arts

MDPI

Article

Ancient Artifacts vs. Digital Artifacts: New Tools for Unmasking the Sale of Illicit Antiquities on the Dark Web

Katie A. Paul

The Antiquities Coalition, 1875 Connecticut Ave NW, Washington, DC 20008, USA; KPaul@theantiquitiescoalition.org; Tel.: +1-202-798-5245

Received: 13 February 2018; Accepted: 22 March 2018; Published: 26 March 2018

Abstract: Since the rise of the Islamic State of Iraq and Syria (ISIS, also known as Daesh and ISIL) in 2014, antiquities have been a widely publicized source of funding for what has become one of the most technologically savvy terrorist organizations of the modern era. The globalization of technology and rise of popularity in cryptocurrencies has changed the face of black-market trade and the actors that carry out these crimes. While art and antiquities have long served as a market with susceptibilities to laundering, the emergence of Dark Web markets, identification-masking software, and untraceable cryptocurrencies such as Bitcoin have opened new doors to potential vulnerabilities. The anonymity that is offered by these technologies acts as a roadblock for authorities, while attracting the likes of terrorists and transnational criminals. Investigative research using cyber security platforms to identify digital artifacts connected to potential traffickers provides the opportunity to unmask the seemingly untraceable actors behind these activities. The evidence of illicit antiquities trafficking on the Dark Web displayed in this article can generate a new discussion on how and where to study black-market antiquities to gain needed insight into combating the illicit trade online and the transnational criminal groups it may finance.

Keywords: antiquities trafficking; artifacts; art market; Bitcoin; Dark Web; ISIS; illicit; cryptocurrency; Deep Web; terrorism; transnational crime

1. Introduction

Art and antiquities are often a frequent target of theft, looting, and trafficking by organized criminals and violent extremists. The grey nature of the art market (Mackenzie and Yates 2016) allows for antiquities to be easily laundered through online sales, falsified documentation, and underground person-to-person trade (May 2017). Terrorist groups such as the Islamic State of Iraq and Syria (ISIS, also known as Daesh and ISIL) have used the trafficking of illicit antiquities from the Middle East and North Africa as a source of financing since shortly after the group's rise to power in 2014 (Gupta 2016; United States Department of State 2015; Al-Azm et al. 2014; Faucon et al. 2017). The rise of antiquities trafficking by terror groups (Terrill 2017) has prompted the U.S. Federal Bureau of Investigation (FBI) to issue a formal warning to dealers and collectors to take extra care in their due diligence of Middle Eastern artifacts (Federal Bureau of Investigation 2015). The recognition of illicit cultural property a terror financing threat that has also precipitated policy moves from the United States (H.R. 1493 2016) and the European Commission (European Commission 2017).

While other transnational criminal groups, such as the Haqqani network in Pakistan (Campbell 2013), and even Italian mafia (Quirico 2016) have been identified as agents of art and antiquities trafficking, the highly advanced technological maneuvering of ISIS's overall operations has placed them in a new level of threats in the digital realm. The group has sustained their operations

through recruitment, extortion, and trafficking of antiquities and more on social networking outlets such as Facebook, Twitter, Telegram, and WhatsApp (Taub 2015; Rawnsley et al. 2017). However, more concerning are the communications and transactions that cannot be traced as ISIS has delved deeper into the Dark Web.

The elusive nature of dark, encrypted, and untraceable online technologies is an appeal for anyone looking to hide illicit activities—it is also a significant obstacle for authorities seeking to track the actors engaging in illicit behavior. Europol's 2015 report, *Exploring Tomorrow's Organised Crime*, found a connection between the use of cryptocurrencies and illicit trade by organized criminal networks on the Dark Web. The report found that "virtual currencies have already had a significant impact on various types of criminal activity facilitating the exchange of funds between criminal actors and giving rise to a flourishing black-market economy on Darknet marketplaces" (Europol 2015, p. 31). Europol found that the core feature of anonymity in cryptocurrencies and overall Dark Web usage would create difficulty in tracking illegal transactions and cyber activity. "Bitcoin laundering services . . . will make transactions practically untraceable, heavily facilitating the trade in illicit goods online" (Europol 2015, p. 27). However, new studies have revealed that criminal activities online may not be entirely untraceable after all.

Digital artifacts, sometimes referred to as software artifacts, are by-products of data, digitally linked to specific users, that are left behind from their activity on the Internet (Gupta and Mehtre 2013, pp. 247–51). Digital artifacts may be remaining pieces of information created during installation or usage of software. Even Blockchain supported technologies such as the Bitcoin public exchange can leave behind these pieces of digital data, and with Bitcoin becoming a popular currency of antiquities dealers and online criminal groups alike, the grey lines in legitimacy of art market transactions become increasingly blurred.

By scanning online forums and communications networks for key antiquities trafficking terms, heritage experts and authorities can begin crawling the Deep Web and the Dark Web for digital artifacts related to illicit online activities. These artifacts can be sourced from information left from any number of Deep and Dark Web sources, from transactions through cryptocurrency to communications on encrypted messaging apps. Combining methodologies of new cyber forensics with those used to track similar illicit online trades such as wildlife, authorities may be able to get a better understanding of the reach of online antiquities trafficking networks and develop targeted strategies to combat them.

2. Terrorists' Love Affair with Bitcoin

While ISIS is best known for its outward manipulation of the Surface Web—that is the web that people can access on any given day using search engines such as Google—their shifting movements into both the Deep Web and Dark Web have made their illicit activities difficult to track. The Deep Web (Egan 2018) (as opposed to the surface web) is all the pieces of unindexed information that will not show up in any of the pages generated by Google. This is the majority of information that is actually on the Internet, but typically inaccessible unless special browsers or web crawling software are used. By contrast, the Dark Web is a small portion of the Deep Web that has been hidden intentionally to maintain anonymity by users.

While both the Deep and Dark Web have a role in illicit cyber activity, the Dark Web has significant appeal to violent extremist groups such as ISIS due to the ability to mask identification (Weimann 2015a). Dark Web surfers often use a Tor browser, which allows for the masking of their IP address—an attractive feature for individuals engaging in illicit trade (Wechsler 2016).

In 2015, following the terror attacks in Paris, ISIS moved (Weimann 2015b) many of their communications and recruiting operations to the Deep Web (Django 2017) and the Dark Web (Berton 2015) to avoid hacktivists (activist hackers) trying to infiltrate their networks. The result has led to a largely untraceable network of communication, prime conditions for more openly trafficking artifacts, weapons, and other illicit materials online. In fact, the weapon used for the deadly July 2016 Munich attack is believed to have been purchased on the Dark Web, less than one year after the Paris

attacks that expedited violent extremists' online operations shift to the Dark Web (Sengupta 2016; Cox 2017).

ISIS had reason to be worried about online tracking. Following the attacks in Paris, GhostSec, an offshoot of the global network of hacktivists known as Anonymous (Figure 1), digitally targeted the terror group revealing the discovery of a Bitcoin wallet in excess of $3 million (Madore 2015). The use of Bitcoin for funding by ISIS goes beyond Munich. In 2015, a U.S.-based ISIS cell was soliciting Bitcoin through online networks (Harman 2015). In the three years since, the broader use of cryptocurrency globally has vastly expanded (Hackett and Wieczner 2017), with the Bitcoin market—while volatile—continuing to remain on the overall incline.

Figure 1. Flag of the activist hacker group known as Anonymous (Anonymous 2009).

But why does this matter?

Since the hacktivism breach by GhostSec, ISIS has had time to maneuver through the depths of the Dark Web—giving them ample headway to mask their communication, trafficking, and financing. The group is known from media reports of their march of destruction and looting across the Middle East to establish their caliphate, but they have lost significant ground since their rise in 2014. However, the danger of ISIS is not limited to their regional territories.

The threat of a digitally-globalized caliphate, one that transcends the physical national boundaries where the group held territory, makes ISIS virtually impossible to fully eradicate. While militants attempt to regroup forces on the ground, their followers and financiers can hide in the shadows of the Dark Web, manipulating more covert opportunities for recruitment and funding. With the wildly popular rise of Bitcoin (Figure 2) and other cryptocurrencies (Sanders 2015), the group's available vehicles for funding become more complex and even more difficult to trace.

The anonymous and unalterable nature of Bitcoin is made possible through Blockchain technology. The attraction of Bitcoin and other cryptocurrencies lies in the anonymity attached to the transactions through the untraceable online wallet. "Darknet markets, by hiding the identities of those involved in transactions and often conducting business via Bitcoin, inherently represent illegality and regulatory evasion. As demonstrated by the Silk Road drug market and its successors, a massive number of Darknet transactions involve contraband" (Sui et al. 2015, p. 10).

For terrorist groups and other criminals an untraceable and unregulated currency that can be accessed from anywhere in the world has obvious benefits. Pair this currency with the veil provided by the Dark Web and criminals have a seemingly impenetrable digital playground for illicit activity.

