Studies in Conflict & Terrorism

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/uter20

The Role of Financial Technologies in US-Based ISIS Terror Plots

Joe Whittaker

To cite this article: Joe Whittaker (2022): The Role of Financial Technologies in US-Based ISIS Terror Plots, Studies in Conflict & Terrorism, DOI: 10.1080/1057610X.2022.2133345

To link to this article: https://doi.org/10.1080/1057610X.2022.2133345

Published online: 12 Oct 2022.

STUDIES IN CONFLICT & TERRORISM
https://doi.org/10.1080/1057610X.2022.2133345

The Role of Financial Technologies in US-Based ISIS Terror Plots

Joe Whittaker

Department of Criminology, Sociology, and Social Policy, Swansea University, UK

ABSTRACT

This study explores how terrorists use financial technologies in their plots. Using a database of 231 US-based Islamic State actors, it analyses how they move money and make purchases, as well as whether the use of technology affects success. Fundamentally, terrorists opt for simplicity; there is little evidence of sophisticated financial plots. Terrorists tend to use the Internet in two ways: to make purchases and to coordinate transactions. Transactions via Money Service Businesses are more likely to be part of successful plots. Finally, the paper discusses factors which explain this simplicity as well as discussing whether this may change moving forward.

ARTICLE HISTORY
Received 1 October 2021
Accepted 30 September 2022

The study of finance has been at the forefront of terrorism policy and research since the events of 11 September 2001.[1] The coordination and planning of the attack cost al-Qaeda (AQ) between $400,000–$500,000[2] and each of the attackers were able to set up bank accounts and receive international money transfers with little-to-no oversight from the banking sector.[3] In the two decades since, regulation on financial institutions – such as Suspicious Activity Reports (SARs) and "know-your-customer" protocols – has tightened substantially and international transfers have become more difficult, resulting in the flow of money to terrorists decreasing.[4] This has coincided with a reduction in large-scale terror attacks of the ilk of 9/11 and in increase in attacks by lone actors and small cells that are inspired by groups such as the Islamic State (IS) or AQ.[5]

Despite the tightening of regulations of the financial sector, several technologies have been developed which can, in theory, be exploited by terrorists. These include online peer-to-peer payment services such as PayPal,[6] cryptocurrency technologies like Bitcoin,[7] as well as using social media platforms to orchestrate the movement of funds.[8] Policymakers have expressed concern that these technologies do not have the same regulatory oversight as the traditional financial sector and, as such, may represent a vulnerability.[9]

Although there is a sizable literature on the last two decades of counter-terror financing (CTF), it is mostly focused on financial transactions at the group level – that is to say, how organizations such as IS or AQ generate, move, and spend money.[10] There is a small but growing empirical literature which systematically analyses the

CONTACT Joe Whittaker j.j.whittaker@swansea.ac.uk Department of Criminology, Sociology, and Social Policy, Swansea University, UK

ways in which individual terrorist actors or small cells have financed their plots.[11] However, these studies tend to focus on finance more broadly rather than the role of technology. There is a dearth of empirical research into how terrorists have innovated using financial technologies, with the literature tending to ask questions such as "where does the money come from and what is it used for?"[12]

This study addresses this gap by empirically analyzing a dataset of 231 IS terrorists that operated in the US from the years 2012–2020. The following research questions are explored to better understand the role of financial technology in contemporary terrorism:

1. What kinds of technology do terrorists use to move money?
2. What technology do terrorists use to make purchases in pursuit of their plots?
3. Does the technology that terrorists use affect their chances of success?

While previous studies have analyzed terrorists' financial activity at the *actor* level – for example, by creating databases based on individual case files and reporting behaviors,[13] this research builds on this by becoming the first study to code at the *transaction* level, and in doing so, adding a layer of depth.

This article first discusses the existing relevant literature on the topic of financial technologies in terror plots, before outlining the study's methodological considerations. This is followed by the findings – which broadly suggest that terrorists favor technological simplicity in financial transactions both when moving money and making purchases. The paper concludes by discussing why terrorists opt for simplicity by drawing on six terror finance considerations which are posited by Freeman & Ruehsen: Volume, Risk, Convenience, Simplicity, Cost, Speed,[14] before questioning whether we should expect to see an increase in cryptocurrencies and other sophisticated types of transaction in future.

