/2014/dozens-of-online-dark-markets-seized-pursu ant-to-forfeiture-complaint-filed-in-manhattan-federal-court-in-conjunction-with-the-ar rest-of-the-operator-of-silk-road-2.0.

FBI Internet Crime Complaint Center (IC3). 2013. *IC3 2012 Internet Crime Report Released*. Fairmont, WV: FBI National Press Office.

FDA – Food and Drug Administration. 2012. *FDA Takes Action Against Thousands of Illegal Internet Pharmacies.* Press Announcement from U.S. Department of Health & Human Services. Released 2012, October 4.

Fox-Brewster, Th. 2015. A $50m Drug and Gun Dark Web Market Just Disappeared and Millions in Bitcoin with it. *Forbes Security*. URL: http://www.forbes.com/sites/thomasbrewster/2015/03/18/evolution-market-a-scam-says-site-pr/.

Grossman, L., and Newton-Small, J. 2013. The Secret Web: Where Drugs, Porn, and Murder Hide Online. *TIME* Magazine. November 11th edition: 26–33.

Halder, D., and Jaishankar, K. K. 2011. Cyber Gender Harassment and Secondary Victimization: A Comparative Analysis of the United States, the UK, and India. *Victims & Offenders* 6(4): 386–398. doi:10.1080/15564886.2011.607402.

Harvey, D. 1990. *The Condition of Postmodernity: An Enquiry into the Origins of Cultural Change*. Oxford: Blackwell.

Hunt, J. 2011. The New Frontier of Money Laundering: How Terrorist Organizations Use Cyberlaundering to Fund Their Activities, and How Governments are Trying to Stop Them. *Information & Communications Technology Law* 20(2): 133–152.

IWS – Internet World Statistics. 2015. *World Internet Users and 2014 Population Stats*. URL: http://www.internetworldstats.com/stats.htm.

Lipton, J. D. 2011. Combating Cyber-Victimization. *Berkeley Technology Law Journal* 26(2): 1103–1155.

Mackey, T. K., and Liang, B. A. 2011a. Promoting Online Drug Safety: Using Public–Private Partnerships to Deter Illicit Online Drug Sales. *Journal of Commercial Biotechnology* 17(3): 266–271.

Mackey, T. K., and Liang, B. A. 2011b. The Global Counterfeit Drug Trade: Patient Safety and Public Health Risks. *Journal of Pharmaceutical Sciences* 100(11): 4571–4579.

Markoff, J. 2005. *What the Dormouse Said: How the Sixties Counterculture Shaped the Personal Computer Industry.* New York: Penguin Group Publishers.

Martin, J. 2014. Lost on the Silk Road: Online Drug Distribution and the 'Cryptomarket'. *Criminology and Criminal Justice* 1748895813505234.

McCusker, R. 2006. Transnational Organized Cybercrime: Distinguishing Threat from Reality. *Crime, Law and Social Change* 46(4–5): 257–273.

Molnar, D., Egelman, S., and Christin, N. 2010. This is Your Data on Drugs: Lessons Computer Security can Learn from the Drug War. In *Proceedings of the 2010 Workshop on New Security Paradigms* (pp. 143–149). ACM.

Navarro, J. N., and Jasinski, J. L. 2012. Going Cyber: Using Routine Activities Theory to Predict Cyberbullying Experiences. *Sociological Spectrum* 32(1): 81–94.

Ngo, F. T., and Paternoster, R. 2011. Cybercrime Victimization: An Examination of Individual and Situational Level Factors. *International Journal of Cyber Criminology* 5(1): 773–793.

Passas, N. 1997. Anomie, Reference Groups, and Relative Deprivation. In Passas, N., and Agnew, R. (eds.), *The Future of Anomie Theory* (pp. 62–94). Boston, MA: Northeastern University Press.

Passas, N. 1999. Globalization, Criminogenic Asymmetries, and Economic Crime. *European Journal of Law Reform* 1(4): 399–423.

Passas, N. 2000. Global Anomie, Dysnomie, and Economic Crime: Hidden Consequences of Neoliberalism and Globalization in Russia and Around the World. *Social Justice* 27(2): 16–44.

Pratt, T. C., Holtfreter, K., and Reisig, M. D. 2010. Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory. *Journal of Research in Crime and Delinquency* 47(3): 267–296.

Pyrooz, D. C., Decker, S. H., and Moule, R. K., Jr. 2015. Criminal and Routine Activities in Online Settings: Gangs, Offenders, and the Internet. *Justice Quarterly* 32(3): 471–499.

Reyns, B. W. 2013. Online Routines and Identity Theft Victimization Further Expanding Routine Activity Theory beyond Direct-Contact Offenses. *Journal of Research in Crime and Delinquency* 50(2): 216–238.