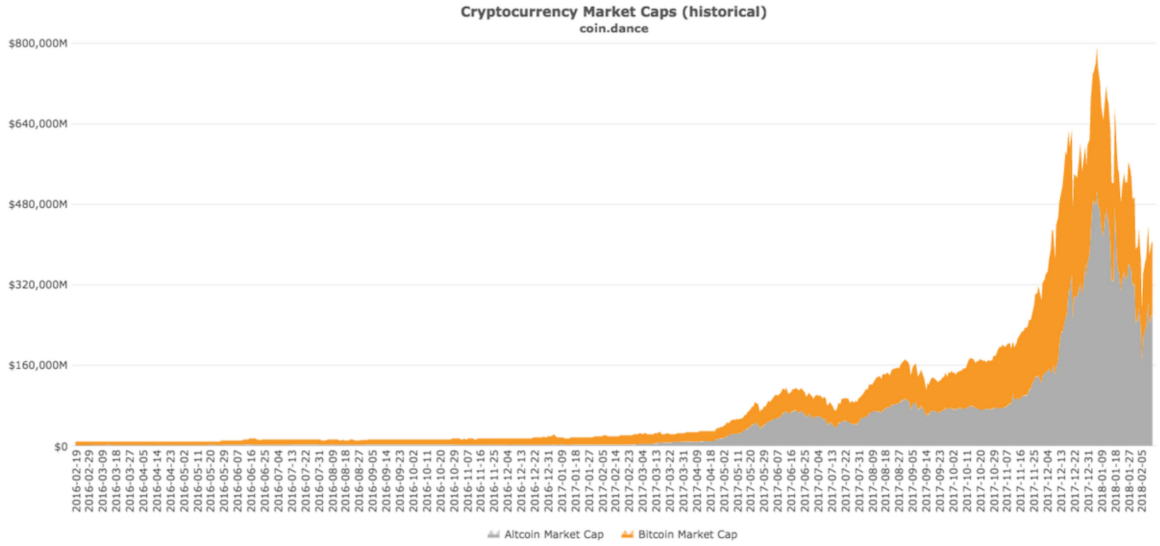

Figure 2. Overall Bitcoin and Altcoin cryptocurrency market gains and losses from 19 February 2016 through 5 February 2018 (Coin Dance 2018).

3. Art and More on the Dark Web

There is precedence for the illicit trade of more than just drugs and guns online. Illicit wildlife sales, a black market similar and often connected to that in antiquities, have been occurring on the Dark Web for years (Mead 2013). In 2017, INTERPOL Global Complex for Innovation in collaboration with International Fund for Animal Welfare (IFAW), the U.S. Department of State, and the African Wildlife Foundation (AWF) identified an illegal market for wildlife and ivory on the Dark Web, with some sale offerings reportedly dating back to 2015 (International Fund for Animal Welfare 2017). The research project revealed that the primary means of transactions for these illegal offerings were Bitcoin and other cryptocurrencies. Further studies have used what information is accessible to researchers to identify markets and key terms for wildlife trafficking on the Dark Web (Harrison et al. 2016).

In J.T. Jackman's 2014 book *Bitcoin for Beginners: How to Buy Bitcoins, Sell Bitcoins, and Invest in Bitcoins*, he specifically mentions untraceable illegal antiquities auctions as one of the markets that could be lured by the appeals of Bitcoin as a currency for criminal activity. "There are those who view the anonymity of Bitcoin is a definite "pro" for many. Unfortunately, that includes the "bad guys" of the world too. After all, there is zero "paper trail" behind the use of it . . . So, it makes it easy for the criminally minded to conduct all kinds of activities—from selling drugs to auctioning antiquities on illegal underground sites" (Jackman 2014, p. 49).

While much of the information on the Dark Web, including networks behind Darknet Markets (DNM), is difficult to maneuver or inaccessible to researchers and law enforcement (Merchant 2014), recent reports have revealed that the trafficking of illicit art and antiquities are among the many types of transactions taking place.

An October 2017 report from the Wall Street Journal stated that authorities have indicated they are seeing an increase in the sale of illicit antiquities on the Dark Web (Kantchev 2017). However, this is not the first mention of this illicit commodity appearing in the online markets of this shady network—two years ago, a user on the social network and communication forum Reddit, with the username "keepen_it_one_hunnid", claimed in an online discussion about Dark Web access

to have seen first-hand the sale of black-market antiquities and many other illicit materials on underground sites.

> "I have personally seen for sale: Fake passports/I.D. packages, cloned credit cards/ fake visa gift cards, long standing eBay accounts with positive ratings, hacking services, wet work, foreign knock-offs of any product imaginable (cell phones, laptops, coats, purses, watches, etc.) Counterfeit art and jewelry, black market antiquities, exotic animals, ivory/ rhino horn/ shark fins, counterfeit money . . . Really anything that you could think of" (keepen_it_one_hunnid 2015).

Although a seemingly obscure source, reddit has been used to identify networks in illegal wildlife trafficking on the Dark Web. A 2016 study on Dark Web markets specifically listed sources in subreddit (Harrison et al. 2016, p. 5) as the basis for identifying code words used by networks in illegal wildlife trafficking. These code words were then run though many of the underground online marketplaces to identify offerings of illicit wildlife.

Known stolen art has also already shown up on the Dark Web (Figure 3). In November 2017, a 133-year-old painting that had been stolen from the International Art Centre in New Zealand on 1 April 2017 appeared for auction on the Dark Web auction site known as White Shadow (Burgess 2017; Maneker 2017). The seller, listed as "Diablo," offered the painting with the description, "Here you can bid on an [sic] TOP SECRET original Painting from Bohemian painter Gottfried Lindauer that was stolen in New Zealand, Auckland 2017." While the authenticity of the painting has been debated by experts, the piece still sought to pull in hundreds of thousands of dollars (Burgess 2017).

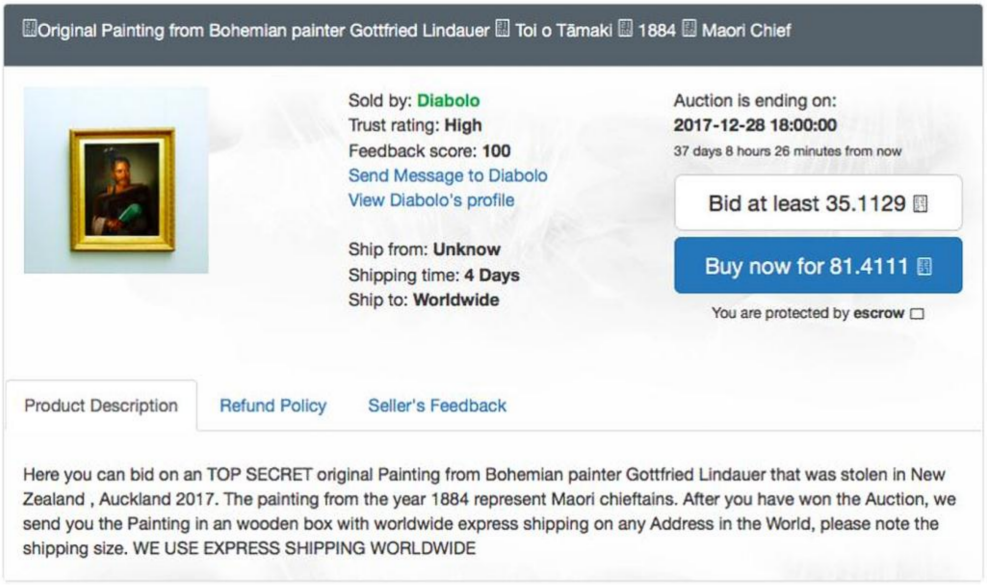

Figure 3. Screen grab of the listing for the stolen Chief Ngatai-Raure painting on the Dark Web auction site White Shadow, the painting was available to ship worldwide (Courtesy of Burgess/WIRED UK 2017).

The stolen painting's listing online had it offered for $350,000—all to be paid in Bitcoin (Rea 2017; Burgess 2017; Maneker 2017). In addition, while this particular piece was not stolen by ISIS, the incident is notable for the clear connections between stolen art and cryptocurrency on the Dark Web.

ISIS has also been reported to have sold illicit antiquities on the Dark Web by using Bitcoin as an untraceable source of transactions. Haroon Ullah identified a member of ISIS who went by the name of Javaid. The ISIS recruit detailed how he would move antiquities looted from Iraq and Syria by first identifying buyers through social media, specifically connecting to interested buyers in North America and Europe. He would then secure the transactions through sites on the Dark Web, accepting Bitcoin

as payment for the pieces. "That was the key: black-market sales using digital cash, with no footprints left behind" (Ullah 2018, p. 174).

This is not the only mention of ISIS selling illicit artifacts for Bitcoin on the Dark Web. Jan Peter Hammer, director of the "Art of War" research project, also encountered a journalist who reported that ISIS was allegedly using Bitcoin for all Dark Web transactions of looted antiquities (Hammer 2017). Artifacts looted from territories with large terrorist and transnational criminal presence, such as Iraq, Syria, and Yemen, are commonly smuggled through transit routes in Turkey and the Gulf States and then on to Europe, with valuable pieces often held in free ports for years.

The use of free ports to hide artifacts is not a new tactic in the era of ISIS. In 2016, Swiss authorities seized a trove of artifacts that had been looted from Yemen, Syria, and Libya and found in a Swiss free port (Figure 4a,b) where they had been sitting since 2009 and 2010 (Geneva Public Ministry 2016).

Many of these valuable pieces that are smuggled out of the Middle East and North Africa have not yet surfaced on the public market and likely will not for ten years or more, particularly those that may be laying low in free ports. Hito Steyerl referred to free ports as "a museum of the Internet era, but a museum of the dark net, where movement is obscured, and data-space is clouded" (Steyerl 2015). We are only at the beginning of the effects of this underground trade online and its implications for the smuggling and laundering of artifacts in the real world.

(**a**) (**b**)

Figure 4. Two of the artifacts seized from Swiss free port (Geneva Public Ministry 2016). (**a**) Relief from the UNESCO World Heritage Site of Palmyra, Syria. (**b**) Yemeni carved ancient artifact.

4. Bitcoin and the Art Market

Bitcoin is no longer a currency just used on the Dark Web—even brick and mortar antiquities dealers now advertise that they accept cryptocurrency. With the United States serving as the world's largest art and antiquities market (Pownall 2017), there is even greater opportunity for illicit actors to use U.S. outlets as a means of laundering both artifacts and finances.