Previous Research

Tried and Tested Methods

Recent studies into CTF have tended to suggest that, for the most part, terrorists have tended to opt for simple methods of engaging in financial activities rather than using innovative methods. When considering how money is moved, the traditional banking sector and Money Service Businesses (MSBs)[15] – such as Western Union or MoneyGram – are utilized heavily. In their most recent *National Terrorist Financing Risk Assessment*, the US Department of Treasury highlights these two methods as popular amongst US terrorists, noting that both are attractive because they offer the ability to send money globally quickly and efficiently.[16] Moreover, both of these methods are highlighted as vulnerable because low amounts of money are typically sent, therefore making it easy to bypass CTF regulations.[17] Similarly, a 2020 report for the UN Security Council – made up of surveys completed by member states – found that the majority of respondents identified the both the formal banking system and MSBs as methods that are used by terrorists to move funds.[18] In the Financial Action Task Force's 2015 *Emerging Terrorists Financing Risks* report, they note that despite a host of new potential

technological vulnerabilities, the banking system continues to be the most reliable and efficient way to move funds, while MSBs are also exploited, highlighting the latter's lack of regulation.[19]

Studies that have focused on individual terrorists and small cells have tended to paint a similar picture. Most relevant to this study, Vidino, Lewis, and Mines' report on 204 US-based IS terrorists found that the financing of plots is low in terms of sophistication and that MSBs were frequently used.[20] In her study on 40 European jihadist cells, Oftedal finds that cash, MSBs, and bank transfers were the most common methods of transferring money, both for receiving external support, as well as moving money between cell members. In short, both governmental reports and academic scholarship suggest that terrorists opt for low sophistication, tried and tested methods of moving money.

Another means of moving money that has been popular is the payment system of *hawala*. Likely tracing its origins to South Asia, the system is possibly as old as the beginning of monetary transactions themselves.[21] As Salami explains:

> It works with a network of operators. An individual wishing to transfer funds would contact an operator at his location and pay a commission for money he wishes to transfer. The collector, at another location, contacts the local operator and collects the money less the commission. Its usage is now widespread but purely based on trust.[22]

The benefits of this option for would-be terrorists should be clear – by offering an opportunity to bypass the traditional banking sector, MSBs, or some online platforms it means that CTF regulations can be avoided, and money sent in a relatively anonymous and fast way.[23]

Several scholars have highlighted this as a method that is utilized for the purposes of terror financing,[24] as well other stakeholders including the Financial Action Task Force[25] and Europol.[26] Research conducted with providers of illegal financial services and law enforcement found that Switzerland could be vulnerable for terror financing using this method.[27] Given the international nature of terrorism, it has been argued that it can provide the opportunity to move large sums of money across borders, which is challenging to trace once it has left its host country.[28] Presently there are few empirical studies that directly quantify *hawala's* popularity within terror plots. There are exceptions, however: In the above-mentioned report by the UN Security Council, a majority of member states highlighted it as a method that is used,[29] but in Oftedal's study on European jihadists, she finds that it plays no direct role.[30] It is important to note that *hawala* should not be seen as an independent category of payment because it protrudes into different types of money transfers, it is often used in conjunction with MSBs and cash transfer,[31] suggesting an interweaving of the regulated and underground banking sectors.

Online Movement

Although the above-presented research suggests terrorists opt for tried and tested methods of moving money, online technologies have been repeatedly signaled out as ripe for exploitation. It should be noted here that online peer-to-peer technologies such as PayPal are MSBs. However, for the purposes of this discussion and research, they will be treated as distinct from their brick-and-mortar counterparts.