Reyns, B. W., Henson, B., and Fisher, B. S. 2011. Being Pursued Online Applying Cyber-lifestyle – Routine Activities Theory to Cyberstalking Victimization. *Criminal Justice and Behavior* 38(11): 1149–1169.

Robertson, R. 1995. Glocalization: Time-Space and Homogeneity – Heterogeneity? In Featherstone, M., Lash, S., and Robertson, R. (eds.), *Global Modernities* (pp. 25–44). London: Sage.

Ryan Haight Online Pharmacy Consumer Protection Act of 2008, 21 U.S.C. §§802(50)-(56), 829(e), 841(h) (2008).

Tor Project. 2014. Tor Project Overview. URL: https://www.torproject.org/about/overview.html.en.

UNODC – United Nations Office on Drugs and Crime. 2010. *The Globalization of Crime: A Transnational Organized Crime Threat Assessment*. Vienna: UNODC.

UNODC – United Nations Office on Drugs and Crime. 2013. *Comprehensive Study on Cybercrime.* Vienna: UNODC.

Van Hout, M. C., and Bingham, T. 2013a. Surfing the Silk Road: A Study of Users' Experiences. *International Journal of Drug Policy* 24(6): 524–529.

Van Hout, M. C., and Bingham, T. 2013b. 'Silk Road', the Virtual Drug Marketplace: A Single Case Study of User Experiences. *International Journal of Drug Policy* 24(5): 385–391.

Van Hout, M. C., and Bingham, T. 2014. Responsible Vendors, Intelligent Consumers: Silk Road, the Online Revolution in Drug Trading. *International Journal of Drug Policy* 25(2): 183–189.

Walsh, C. 2011. Drugs, the Internet and Change. *Journal of Psychoactive Drugs* 43(1): 55–63.

Zhang, S., and Leidner, D. 2014. Workplace Cyberbullying: The Antecedents and Consequences. *Social-Technical Issues and Social Inclusion Track*. Twentieth Americas Conference on Information Systems, Savannah, GA.

APPENDICES

Appendix A

Top 10 Countries of Origin for Drugs

Evolution		Silk Road 2	
Country by Rank	**% of Drugs**	**Country by Rank**	**% of Drugs**
United States	20.7	United States	26.4
Netherlands	12.5	Germany	14.0
United Kingdom	12.2	United Kingdom	13.8
Germany	11.0	Australia	12.9
Canada	6.5	Netherlands	6.0
Australia	4.5	Canada	5.2
China	3.0	Belgium	2.3
Poland	1.9	China	2.3
France	1.8	Switzerland	1.7
Spain	1.2	Czech Republic	1.4
Worldwide	18.1	*Undeclared*	8.3

Appendix B

All Countries of Origin for eBooks

Evolution		Silk Road 2	
Country by Rank	**% of eBooks**	**Country by Rank**	**% of eBooks**
United Kingdom	4.2	Belgium	21.2
United States	3.8	United States	3.8
Australia	0.2	*Undeclared*	*75.0*
Columbia	0.1		
China	0.5		
India	0.5		
Italy	0.5		
Netherlands	0.5		
Worldwide	*91.5*		

Appendix C

Countries of Origin for Counterfeit or Stolen Data

Evolution		Silk Road 2	
Country by Rank	**% of Counterfeit or Stolen Data***	**Country by Rank**	**% of Counterfeit or Stolen Data**
1	2	3	4
United States	4.3	Belgium	37.5
United Kingdom	1.3	United States	2.4
Australia	1.0	Canada	1.2
Columbia	0.5	Australia	0.3
Germany	0.5	Poland	0.3
Argentina	0.2	*Undeclared*	*58.2*
Netherlands	0.2		
1	2	3	4
China	0.2		
Italy	0.2		
Czech Republic	0.1		
Worldwide	*91.5*		

Note: * only top 10 countries of origin listed for this variable

Appendix D

Top 10 Countries of Origin for Other

Evolution		Silk Road 2	
Country by Rank	**% of Other**	**Country by Rank**	**% of Other**
Hong Kong SAR China	23.9	China	35.7
United States	5.9	Hong Kong SAR China	21.2
Germany	2.2	Belgium	10.8
China	1.6	United States	4.8
Thailand	0.7	United Kingdom	3.3
United Kingdom	0.7	Finland	0.4
Australia	0.5	Australia	0.2
Netherlands	0.5	Canada	0.2
Canada	0.3	India	0.2
Spain	0.2	Netherlands	0.2
Worldwide	*63.3*	*Undeclared*	*23.0*