In 2017, the University of Cambridge Centre for Alternative Finance released its inaugural Global Cryptocurrency Benchmarking Study. The study collected data from nearly 150 companies and individuals that had not previously been publicly accessible. The data illustrated the nuances of the rapidly growing cryptocurrency market and its constituents (Hileman and Rauchs 2017).

Findings from the individuals and cryptocurrency organizations that participated in the study revealed that currency from the U.S. also serves as one of the five currencies dominating cryptocurrency trading, with 65 percent of trading platforms supporting the USD (the other four are EUR, JPY, CNY, and GBP). In addition, the highest number of crypto wallet holders based on the data available in

this study—51 percent—are based in Europe (31 percent) and North America (30 percent) (Hileman and Rauchs 2017, pp. 29, 54). Thus, while terrorist organizations such as ISIS and other transnational criminal groups may be accepting Bitcoin for antiquities, a large portion of individuals trading in the currency and holding crypto wallets are likely coming from western countries in North America and Europe.

Art and antiquities galleries are making moves to capitalize on the rise of cryptocurrency popularity. Archaeologist Sam Hardy identified a Chicago-based gallery advertising Syrian antiquities for sale along with the gallery's willingness to accept Bitcoin (Hardy 2015). In 2017, Dadiani Fine Art in London became the first art gallery to announce it would begin accepting Bitcoin as payment (Campbell 2017). Later that same year, Sant 'Agostino in Turin, Italy's oldest auction house, announced they would accept the popular cryptocurrency along with several others (Auction Payment With Cryptocurrency 2017).

Ancient coin and antiquities dealer Harlan J. Berk Ltd. in Chicago advertises on their social media and homepage of their website (Figure 5) that they accept Bitcoin for their transactions. It is unclear if this is the same Chicago-based dealer referenced by Hardy. The coin and antiquities dealer has been identified as one of the three most important ancient coin auction houses in the United States (Elkins 2009).

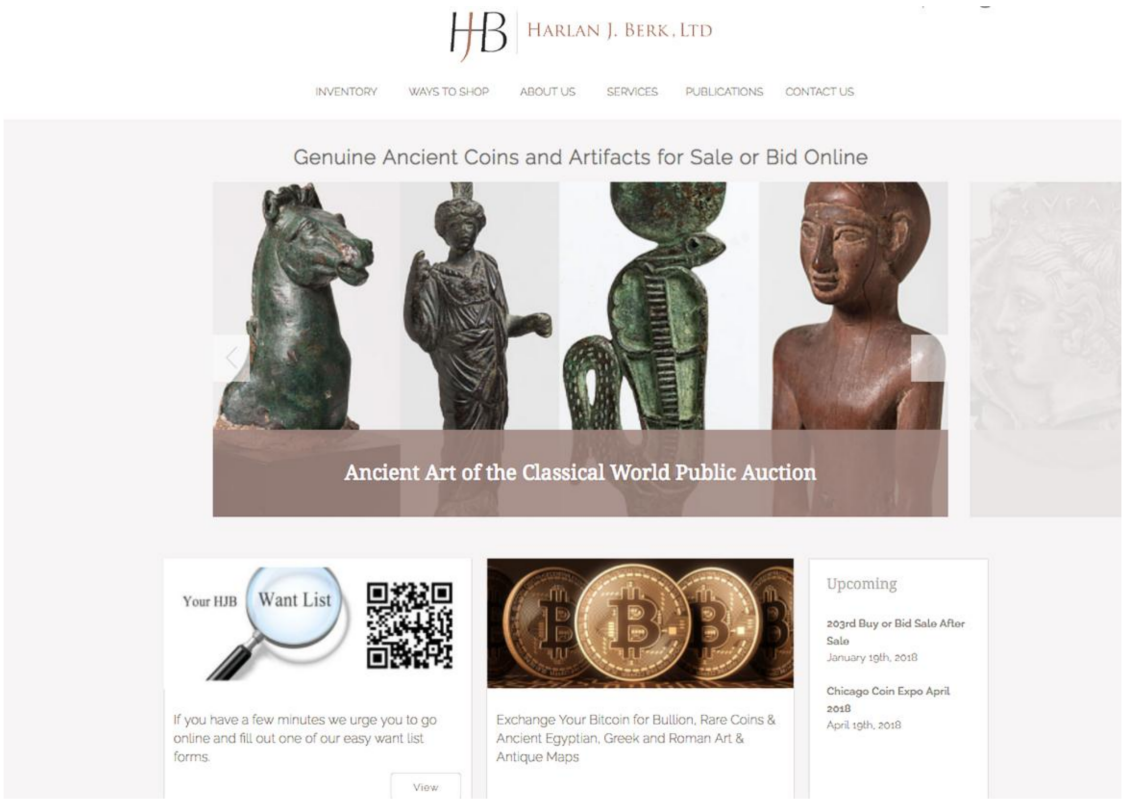

Figure 5. Screen grab taken on 11 February 2018 of the homepage for ancient coin and antiquities dealer Harlan J. Berk Ltd. in Chicago advertising Bitcoin as a newly accepted currency by the dealer. (Screen grab by author 2018).

Some dealers see the acceptance of Bitcoin as an opportunity to disrupt a market largely dominated by auction houses such as Christie's and Sotheby's. "More practical factors come into play when buyers choose Bitcoin, such as the speed of the transactions and lower fees compared to traditional payment methods like credit cards" (Wall 2017). However, it also may open new doors to an influx of illicit materials onto the market and nefarious actors trading material through an untraceable method of payment in an effort to launder their digital funds.

However, this should not be news to the art market. In 2015, German news outlet Handelsblatt published a piece on the connections between cryptocurrency and terrorism, warning specifically that art and antiquities dealers should be prepared to report if they suspect someone trying to use artifacts to launder money (Brächer 2015).

Money laundering more broadly and its connections to the art market are not new. "This sector appears as a vector for laundering funds of illicit origin. In the files transmitted by the [Cellule de Traitement des Informations Financières (CTIF), a unit under the Belgian system for preventive anti-money laundering and counter-terrorist financing (AML/CFT)] CTIF, investment in the art sector is a method used to conceal illegal cash inflows including corruption, drug trafficking and smuggling of labor" (23e Rapport d'activités 2016). CTIF found that there were multi-faceted techniques employed for concealing illicit transactions, including: "false invoices (when a professional agrees to make a false invoice to a customer); fake auctions (this is for the launderer to put in sales of works of art that will be bought by an accomplice with dirty money) or the fake sales of works of art on the Internet" (23e Rapport d'activités 2016).

The online art and antiquities sector promotes anonymity and allows for fast and frequent changes in ownership of material that is often unprovenanced (Brodie 2017) and entails transfer of large sums of money (Financial Action Task Force 2015; 23e Rapport d'activités 2016). According to the 2017 report "Transnational Crime and the Developing World" from the Washington-based non-profit Global Financial Integrity (GFI), "Art and antiquities also can serve as an alternative currency and be exchanged for other illicit goods such as arms or drugs. This is not to say that most of the global art market, or even a robust minority, operates illicitly; nonetheless, opacity provides an environment for crime to flourish" (May 2017). The rapid growth of the online industry and the incorporation of cryptocurrencies enhances vulnerabilities in the art market, particularly anonymous payments made by virtual currencies (23e Rapport d'activités 2016).

Although cryptocurrencies have yet to be adopted by major financial institutions, their lack of centralized adoption is part of the appeal. Cryptocurrency was designed to be an alternative to central bank currency and therefore outside of the reach of regulations (Lam 2017). When art market players provide buyers with the opportunity to turn their Bitcoin into real material assets, they are presenting cryptocurrency holders with a transaction that takes their un-adopted currency and turns it into an entity with material value - one that can then be resold for currencies banks do accept or donated to museums for tax breaks that governments recognize.

A 2015 survey released in the "Money Laundering and Financial Crimes Country Database" report from the U.S. Department of State revealed that of the 212 countries surveyed on anti-money laundering (AML) practices, only Algeria, Georgia, Guatemala, Honduras, Lithuania, Monaco, Syria, and the West Bank and Gaza included practices and due diligence efforts that specifically included dealers in antiquities (United States Department of State Bureau for International Narcotics and Law Enforcement Affairs 2015). While some countries have made efforts to examine antiquities dealers for AML, these efforts are not enough to thwart these crimes as the art and antiquities market continues to evolve and grow ever-greyer while dealers and criminals alike and employ masking technologies and untraceable currencies. Since the 2015 survey, many illicit actors have moved further underground to elude authorities, including terror groups that traffic on the Dark Web (Paganini 2015; Gupta 2016), further AML due diligence efforts are necessary to keep up with evolving transnational crime.

While the art and antiquities market appears increasingly willing to start opening their doors to cryptocurrency for the purchase of artifacts, some cryptocurrency platforms are not as eager to have antiquities offered as a product to be purchased using Bitcoin. One exchange platform, Coinhub India, includes both religious artifacts and antiquities in their list of items banned from trading. Among drugs, weapons, and human organs, the list explicitly bans, "7. Religious items, including books, artefacts, etc. of any description or any other such item which is likely to affect the religious sentiments of any person. 8. "Antiquities" and "Art Treasures"" (Coinhub India 2018). In fact, users of Coinhub

India must sign an agreement in the site's terms and conditions that they will not purchase or distribute these products lest they lose their access to the cryptocurrency trading site.