As early as 2010, Jacobson noted that terrorists were exploiting the Internet by using it to raise and move funds, which he argues was likely to expand in future, particularly given the broad reach, time efficiency, and anonymity for donors and recipients.[32] Basaranel argues that the Internet presents a challenge to security services because of the unprecedented opportunities for anonymity, secrecy, speed which can circumvent CTF efforts.[33] The US Treasury highlights online person-to-person transfer companies as vulnerable to exploitation because many have not maintained the same degree of AML/CTF controls as their brick and mortar counterparts.[34]

Despite these concerns, there is relatively little empirical evidence that online payment systems have been heavily utilized by terrorists. While the UN Security Council report highlights a majority of nation-states were concerned about the formal banking sector, MSBs, and *hawala*, only 27% were concerned with the abuse of technology (including social media, prepaid cards and mobile banking).[35] Similarly, in Oftedal's study on European jihadists, there are no cases which involved online or mobile technologies to finance plots.[36] Although the literature makes frequent mention to case studies of individuals using the Internet,[37] there is little way of knowing how widespread the practice is in terror plots compared to other methods.

Beyond using online payment systems, scholars have also noted in the importance of social media as a facilitator of terror finance. Keatinge & Keen argue that the literature in CTF has neglected this topic and that it presents an important vulnerability as it offers the opportunity to harness the viral nature of social media – as has been done with terrorist propaganda – while at the same time noting the social media platforms contrast with the traditional banking sector because they are not legally obliged to deploy resources to identify, report and disrupt terror finance.[38] Similarly, the Camstoll Group reported in 2016 that there were a number of financiers and fundraisers for both IS and al-Qaeda on mainstream platforms such as Facebook, Twitter, and YouTube who were able to utilize these platforms to raise funds to pay for weapons, salaries, and infrastructure, totaling an amount in the millions of dollars.[39]

One topic that has received substantial attention in recent years is the possibility of terrorists exploiting cryptocurrencies. Several studies have highlighted the clear dangers that they pose: they offer the ability to bypass the regulated banking sector as well as possibility for anonymous peer-to-peer transfer.[40] The general argument offered is: CTF has become substantially more sophisticated and moving money has become difficult, this may spur innovation toward blockchain technology because of these upsides.[41] Moreover, it is clear that at the organizational and supporter level, terror groups are interested in soliciting funds via these methods. Research by both Conway and Malik highlight several online pages that were set up from late 2017 to solicit funds for IS and other groups,[42] although it is not clear how successful these attempts have been.

Despite this growing body of academic attention, the scholarly consensus is that there is currently little reason to believe that individual terrorist actors are regularly exploiting cryptocurrencies, although many warn that this may increase in future. For example, Keatinge and Danner note that terrorists' use of cryptocurrencies has been limited, but it may be one of a number of innovations that emerge in the future.[43] Similarly, Malik highlights many of the advantages to terrorists, but also concedes that the evidence is anecdotal and there is little indication that it has been adopted on a

larger scale. Dion-Schwarz and colleagues find that there is little evidence of the adoption of cryptocurrencies, and little motivation from terror organizations to do so, but they too note that this may change in the future if other forms of finance are shut off.[44] Whyte also notes that there is limited evidence of their usage, while also arguing that they contain several unique opportunities for terror financing. Finally, Eisermann observes that the existing studies on terror finance suggest that there is only a small number of publicly documented cases of cryptocurrencies being used, that the combination of a dynamic situation and high potential risks should concern policymakers.[45]

Financial Technology in Purchases

Although there is a sizable literature on the types of methods that are used to raise and move funds,[46] there is very little on whether – and if so, how – technology is used when buying goods for terrorist events. Salami suggests that vendors such as eBay and Amazon have been known to accept cryptocurrencies, but only presents this as a potential vulnerability rather than providing evidence.[47] There is some anecdotal data which can guide an understanding of this question. For example, the US Department of Treasury's risk assessment reports include several examples to highlight their point, including the case of Ahmad Rahimi – who is also in this sample – who acquired much of his materials to construct a bomb via eBay.[48] However, anecdotal evidence runs the risk of misunderstanding how frequently phenomena actually occur, particularly when it happens in a highly newsworthy event such as a successful terror attack. Therefore, the empirical basis for the use of financial technologies when planning events is low; it is unknown if terrorists opt to use cash to pay for goods, rather than using bank cards or online technologies.

The Relationship between Financial Technologies and Event Success

Terrorists have become adept at exploiting the Internet for a range of behaviors including the dissemination of propaganda, recruitment, and attack planning.[49] However, recent research suggest that using the Internet may actually be an impediment to terrorists successfully conducting plots, often because they recklessly alert law enforcement to their activity.[50] Presently, there is little empirical literature which analyses whether the use of online financial technologies helps or impedes the chances of a plot being successful. In their risk assessment, the US Department of Treasury notes that online peer-to-peer transactions are not subject to AML/CTF controls which has created a vulnerability, which could be interpreted as indicative of success.[51]

There is some indication that other factors, notably the amount of money being transferred, may affect the chances of success. For example, Keatinge and Keen observe that within their sample of actors, the amounts of money that were being transferred were generally below a threshold which could have reasonably been flagged by financial institutions, which they highlight as being problematic for law enforcement investigations.[52] The US Department of Treasury also highlights that most cases of terror finance are small and not suspicious in nature, which they also consider a vulnerability.[53]

Summary

A brief overview of the existing literature leads to several inferences for further study. Firstly, research tends to suggest that terrorists opt for simplicity when moving money and there is little reason to believe that online financial technologies are currently being exploited. However, almost every author cautions that this situation could change in future as terrorists become more literate with these technologies. Secondly, we know very little – aside from some anecdotal evidence – about how terrorists use technology to purchase items that they use as part of their plot, and finally, there is also a knowledge gap as to whether using online technologies are a net-positive or negative in the pursuit of their plots.

Methodology

Data

The data for this study are generated from an existing open-source database which analyzed the online behaviors of Islamic State terrorists in the US from 2012 to 2020 by this author.[54] This database was created by constructing a directory of terrorist actors using three approaches. Firstly, by collecting the names on the George Washington University's *Program on Extremism* (PoE) IS repository, which details the criminal investigation of 205[55] terrorists in the US[56] Secondly, by consulting two reports which detail 100 individuals that either attempted or were successful in traveling from the US to the caliphate,[57] and finally, by generating a list of terror attacks from the Global Terrorism Database (GTD) by searching for incidents in the US from 2010–2018.[58] Having created a directory of actor names, case files were generated for each terrorist from a range of court document sources such as: the PoE repository, the Department of Justice website, the Investigative Project on Terrorism, as well as legal search engines such as CourtListener. This was supplemented with data from academic and gray literature which outline cases of US-based jihadist terrorists.[59] Finally, news data were collected from LexisNexus News and Monitoring and Google News. Where accounts conflicted, the hierarchy of open-source data proposed by Gill was followed, favoring official court transcripts the most, followed by affidavits, local journalism, then national journalism.[60] The reliability of academic and gray documents was dependent on which of the above sources were cited.

After data collection, inclusion and exclusion criteria were applied. To be considered an IS terrorist, it would be too narrow to focus only on "formal" membership given the number of individuals that are inspired by the group rather than directly guided. Therefore, the database follows the lead of the Profiles of Individual Radicalization in the United States (PIRUS) codebook, who define membership broadly, even if the group does not acknowledge it.[61] Actors are deemed to be IS inspired if they either explicitly support the group or if they engage with its ideological materials, as long as their actions are deemed to be in furtherance of the group's goals. To be deemed as operating in the US, the actor must fulfill one of the following criteria:

a. Been charged in the US, or
b. Be a US Citizen or permanent resident and resided in the US until five years before their event, or
c. Resided in the US at the time of their activity.

The database includes those that acted from the earliest identified actor joining the group in 2012 until data collection was complete in May 2020. In some instances, the available data for terrorist actors were so little that no antecedent or event behaviors could be identified. In these cases, they were excluded – this amounted to 21 in total. After applying these criteria, the database consists of 231 terrorist case studies.

Coding

For the present study, data were coded to assess the ways in which terrorists used financial technologies. To begin, demographic and socioeconomic factors from the previous study on terrorists' use of the Internet are detailed to offer a snapshot of the cohort. Then, twelve coding variables are used to detail how terrorists moved money. This includes: the details regarding the individual that sends the money, those that receive it, the date of the transaction, the amount in USD, as well as the source of the funds (i.e. was the money from the sending actor or did they procure it from other sources such as peers, IS, the FBI, or via credit). With regards to variables relating specifically to the use of technology, the data are also coded into categorical variables which describe the type of movement (Cash, MSB, bank transfer, online payment service, cryptocurrency, and other virtual currencies). Furthermore, a dichotomous variable is included to identify whether the transaction took place online or offline, as well as two more dichotomous variables if they transactions were coordinated by online or offline discussions.