5. Tracing the "Untraceable"

Although Blockchain, the technology behind online currencies such as Bitcoin, and the concept of a digital currency that is untamperable and unregulated has been criticized for the opportunities it may present to criminals and terrorist groups (Chester 2015), it should be noted that this technology also holds new potential for cyber security investigations, including efforts in the fight against terrorism and trafficking.

Blockchain technology allows for the creation of digital records or tags that cannot be altered or tampered with. The permanent and unchanging nature of the digital records that can be created by Blockchain technologies present opportunities in the protection of artifacts against illicit trade while addressing some of the vulnerabilities of existing documentations (Cooper 2016; Campbell 2017). In addition to its more well-known applications to cryptocurrency, Blockchain technology can be used for the creation of title deeds and smart contacts (Underwood 2016). Like land, antiquities and other cultural property elements can be treated in the same manner as Bitcoin, with Blockchain technology used to assign a smart contract (also known as a cryptocontract) (Marr 2018) to the owner of the piece—in the case of registered antiquities, the ownership would go to a national government or museum.

While Blockchain technology holds potential to create valuable records that can help combat the illicit antiquities trade and increase the legitimacy of artifacts on the legal market, online illicit trafficking networks are moving more quickly than the infrastructure and capacity of cultural heritage institutions can keep up with. Understanding how criminals are using the Dark Web, cryptocurrency, and masking software is of critical importance to expedite law enforcement efforts to shut off a vein of the illicit antiquities trade that has yet to be fully explored.

Legally, options to pursue the illicit actors on the Dark Web who may manipulate transaction opportunities using Bitcoin are few. The regulatory environment in illicit cyber activity is still in the very early stages of development. However, new monitoring mechanisms are constantly evolving.

The rise of the usage of cryptocurrency may open new doors to tracking financial movements (Bohannon 2016) of terrorist organizations, transnational trafficking networks, and other illicit online actors—including those trafficking in art and antiquities. Cryptocurrencies leave behind artifacts of their own—digital artifacts—which can be traced to identify the online activity of otherwise "untraceable" users (Stokel-Walker 2018). Much in the same way that pieces of websites, articles, sales, and more can be found through crawling the Deep Web, pieces of cryptocurrency transactions from the public exchange and elsewhere can also be identified. "These evidentiary artifacts, whether a timestamp, an electronic document or e-mail provides a digital case with the solid foundation it needs in order to hold up in the eyes of the court" (Doran 2015). Digital web crawling tools such as Internet Evidence Finder (IEF) or cyber intelligence platform Sixgill can recover artifacts left behind by Bitcoin transactions, social media activity, email accounts and more, opening the door to tracking illicit cyber activity (Doran 2015; O'Hear 2016; Murray 2013). Cyber forensics experts use web crawling software and intelligence platforms such as these to gather evidence from laptops, computers, and online accounts, in the form of digital artifacts.

Using the Sixgill cyber intelligence platform for a preliminary search of illicit antiquities and cultural property on the Dark Web, digital artifacts of Telegram communications revealed that jihadi networks are indeed illicitly trading coins (Figure 6) and artifacts (Figure 7) (Daily Telegram Group 2018). Digital artifacts, discovered using the Sixgill web crawling technology, from a Telegram chat group known for trafficking communications among jihadi and militant users, included photos and even phone numbers of the offending traffickers.

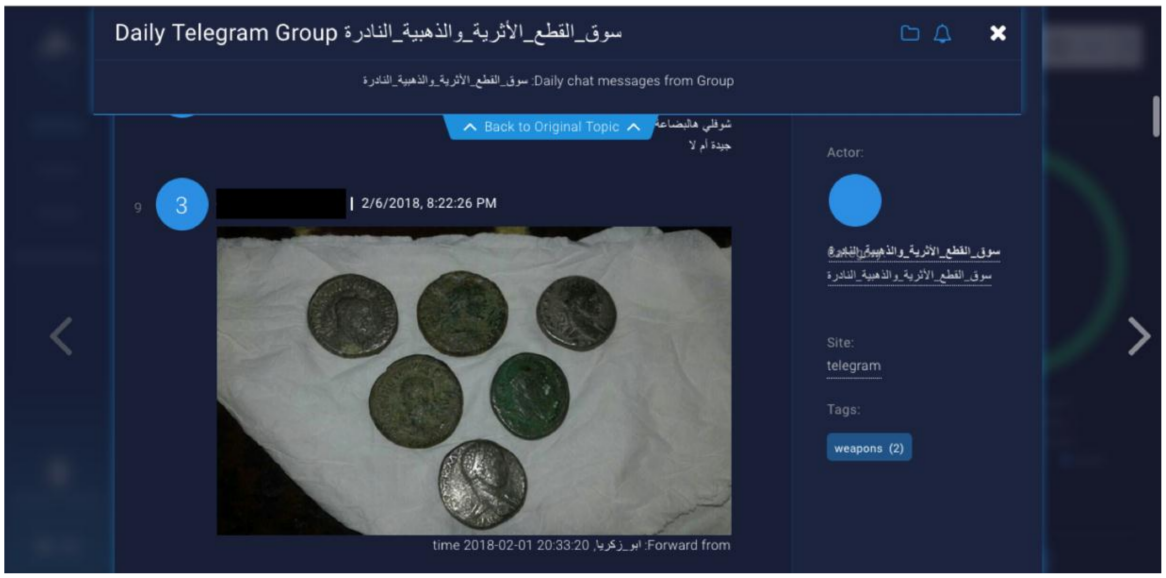

Figure 6. Screen grab of Sixgill platform search that turned up ancient coins illicitly offered for sale through a jihadi Telegram communication group. Phone number of offending individual has been redacted for the purposes of this paper. (Screen grab by author 2018).

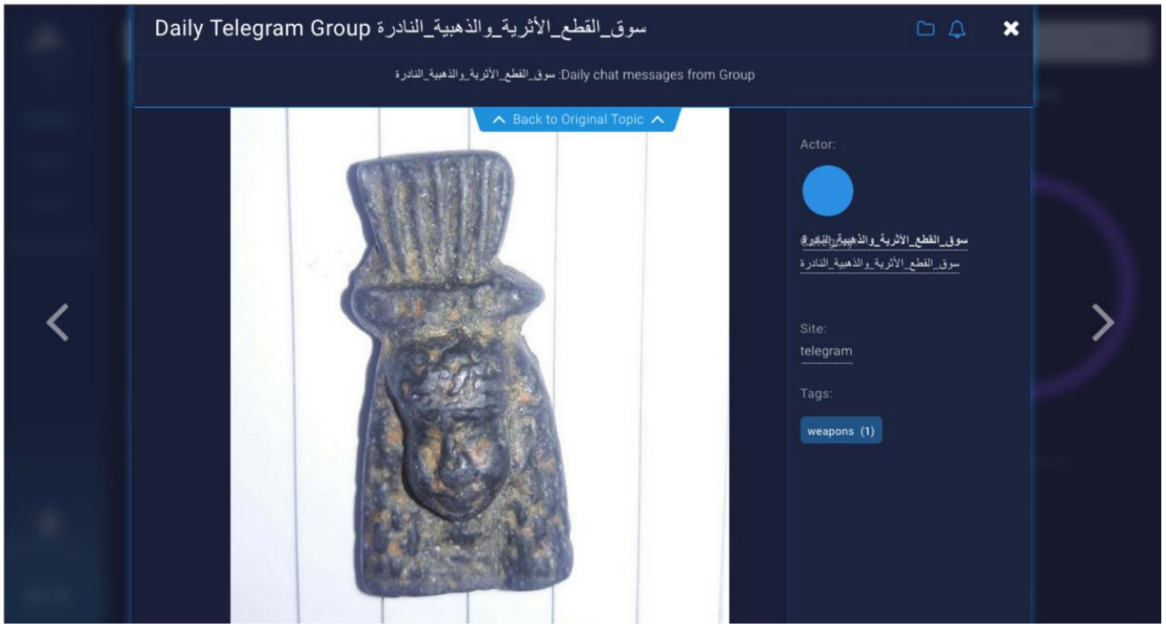

Figure 7. Screen grab of Sixgill platform search that turned up small artifact (authenticity unverified) illicitly offered for sale through a jihadi Telegram communication group. (Screen grab by author 2018).

These coins and small artifacts being offered in this particular Telegram group were posted in February 2018. The primary communications in this group were composed of Islamist propaganda and trafficking in coins, artifacts, and weapons. The platform also includes a tag for the "weapons" that Sixgill had assigned to this Telegram group as illustrated in Figures 6 and 7. (Daily Telegram Group 2018).

New analysis from researchers at Qatar University in January 2018 revealed that they were able to link publicly available information on the Blockchain, social media, and Deep Web sites with the transactions of Bitcoin users on the Dark Web, resulting in the unmasking over 125 Tor users (Al Jawaheri et al. 2018). The Qatar University team was able to trace back transactions for

years, meaning even the early days of Bitcoin purchases, such as those that were made on the online black-market drug site Silk Road, can be traced (Greenberg 2018).

Applying a similar methodology to that used in identification of the illegal wildlife trade by Harrison et al. on the Dark Web—that is the scanning of Dark Web and Deep Web discussion forums for key terminology to use in Dark Web crawling—may yield results in uncovering the black-market art and antiquities trade online (Harrison et al. 2016). By searching comments on subreddit, interest in—and experience with—Dark Web art and antiquities can be easily found. The subreddit for Dark Net Markets (r/DarkNetMarkets) reveals one user who goes by the name "storytimeppl" with a specific request for Chinese and Egyptian artifacts—he later responds to a commenter about the benefits of using Bitcoin for transactions in this space (Figure 8). Posts such as these can help identify the period and origin of cultural property that Dark Web users are seeking (storytimeppl 2016). In an October 2017 post for the subreddit Darknet (r/Darknet), redditor "tery_mac" sought a "DNM" (abbreviation for Darknet market) in stolen goods (Figure 9)—when asked what he was seeking he specifically noted "paintings, artifacts and rare stuff" (tery_mac 2017).