Next, eleven variables are used to ascertain how individuals made purchases. This includes the actor that made the purchase, the date, the amount, the source of the funds and details of what was purchased. With regards to the role of technology, variables are included which categorize the method used to purchase the goods or services (Cash; bank transfer; credit/debit card; check; MSB; online payment service; virtual currency; other). As well as this, categories of the type of seller are included (co-ideologue; unlicensed trader; offline licensed trader; online trader; FBI; US government; other). Finally, a dichotomous variable is included as to whether the purchase took place online or offline.

This research follows the lead of Vidino, Lewis, and Mines by only considering transactions that are relevant to terrorists' plots as opposed to mundane everyday purchases. Terrorists purchased food to eat, yet these types of habitual expenses are not deemed as being materially relevant to the plot.[62] There are some gray areas; for example, actors often bought clothes in preparing their trip for the caliphate, yet it was only coded if the clothes were deemed relevant. In this case, the purchase of "everyday" clothes like t-shirts was excluded, but combat boots and camouflage were included.

There are some instances in which the data aggregate a range of transactions. The starkest example of this is the case of Mohamed Roble, in which the court documents outline 45 different ATM transaction between the dates of December 28, 2014 and May 11, 2015 for a total of $47,071.62.[63] In these cases, the mean USD amount and the median date were coded, in this case it was coded at 45 individual instances of $1046.36 withdrawals on March 4, 2015. This should be taken into account when considering the averages involved in money moved and spent as these are approximate figures.

The data were collected and coded by the author. To ensure rigor, twenty-seven cases (c11%) were re-coded by a secondary coder which were tested for inter-rater reliability in two ways. To begin, the number of transactions deemed suitable of inclusion from each of the case studies was calculated using Krippendorf's Alpha, yielding α of .675, which is deemed acceptable to draw tentative conclusions,[64] although with a relatively wide 95% confidence interval of .48-.85. Looking at the coding reflectively, there were some ambiguous inclusion and exclusion cases based on: a) whether a purchase was considered relevant to the plot, as discussed above, or b) whether there was enough information to deem something a transaction – for example, some behaviors implied a purchase without explicitly mentioning it. Although the secondary coder was trained to look for explicit mention, there were still some edge cases which required a subjective judgment. Next, the transactions which both the primary and secondary coders deemed suitable for inclusion were also tested, resulting in high levels of agreement. The nominal (i.e. categories) and ratio (i.e. monetary amounts) had to be tested separately, yieldeding an α of .85 (95% CI= .81-.89) for the former and an α of .96 (95% CI= .87–1.0) for the latter. This suggests that while there is some subjectivity in deciding which transactions are included, the transactions that do make it are relatively clear cut.

Methods

To help paint a picture of the sample, descriptive findings are outlined below. These include some demographic information of the terrorist actors, as well as findings related to their transactions. This is then followed by the descriptive findings that relate to how terrorists have utilized technology in financial transactions. Finally, chi-square tests and binary logistic regressions are employed to offer a picture of how different types of moving money can affect the success of plots.

Limitations

Utilizing secondary open-source data can be problematic given that the original authors often have different goals to a researcher. Many of the data are collected from court documents in which the prosecutor is attempting to convey enough information to justify charges being brought. Similarly, journalists are typically interested in stories with news values. It is not feasible for either to spend time detailing either behaviors that the terrorist *did not* engage in or discussing activities that do not fit their underlying narrative. This is important because if a financial transaction is not deemed to be important to the case, then it may cause a bias within the data. For example, if an individual sent a large sum of money to IS, this is likely to be detailed. On the other hand, an actor spending $30 filling up their car before a vehicle-based attack may be overlooked.

In a similar vein, collecting data via these sources results in different levels of detail depending on the terrorists' eventual actions. This richest data source available were court documents, but most of the successful travelers have not been publicly charged, which often resulted in there being less information available about their

antecedent and event behaviors. Similarly, when it comes to news journalism, certain types of terrorist actors or events gathered much more information than others. The small numbers of successful attackers often generate long reads from both local and national newspapers, as do pieces on many female actors that traveled to join IS. On the other hand, individuals that were arrested for gun-related offenses or lying to the FBI generated far less attention. Although terrorism is a black swan event which is highly newsworthy and often generates coverage, there is a clear disparity between different cases.

Finally, base rates continue to be problematic in terrorism research. Understanding the prevalence of financial activities in the general population is easier than other behaviors, such as making threats online, which are difficult to quantify.[65] For example, the Federal Reserve conducts an annual report which estimates all the noncash payments each year, while polling companies such as Pew Research conduct surveys on how Americans pay for items. However, these are broad strokes, and it is difficult to account for comparable age ranges of terrorists, socioeconomic status, or geography, which may be reasonably expected to affect the use of financial technology. Given this, it is difficult to identify whether this sample is out of the ordinary.

Results

Demographic

A previous study on this cohort of terrorists offered the following descriptive statistics which outlines their demographic profile as well as details about the cohort's events.[66] The sample consists of 231 terrorist actors, who are predominantly male (90%) and relatively young ($n = 223$, mean, 27, median, 26, mode, 20) with a distribution between 15 and 55.[67] Although it is difficult to use open-source data to establish terrorists' income or level of deprivation,[68] the sample seems to err toward the bottom half of the socioeconomic spectrum. Employment information could be ascertained for 186 actors and 40% did not have a job – this should not be compared with unemployment rates, which track those who are not employed but are willing and able to work – and a further 34% worked in either the service or low-skilled sector. Of the 141 of whom information could be found, two-thirds' high level of education was a high school diploma, with 16% not achieving this, while relatively fewer (14%) had completed a college education and 1% attaining a postgraduate degree.

The sample was made up of individuals with several roles: Those that sought to travel to the caliphate (49%), those that plotted an attack (29%), individuals with peripheral roles such as financier (17%) or non-financial facilitative support (28%), as well as a small number (8%) that made bombs. Most of the terrorists acted within a cell of larger than two individuals (45%), with eighteen percent acting alone without any support, 24% conducted their plot alone but with guidance from a wider network, and 13% acted as a dyad. Slightly fewer than four in ten were judged to have a plot that was successful, and the majority were arrested (83%). The average sentence of the 120 individuals that have been given sentences is around 15 years (mean = 183 months, median = 178 months, mode 180 months).[69]

Movement Transactions

There were 224 financial movement transactions. Of these transactions, 93 (42%) were sent by an IS terrorist within the US, 19 (9%) were sent by IS supporters outside the US, while 15 (7%) were sent by an individual working for the FBI. The rest (43%) were either not identifiable or not applicable (for example ATM deposits). For receivers of money, 87 (39%) were US-based IS supporters, 92 (41%) were foreign-based IS supporters, 19 (9%) were working for the FBI, with 26 (12%) unidentifiable or not applicable. In 212 of the transactions, the amount sent was identifiable, totaling $480,001 with a mean of $2,264.16 and median of $1,000. In cases where the source of the funds could be identified ($n = 169$), the plurality of transactions was financed by the individual sending the money (46%), with other co-ideologues the next most likely (19%). A smaller number of transactions were financed by credit lines or loans (14%), as well as a number being financed by the FBI (9%), crime (7%) and, finally, a relatively small number of transactions were sent by the IS organization itself (6%).

Purchase Transactions

319 purchases of goods or services were made by 102 actors in this sample (44%) that were deemed related to their overall plots. The amount could be identified in 70 instances for a total of $96,980 for a mean of $1,385 and a median of $641. Reflecting on the coding process retrospectively, there may have been a bias toward reporting the amount in transactions of higher value, while neglecting smaller ones. Travel tickets were the most frequently occurring purchase, making up around a quarter, with firearms (and related materials such as ammunition and other paraphernalia) accounting for 14% of transactions, closely followed by bomb-making materials and other attack materials each at 12%, with military style clothing and gear accounting for 10% of purchases. Seven percent of transactions involved the purchase of virtual currency (including prepaid cards), while 1% was for storage. Around 18% was classified as "Other" – which includes travel documents such as passport renewals. Where the source could be identified ($n = 143$), 39% were funded by the purchasing actor, while a quarter were funded via credit or loans. 16% of purchases were funded by the FBI, while 15% were sourced from co-ideologues other than the purchasing actor. Only a handful (4%) were sourced by IS at an organizational level, while even fewer (1%) were paid for directly by criminal activity.