Dark Web markets are not the only place redditors are seeking advice on finding antiquities. The Deep Web is also a subject of discussion. A user - who has since deleted their Reddit account—posted in the Deep Web subreddit (r/deepweb) seeking an antiquities dealer in October 2017 (Figure 10) (Reddit 2017). While such a broad request may seem harmless, seeking the dealer in a subreddit for the Deep Web likely means they are deliberately looking to get items outside of the public legitimate market.

Redditors are not just interested in artifacts and paintings on the Dark Web, there is also interest in smaller portable objects, such as coins, which have even less regulation and oversight than the overall art and antiquities market. Reddit user "highcubist" openly requested markets for coins and other old objects in November 2017 in a subreddit meant for antiques. The redditor noted that he has seen counterfeit items thus far but is interested in the "real deal" (highcubist 2017a). The same redditor went even further with his requests in December 2017 when his interests in illicit ancient material evolved. He asked specifically for Middle Eastern antiquities (Figure 11), with the caveat that he was not interested in provenance, "Have friends interested in Middle Eastern antiquities, do you know of anything available? Not concerned about provenance and origin. Would be happy to discuss a finder's fee" (highcubist 2017b).

The requests by highcubist are of interest due to their specificity for Middle Eastern antiquities and disregard for provenance. Using the Sixgill platform, a query for the screen name "highcubist" was entered to identify any digital artifacts where this user may have engaged elsewhere—and he has. Two posts (Figures 12 and 13) by a screenname for "highcubist" were found where he was seeking information through discussion forums on the Dark Web regarding coins and artifacts available on DNMs (highcubist 2017c; highcubist 2017d). These posts occur around the same general timeframe as the reddit posts by the same screen name, indicating that they are likely to be the same individual due to the atypical screen name and the nature of the requests.

While some art and antiquities market experts have been skeptical of the existence of a Dark Web market for artifacts, the surge of reddit requests for leads on this market in late 2017 would suggest interests of Dark Web users have changed. With reddit serving as a public forum, and commentary accessible even without the security of a reddit account, the comments posted to date show a clear interest in specifically illicit and Deep and Dark Web markets for antiquities as well as interest in unprovenanced items.

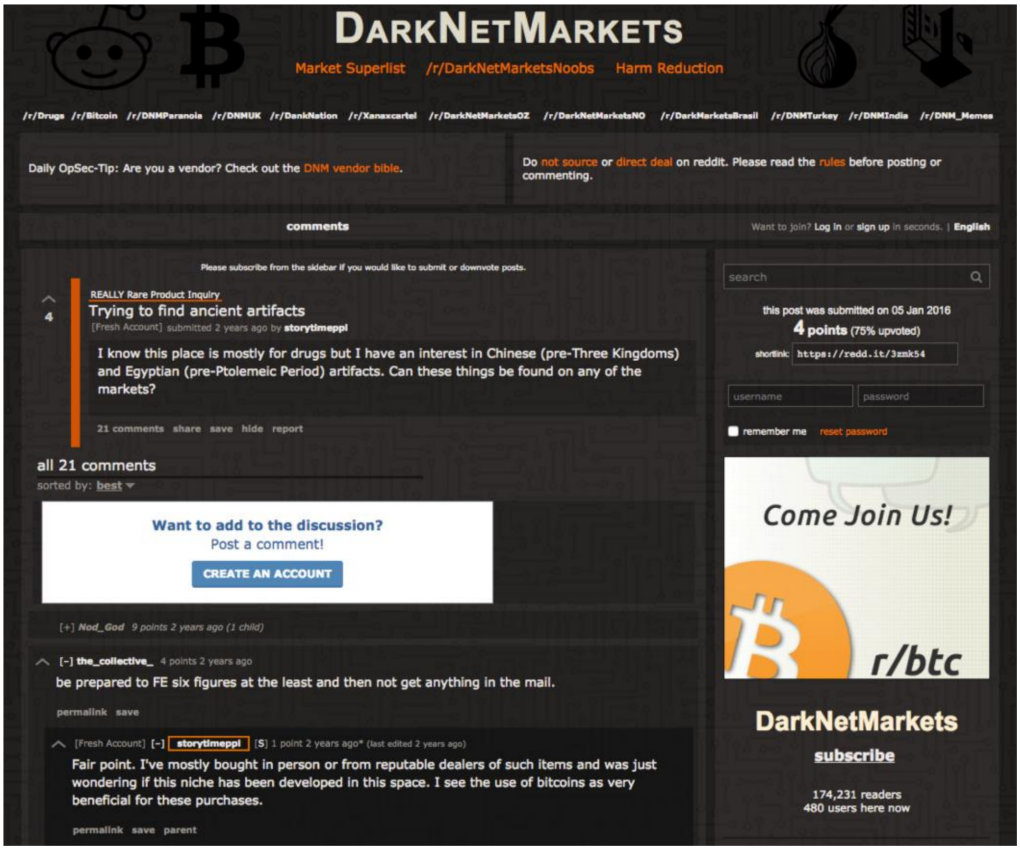

Figure 8. Screen grab of the subreddit for Dark Net Markets (r/DarkNetMarkets) with a specific request for Egyptian and Chinese antiquities. (Screen grab by author 2018).

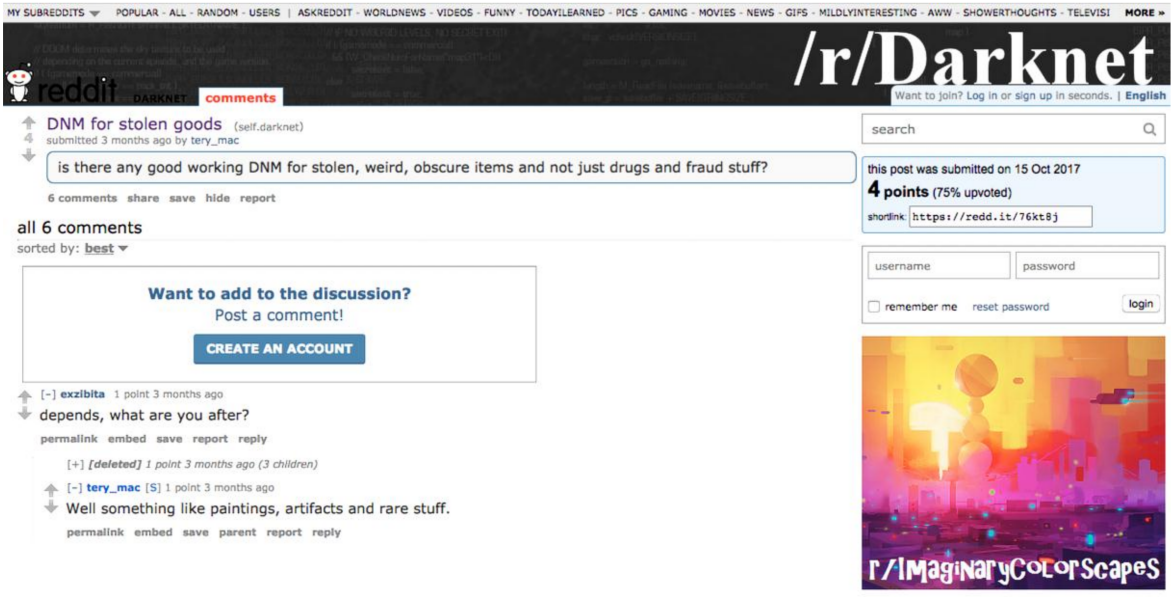

Figure 9. Screen grab of the subreddit for Darknet (r/Darknet) with a request for stolen goods and a conversation to specify artifacts and rare items. (Screen grab by author 2018).

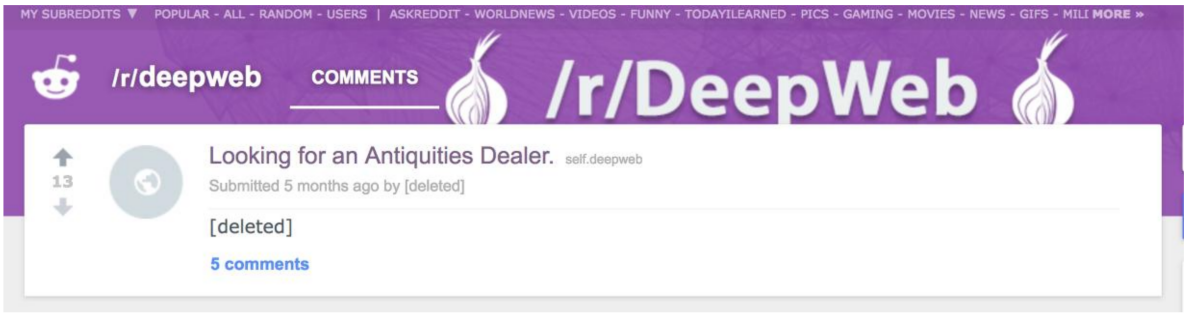

Figure 10. Screen grab of the subreddit for DeepWeb (r/deepweb) with a request for an antiquities dealer from a since-deleted account. (Screen grab by author 2018).

Figure 11. Screen grab of reddit user highcubist's request for "Middle Eastern antiquities" in the subreddit for antiques (r/antiques), making clear they are not concerned about whether or not the object has provenance. (Screen grab by author 2018).