The descriptive findings are seemingly in line with existing research into terror finance. Studies have suggested that when looking at the financing of cases at the micro-level, the amount of money being moved is typically small enough to avoid detection by CTF regulations.[70] For both movement and purchase transactions, the mean was under $3000, which are inflated by a small number of sizable transactions; shown by the median of movement and purchase transactions both being $1000 or under. The data is also in line with previous research which suggest that plots are mostly self-funded, either by the individual making responsible for the transaction or other members of their cell.[71] It should be noted that in both the cases of movement and purchases, data could be entered as "unknown" for the source of funds, which likely undercounts self-funded plots. Similarly, the finding that travel tickets – mostly

airplane – were the most frequent category is in line with the US Department of Treasury who highlight travel-related purchases this as the most common type of IS activity.[72]

Even though it is small number of total transactions in each instance, the presence of the FBI-funded plots is noteworthy. In the entire database of terrorists, there was either an undercover agent or confidential source in 45% of cases (this increases to 57% in cases where the actor was arrested). For movement transactions, they either sent or received funds in 20% of cases and were responsible for financing 9% of these transactions. Similarly, the funds for purchases were provided by the FBI in 16% of cases. Horgan and colleagues discuss the role of undercover FBI agents in counter-terror investigations, finding that terrorist actors came into contact with an undercover agent in around half the cases in their sample and 2% received financial support from them (although this makes up around 10% of all those that received any type of financial support).[73] Similarly, Greenberg & Weiner note that the use of undercover agents has risen steadily in cases of IS investigations in the US,[74] while Human Rights Watch claim that undercover involvement may have created terrorists out of law-abiding individuals while conducting sting operations.[75] The question of the validity of such operations is beyond the scope of this research, but it does posit that in the economy of terror financing, the FBI plays a small but meaningful role.

RQ1: What Kinds of Technology Do Terrorists Use to Move Money?

When assessing how money is moved, the data suggest that terrorists are not regularly exploiting online financial technologies. Actors in this sample heavily favored cash transactions, making up 60% of the 204 identifiable cases. Around 29% were via MSBs such as Western Union or MoneyGram, with 6% using online payment platforms like PayPal. Transactions that involved bank transfers and virtual currencies (excluding cryptocurrencies) were both 2%, while 1% utilized cryptocurrencies to move money. As discussed above, the existing literature focuses heavily on the exploitation of banks[76] and MSBs,[77] whilst simultaneously playing down the role of newer technologies, particularly cryptocurrencies.[78] These findings support the main thrust of the prevailing wisdom: terrorists do not seem to have exploited online payment technologies in any particularly systematic manner, opting instead for the simplicity of tried and tested methods.

The prevalence of cash transactions seems high but can be partially explained by the nature of the coding system; cash deposits into banks were treated as cash transactions. Looking deeper in a three-variable crosstabulation, cash transactions between domestic IS supporters was relatively low – only 5% of cash transactions – which is outnumbered by transactions to and from undercover FBI agents, which were 4% and 8% respectively. The rest were not applicable (i.e. cash deposits or withdrawals from banks), which suggests that terrorists are utilizing the banking system and cash is easily moved in and out of banks with little detection. However, it is also important to note that attempting to track cash transactions between terrorists is open to a bias of available data. Cash transactions between terrorists is likely to be under-reported in court documents compared to cash deposits into banks, which can be subpoenaed, or transactions with FBI agents, which are recorded by law enforcement. Similarly,

when terrorists use MSBs or online payment platforms these can also be traced far more easily than cash and often make up the basis of criminal affidavits.[79] As such, it is difficult to truly gauge the "dark figure" of crime when it comes to cash being used in transactions between terrorists.