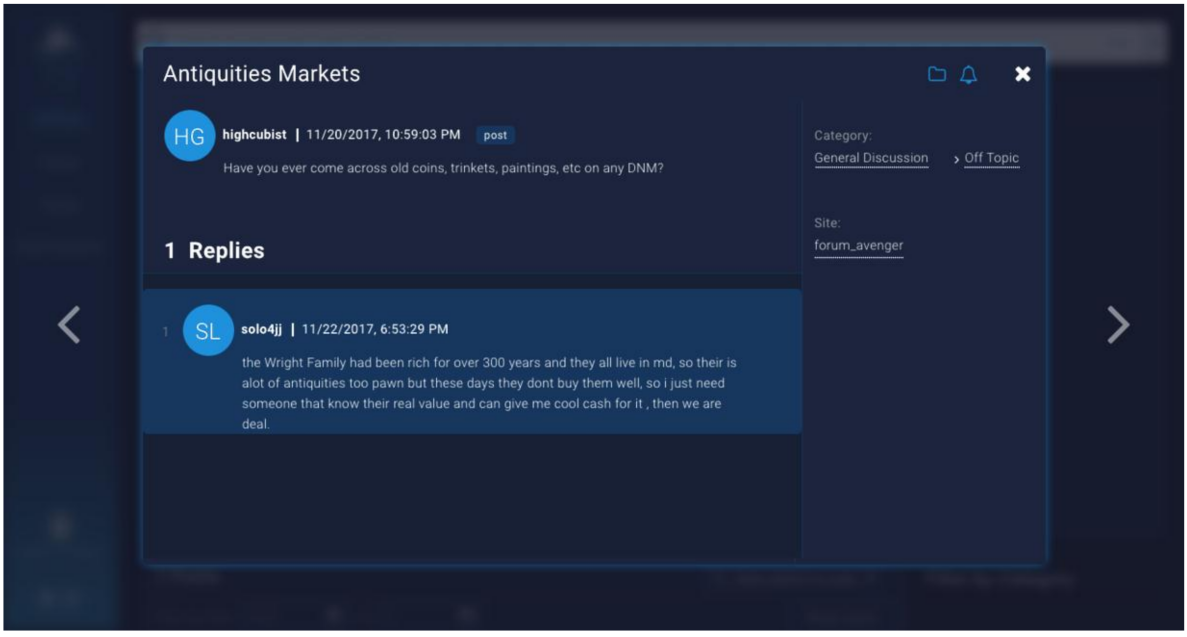

Figure 12. Screen grab of Dark Web forum user highcubist's inquiry regarding old coins on "DNM" (i.e., Darknet Markets) accessed through the Sixgill cyber intelligence platform. (Screen grab by author 2018).

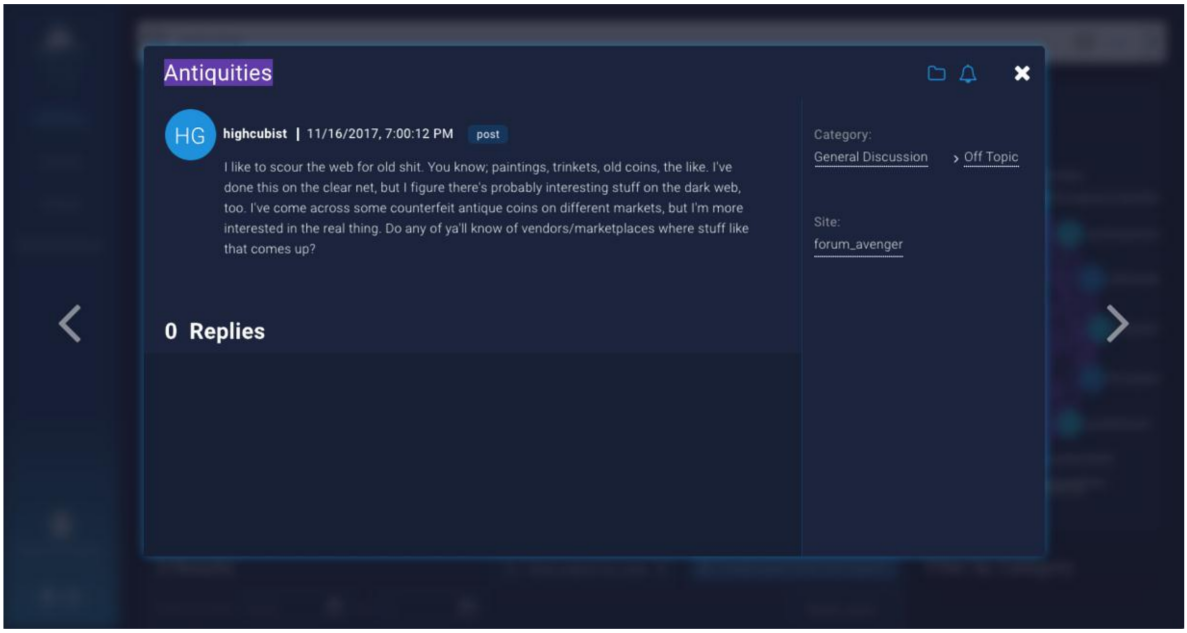

Figure 13. Screen grab of Dark Web forum user highcubist's inquiry regarding old coins on "DNM" (i.e., Darknet Markets) accessed through the Sixgill cyber intelligence platform. (Screen grab by author 2018).

6. Conclusions

Monitoring and intervention of the illicit antiquities trade on the Deep Web and the Dark Web would not only serve to intercept financial sources for violent extremists and organized criminals, but also to address the burgeoning black market for illicit antiquities which has high demand in Western countries including the United States. The highly sophisticated and globalized nature of cybercrime today forces authorities to continue to modify and update their activities in response to these crimes.

Advancements in Blockchain technology, web crawling software, and monitoring and intelligence gathering methodologies are proving more successful for authorities who are continuing to remove black-market Dark Web sites from the Internet, but significant gaps still exist in the types of black-market networks being monitored. The illicit antiquities trade is one of those gaps.

The "Illegal Wildlife Trade in the Darknet" research report released by the INTERPOL Global Complex for Innovation in collaboration with International Fund for Animal Welfare (IFAW), the U.S. Department of State, and the African Wildlife Foundation (AWF) shows there are opportunities for the Department of State and INTERPOL to deploy their web crawling and cyber security tools for the monitoring of black-market trade online—with a focus on the extent of Dark Web trafficking of antiquities and the types of actors engaged in these crimes (International Fund for Animal Welfare 2017).

In response to the reported findings of INTERPOL's Dark Web study on wildlife, the organization launched a special training course on digital forensics of wildlife investigations (International Fund for Animal Welfare 2017). With many parallels between the black-market trade in wildlife and antiquities, a training course on identification of illicit cultural property could be incorporated into INTERPOL's digital forensics efforts to dually combat these often-interconnected trades.

By targeting transactions in art and antiquities using the methodologies applied to other illegal online trades, authorities can fill a gap in our understanding of the demographics of black-market traders. Unmasking some of the world's most sophisticated cyber-traffickers of cultural property and opening doors to understanding the next generation of this rapidly evolving illicit trade.

Acknowledgments: The author would like to thank the Antiquities Coalition for its continued research support. The author would also like to thank Amr Al-Azm at Shawnee State University for his fruitful discussion and insights into terrorism antiquities trafficking.

Conflicts of Interest: The author declares no conflict of interest.

References

23e Rapport d'activités. 2016. Cellule de Traitement des Informations Financières. Brussels: Cellule de Traitement des Informations Financières. (In French). Available online: http://www.ctif-cfi.be/website/images/FR/annual_report/ra2016frsite.pdf (accessed on 15 January 2018).

Al Jawaheri, Husam, Mashael Al Sabah, Yazan Boshmaf, and Aimen Erbad. 2018. *When a Small Leak Sinks a Great Ship: Deanonymizing Tor Hidden Service Users through Bitcoin Transactions Analysis*. Doha: Qatar University, January. Available online: https://arxiv.org/pdf/1801.07501.pdf (accessed on 3 February 2018).

Al-Azm, Azm, Salam Al-kuntar, and Brian I. Daniels. 2014. ISIS' Antiquities Sideline. *New York Times*, September 2. Available online: http://www.nytimes.com/2014/09/03/opinion/isis-antiquities-sideline.html?_r=1 (accessed on 27 December 2017).

Anonymous. 2009. Wikimedia Commons. Available online: https://commons.wikimedia.org/wiki/File:Anonymous_Flag.svg (accessed on 12 February 2018).

Auction Payment With Cryptocurrency. 2017. Sant' Agostino. October 5. Available online: https://www.santagostinoaste.it/public/comunicato-stampa-ing.pdf (accessed on 11 February 2018).

Berton, Beatrice. 2015. The Dark Side of the Web: ISIL's One-Stop Shop? In *European Union Institute for Security Studies*. Paris: European Union Institute for Security Studies. Available online: https://www.files.ethz.ch/isn/192064/Alert_30_The_Dark_Web.pdf (accessed on 13 January 2018).

Bohannon, John. 2016. Why Criminals Can't Hide behind Bitcoin. *Science*, March 9. Available online: http://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin (accessed on 3 February 2018).

Brächer, Michael. 2015. Weshalb Terroristen am liebsten bar bezahlen. *Handelsblatt*, November 24. (In German). Available online: http://www.handelsblatt.com/finanzen/steuern-recht/recht/terrorfinanzierung-weshalb-terroristen-am-liebsten-bar-bezahlen/12631660-all.html (accessed on 15 January 2018).

Brodie, Neil. 2017. *How to Control the Internet Market in Antiquities? The Need for Regulation and Monitoring. The Antiquities Coalition Think Tank*. Washington, D.C.: The Antiquities Coalition, July. Available online: http://thinktank.theantiquitiescoalition.org/wp-content/uploads/2017/07/Policy-Brief-3-2017-07-20.pdf (accessed on 15 January 2018).

Burgess, Matt. 2017. A Rare Painting Is Stolen . . . then It Appears for Sale on the Dark Web. *Wired*. November 23. Available online: http://www.wired.co.uk/article/painting-stolen-new-zealand-sale-gottfried-lindauer-chief-ngatai-raure (accessed on 15 January 2018).

Campbell, Peter. 2013. The Illicit Antiquities Trade as a Transnational Criminal Network: Characterizing and Anticipating Trafficking of Cultural Heritage. *International Journal of Cultural Property* 20: 113–53. [CrossRef]

Campbell, Peter B. 2017. Archaeology and Blockchain: A Social Science Data Revolution? *The Guardian*, October 2. Available online: https://www.theguardian.com/science/2017/oct/02/archaeology-and-blockchain-a-social-science-data-revolution (accessed on 13 January 2018).

Campbell, Rebecca. 2017. Connecting the Luxury Fine Art Industry with the Modern Digital Economy. *Bitcoin Magazine*, October 18. Available online: https://www.nasdaq.com/article/connecting-the-luxury-fine-art-industry-with-the-modern-digital-economy-cm861368 (accessed on 15 January 2018).

Chester, Jonathan. 2015. How Questions About Terrorism Challenge Bitcoin Startups. *Forbes*, December 14. Available online: https://www.forbes.com/sites/jonathanchester/2015/12/14/is-bitcoin-the-currency-of-terrorism/#593e9ab5712d (accessed on 12 January 2018).

Coin Dance. 2018. Cryptocurrencies by Market Cap (Historical) Summary. Available online: https://coin.dance/stats/marketcaphistorical (accessed on 11 February 2018).

Coinhub India. 2018. Terms and Conditions. Available online: https://coinhubindia.com/cms/terms (accessed on 11 February 2018).

Cooper, Chris. 2016. Op. Ed.: Blockchain and the Battle for 'Blood Antiquities': Could Digital Currency Platforms Help to End the World's Deadliest Trade? *DCE Brief*, September 26. Available online: https://dcebrief.com/op-ed-blockchain-and-the-battle-for-blood-antiquities-could-digital-currency-platforms-help-to-end-the-worlds-deadliest-trade/ (accessed on 12 January 2018).

Cox, Joseph. 2017. The Dark Web Gun Trade May Be Bigger Than You Think. *Vice Motherboard*, July 19. Available online: https://motherboard.vice.com/en_us/article/j5qnbg/dark-web-gun-trade-study-rand (accessed on 18 March 2018).

Daily Telegram Group. 2018. Telegram accessed via Sixgill. Accessed via Sixgill, February 19, 2018.

Django. 2017. Fighting ISIS on the Deep Web. *Dark Web News*, July 18. Available online: http://darkwebnews.com/news/fighting-isis-on-the-deep-web/ (accessed on 13 January 2018).

Doran, Michael. 2015. A Forensic Look at Bitcoin Cryptocurrency. In *SANS Institute Reading Room*. Fredericksburg: SANS Institute. Available online: https://www.sans.org/reading-room/whitepapers/forensics/forensic-bitcoin-cryptocurrency-36437 (accessed on 11 February 2018).

Egan, Matt. 2018. What is the Dark Web? What is the Deep Web? How to Access the Dark Web. *Tech Advisor*, January 10. Available online: https://www.techadvisor.co.uk/how-to/internet/dark-web-3593569/ (accessed on 12 January 2018).

Elkins, Nathan T. 2009. The Trade in Ancient Coins in the USA: Scale and Structure. *Kunstrechtsspiegel* 9: 90–94.

European Commission. 2017. Security Union: Cracking Down on the Illegal Import of Cultural Goods Used to Finance Terrorism. *European Commission*, July 13. Available online: http://europa.eu/rapid/press-release_IP-17-1932_en.htm (accessed on 18 March 2018).

Europol. 2015. *Exploring Tomorrow's Organised Crime*. The Hague: European Police Office.

Faucon, Benoit, Georgi Kantchev, and Alistair MacDonald. 2017. The Men Who Trade ISIS Loot. *The Wall Street Journal*, August 6. Available online: https://www.wsj.com/articles/the-men-who-trade-isis-loot-1502017200 (accessed on 29 December 2017).

Federal Bureau of Investigation. 2015. ISIL and Antiquities Trafficking: FBI Warns Dealers, Collectors About Terrorist Loot. August 26. Available online: https://www.fbi.gov/news/stories/isil-and-antiquities-trafficking (accessed on 17 March 2018).

Financial Action Task Force. 2015. *Anti-Money Laundering and Counter-Terrorist Financing Measures Belgium Mutual Evaluation Report*. Belgium: Financial Action Task Force (FATF), April. Available online: http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Belgium-2015.pdf (accessed on 15 January 2018).

Geneva Public Ministry. 2016. Vestiges Archéologiques: Le Ministère Public Confisque Des Objets Provenant De Palmyre En Syrie, Du Yémen Et De Libye. *Pouvoir Jucidiaire*, December 2. (In French). Available online: http://ge.ch/justice/vestiges-archeologiques-le-ministere-public-confisque-des-objets-provenant-de-palmyre-en-syrie-du-ye (accessed on 11 February 2018).

Greenberg, Andy. 2018. Your Sloppy Bitcoin Drug Deals Will Haunt You for Years. *Wired*, January 26. Available online: https://www.wired.com/story/bitcoin-drug-deals-silk-road-blockchain/ (accessed on 3 February 2018).

Gupta, Shreyangshi. 2016. Illegal Trading of Cultural Property by ISIS—The Need for Deep Web Monitoring with Peacekeeping Operations. *Journal of International Humanitarian and Human Rights Law*, August 10. Available online: http://ilnu-jihlhr.org/illegal-trading-of-cultural-property-by-isis-the-need-for-deep-web-monitoring-with-peacekeeping-operations/ (accessed on 1 February 2018).

Gupta, Deepak, and Babu M. Mehtre. 2013. Mozilla Firefox Browsing Artifacts in 3 Different Anti-forensics Modes. Paper presented at Digital Forensics and Cyber Crime: Fifth International Conference, ICDF2C 2013, Moscow, Russia, September 26–27; Revised Selected Papers. Edited by Pavel Gladyshev, Andrew Marrington and Ibrahim Baggili. Berlin: Springer.

H.R. 1493. 2016. 114th Congress. Available online: https://www.congress.gov/114/plaws/publ151/PLAW-114publ151.pdf (accessed on 13 February 2018).

Hackett, Robert, and Jen Wieczner. 2017. How High Can Bitcoin's Price Go in 2018? *Fortune*, December 21. Available online: http://fortune.com/2017/12/21/bitcoin-price-value-prediction-bubble/ (accessed on 13 January 2018).

Hammer, Jan Peter. 2017. Stipendiatprosjekt: The Art of War, Kunsthøgskolen i Oslo. Available online: https://brage.bibsys.no/xmlui/handle/11250/2425901 (accessed on 10 February 2018).

Hardy, Samuel A. 2015. Is Looting-to-Order "Just a Myth"? Open-Source Analysis of Theft-to-Order of Cultural Property. *Cogent Social Sciences* 1: 1087110. Available online: https://doi.org/10.1080/23311886.2015.1087110 (accessed on 15 January 2018). [CrossRef]

Harman, Danna. 2015. U.S.-Based ISIS Cell Fundraising on the Dark Web, New Evidence Suggests. *Haaretz*, January 29. Available online: https://www.haaretz.com/.premium-isis-uses-bitcoin-for-fundraising-1.5366305 (accessed on 13 January 2018).

Harrison, Joseph R., David L. Roberts, and Julio Hernandez-Castro. 2016. Assessing the extent and nature of wildlife trade on the dark web. *Conservation Biology* 30: 900–4. [CrossRef] [PubMed]

highcubist. 2017a. Post in Antiques Subreddit, Antiquities Dark Net Markets. *Reddit (forum)*, November 20. Available online: https://www.reddit.com/r/Antiques/comments/7ecmud/antiquities_dark_net_markets/ (accessed on 11 February 2018).

highcubist. 2017b. Post in Antiques Subreddit, Middle Eastern Antiquities. *Reddit (forum)*, December 12. Available online: https://www.reddit.com/r/Antiques/comments/7jc60d/middle_eastern_antiquities/ (accessed on 11 February 2018).

highcubist. 2017c. Post in Dark Web Forum_Avenger. November 16, Accessed via Sixgill, February 19, 2018.

highcubist. 2017d. Post in Dark Web Forum_Avenger. November 20, Accessed via Sixgill, February 19, 2018.

Hileman, Garrick, and Michel Rauchs. 2017. *Global Cryptocurrency Benchmarking Study*. Cambridge: University of Cambridge Centre for Alternative Finance. Available online: https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf (accessed on 11 February 2018).

International Fund for Animal Welfare. 2017. Research identifies illegal wildlife trade on the Darknet. *International Fund for Animal Welfare*. June 14. Available online: http://www.ifaw.org/united-states/news/research-identifies-illegal-wildlife-trade-darknet (accessed on 3 February 2018).

Jackman, J. T. 2014. *Bitcoin for Beginners: How to Buy Bitcoins, Sell Bitcoins, and Invest in Bitcoins*. Minoan Marketing.

Kantchev, Gerogi. 2017. Buyer Beware: Looted Antiquities Flood Online Sites Like Amazon, Facebook. *The Wall Street Journal*, November 1. Available online: https://www.wsj.com/articles/the-online-bazaar-for-looted-antiquities-1509466087 (accessed on 3 February 2018).

keepen_it_one_hunnid. 2015. Comment on Durnofbranches, People Who Have Been to the Deep Internet, What's Some Stuff You've Seen? *Reddit (forum)*, July 19. Available online: https://www.reddit.com/r/AskReddit/comments/3dti4r/people_who_have_been_to_the_deep_internet_whats/ct8in5r/ (accessed on 3 February 2018).

Lam, Eric. 2017. What the World's Central Banks Are Saying about Bitcoin. *Bloomberg*, January 29. Available online: https://www.bloomberg.com/news/articles/2017-12-15/what-the-world-s-central-banks-are-saying-about-cryptocurrencies (accessed on 11 February 2018).

Mackenzie, Simon, and Donna Yates. 2016. What is Grey about the "Grey Market" in Antiquities. In *The Architecture of Illegal Markets: Towards an Economic Sociology of Illegality in the Economy*. Edited by Jens Beckert and Matias Dewey. Oxford: Oxford University Press. Available online: https://osf.io/preprints/socarxiv/gdw4k/download?format=pdf (accessed on 31 January 2018).

Madore, P. H. 2015. GhostSec: ISIS Has Bitcoin Wallet Worth $3 Million. *CCN*, November 16. Available online: https://www.ccn.com/ghostsec-isis-bitcoin-wallet-worth-3-million/ (accessed on 13 January 2018).

Maneker, Marion. 2017. Stolen Maori Portrait Appears For Sale on Dark Web. *Art Market Monitor*, November 28. Available online: https://www.artmarketmonitor.com/2017/11/28/stolen-maori-portrait-appears-for-sale-on-dark-web/ (accessed on 15 January 2018).

Marr, Bernard. 2018. Blockchain: A Very Short History of Ethereum Everyone Should Read. *Forbes*, February 2. Available online: https://www.forbes.com/sites/bernardmarr/2018/02/02/blockchain-a-very-short-history-of-ethereum-everyone-should-read/#334e4511e892 (accessed on 18 March 2018).

May, Channing. 2017. *Transnational Crime and the Developing World*. Washington, D.C.: Global Financial Integrity. Available online: http://www.gfintegrity.org/wp-content/uploads/2017/03/Transnational_Crime-final.pdf (accessed on 5 February 2018).

Mead, Derek. 2013. The Rhino Horn Crisis and the Darknet. *Motherboard*, January 24. Available online: https://motherboard.vice.com/en_us/article/vvvnj4/rhino-horn-crisis-and-the-darknet (accessed on 3 February 2018).

Merchant, Senya. 2014. How the Web Presents New Challenges for Law Enforcement Agencies. *The e-Newsletter of the COPS Office*, January. Available online: https://cops.usdoj.gov/html/dispatch/01-2014/how_the_web_presents_new_challenges_for_law_enforcement_agencies.asp (accessed on 3 February 2018).

Murray, Nick. 2013. Internet Evidence Finder Report. In *The Patrick Leahy Center for Digital Investigation (LCDI)*. Burlington: Champlain College. Available online: https://www.champlain.edu/Documents/LCDI/archive/Internet-Evidence-finder-ReportPDF.pdf (accessed on 18 March 2018).

O'Hear, Steve. 2016. Sixgill claims to crawl the Dark Web to detect future cybercrime. *Tech Crunch*, July 14. Available online: https://techcrunch.com/2016/06/14/sixgill/ (accessed on 17 March 2018).

Paganini, Pierluigi. 2015. The ISIS advances in the DeepWeb among Bitcoin and darknets. *Security Affairs*, May 22. Available online: http://securityaffairs.co/wordpress/36961/intelligence/isis-in-the-deepweb.html (accessed on 11 February 2018).

Pownall, Rachel. 2017. *TEFAF Art Market Report 2017*. Helvoirt: The European Fine Art Foundation (TEFAF).

Quirico, Domenico. 2016. How to Buy Antiquities Looted By ISIS from an Italian Mobster. *La Stampa*. October 19. Available online: http://www.lastampa.it/2016/10/19/esteri/lastampa-in-english/how-to-buy-antiquities-looted-by-isis-from-an-italian-mobster-ycO3vQFJdd14Ug5itCXNzH/pagina.html (accessed on 29 December 2017).

Rawnsley, Adam, Eric Woods, and Christiaan Triebert. 2017. The Messaging App Fueling Syria's Insurgency. *Foreign Policy*, November 6. Available online: https://foreignpolicy.com/2017/11/06/the-messaging-app-fueling-syrias-insurgency-telegram-arms-weapons/ (accessed on 29 December 2017).

Rea, Naomi. 2017. Dark-Web Shoppers Are Bidding $350,000 in Bitcoin for a Stolen Painting—and It's Likely a Fake. *Artnet News*, November 28. Available online: https://news.artnet.com/art-world/new-zealand-art-center-director-dubs-dark-web-lindauer-hoax-1161812 (accessed on 15 January 2018).

Reddit. 2017. Looking for an Antiquities Dealer, post in deepweb subreddit. *Reddit (forum)*, October 14. Available online: https://www.reddit.com/r/deepweb/comments/76bv9a/looking_for_an_antiquities_dealer/ (accessed on 11 February 2018).

Sanders, Lewis, IV. 2015. Bitcoin: Islamic State's online currency venture. *Deutsche Welle*, September 20. Available online: http://www.dw.com/en/bitcoin-islamic-states-online-currency-venture/a-18724856 (accessed on 13 January 2018).

Sengupta, Kim. 2016. The dark web is a dangerous new frontier for those who try to keep terrorists at bay. *Independent*, August 26. Available online: http://www.independent.co.uk/voices/germany-munich-attack-shooting-ali-david-sonboly-a7212151.html (accessed on 13 January 2018).

Steyerl, Hito. 2015. Duty-Free Art. *e-Flux Journal #63*, March. Available online: http://www.e-flux.com/journal/63/60894/duty-free-art/ (accessed on 10 February 2018).

Stokel-Walker, Chris. 2018. Dark web users are easy to unmask through their bitcoin use. *New Scientist*, February 1. Available online: https://www.newscientist.com/article/2160066-dark-web-users-are-easy-to-unmask-through-their-bitcoin-use/ (accessed on 11 February 2018).

storytimeppl. 2016. Post in DarkNetMarkets subreddit, Trying to find ancient artifacts. *Reddit (forum)*, January 5. Available online: https://www.reddit.com/r/DarkNetMarkets/comments/3zmk54/trying_to_find_ancient_artifacts/ (accessed on 11 February 2018).

Sui, Daniel, James Caverlee, and Dakota Rudesill. 2015. The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box. In *Science and Technology Innovation Program 03*. Washington, D.C.: Wilson Center. Available online: https://www.wilsoncenter.org/sites/default/files/stip_dark_web.pdf (accessed on 14 January 2018).

Taub, Ben. 2015. The Real Value of the ISIS Antiquities Trade. *The New Yorker*, December 4. Available online: https://www.newyorker.com/news/news-desk/the-real-value-of-the-isis-antiquities-trade (accessed on 29 December 2017).

Terrill, W. Andrew. 2017. Antiquities Destruction and Illicit Sales as Sources of Isis Funding and Propaganda. In *The Letort Papers*. Carlisle: Strategic Studies Institute, Carlisle: U.S. Army War College Press. Available online: https://ssi.armywarcollege.edu/pdffiles/PUB1348.pdf (accessed on 18 March 2018).

tery_mac. 2017. Post in Darknet subreddit, DNM for stolen goods. *Reddit (forum)*, October 15. Available online: https://www.reddit.com/r/darknet/comments/76kt8j/dnm_for_stolen_goods/ (accessed on 11 February 2018).

Ullah, Haroon. 2018. *Digital Rebels: Islamists, Social Media and the New Democracy*. New Haven and London: Yale University Press.

Underwood, Sarah. 2016. Blockchain beyond Bitcoin. *Communications of the ACM* 59: 15–17. [CrossRef]

United States Department of State. 2015. Conflict Antiquities: Forging a Public/Private Response to Save the Endangered Patrimony of Iraq and Syria. *Bureau of Educational and Cultural Affairs*, September 30. Available online: https://eca.state.gov/highlight/conflict-antiquities-forging-publicprivate-response-save-endangered-patrimony-iraq-and (accessed on 27 December 2017).

United States Department of State Bureau for International Narcotics and Law Enforcement Affairs. 2015. Money Laundering and Financial Crimes Country Database. In *INCSR 2015 Volume II Country Database*; Washington, D.C.: United States Department of State Bureau for International Narcotics and Law Enforcement Affairs, June. Available online: https://www.state.gov/documents/organization/239329.pdf (accessed on 15 January 2018).

Wall, Matthew. 2017. How Bitcoin is infiltrating the $60bn global art market. *BBC*, July 25. Available online: http://www.bbc.com/news/business-40703182 (accessed on 11 February 2018).

Wechsler, Pat. 2016. 'Dark Web' Gives Cover to Criminals. In *SAGE Business Researcher*. Thousand Oaks: SAGE Publishing, February 1. Available online: http://businessresearcher.sagepub.com/sbr-1775-98146-2715485/20160201/dark-web-gives-cover-to-criminals (accessed on 13 January 2018).

Weimann, Gabriel. 2015a. Going Dark: Terrorism on the Dark Web. *Studies in Conflict & Terrorism* 39: 195–206.

Weimann, Gabriel. 2015b. Terrorist Migration to the Dark Web. *Perspectives on Terrorism* 10. Available online: http://www.terrorismanalysts.com/pt/index.php/pot/article/view/513/html (accessed on 13 January 2018).