The relative lack of online transactions is instructive – only 21 transactions sent money using any type of Internet technology (10%). Like many aspects of the Internet, terrorists can, in theory, send and receive money from all over the world at almost no cost. The US Department of Treasury suggested that such online payments are ripe for exploitation because they have not kept the same CTF norms as their brick and mortar counterparts.[80] One of the cases in which it was used was that of Mohamed Elshinawy, who received five payments through PayPal from Siful Sujan on behalf of IS for $7,700 in total.[81] It was a single payment made via Western Union, which the FBI observed him picking up which triggered the investigation into motion, but Elshinawy had already received a number of PayPal payments by this point. This case highlights some of the advantages that can come from using online payment methods; this plot disguised the transaction by using a U.K.-based IT company to erroneously invoice Elshinawy via eBay which seemingly avoided detection from law enforcement. However, cases like this seem to be very much the outlier. Where online payment systems are used, they seem to be used in plots alongside MSBs.[82]

Even less commonly used are cryptocurrencies, which were utilized by only one terrorist in this sample – Zoobia Shahnaz. As noted above, there is a growing literature which warns of the potential for exploitation of this type of movement, often citing this case as an example.[83] In July of 2017, Shahnaz fraudulently obtained a bank loan and used credit cards to purchase over $62,000 of cryptocurrencies, which she then converted back into US dollars and subsequently wired over $150,000, to various individuals and shell companies in China, Turkey, and Pakistan that were associated with IS, before attempting to travel to the caliphate herself.[84] Although the cryptocurrency aspect of this case gathered substantial attention from the media and academics, the instructive takeaway from this plot is the range of different types of terror financing that were employed by a relative novice – Shahnaz searched Google for simple questions relating to the movement of money.[85] To source this plot, she used her own funds from her well-paid job as a lab technician, a loan, and more than 10 credit cards. She then purchased and sold cryptocurrencies to take advantage of the pseudonymity that it can provide, before using both brick and mortar MSBs and bank transfers to send the money to shell companies. Moreover, she carried $9,500 in cash with her as she attempted to travel, knowing that she would not have to report this to the border authorities.

To further highlight the simplicity of actors' plots, it is instructive to look at how many different types of movement transaction were utilized. There were 36 different actors that sent money, resulting in 86 different transactions, but no actor used more than two methods, and each utilized either cash or MSBs as one of the methods. One of these actors was Lionel Nelson Williams, who sent an undercover officer $50 via an electronic transfer service at Walmart as well as purchasing a $200 prepaid Visa gift card and sending the balance virtually to the same agent.[86] Conversely, 34 actors received money from 133 transactions, but a maximum of three different types of transaction were used and only by two individuals. These individuals have already

been discussed: Zoobia Shahnaz, who received money via cash withdrawals, bank transfer, and virtual currencies as part of her plot[87] and Mohamed Elshinawy who made cash withdrawals, as well as receiving money via Western Union and PayPal.[88] While these cases stand out as being relatively sophisticated, this study shows that they appear to be the outliers rather than the norm.

Although terrorists in this sample opt for simpler methods of transferring money, this does not mean that online technologies are not utilized in facilitating these transactions. Even though only 21 of the 202 identifiable transactions (10%) took place online, seventy-seven (34%) were coordinated via the Internet. Given the trans-national reach of this sample, this makes sense. Take, for example, the alleged cell of three individuals Abdulrahman El Bahnasawy, Talha Haroon, and Russell Salic, who were based in Canada, Pakistan, and the Philippines, respectively. El Bahnasawy and Haroon planned an attack in multiple parts of New York City, including Times Square, the subway system, and music concerts.[89] To fund this plot, Salic allegedly sent $423.80 from a Western Union in Cagayan de Oro to an undercover officer.[90] The three men do not appear to have known each other offline and the communication between them was facilitated via different online messaging applications. Online coordination can be seen in the cases of the first wave of Minnesotans to travel to IS,[91] the group of individuals indicted for the financing of the foreign fighter Abdullah Ramo Pazzara,[92] and the case of Mohamed Naji, which all involved funds being sent using physical MSBs but were facilitated online. Although there may be a relatively small cyber footprint in the actual movement of money, communications technologies still offer important support to traditional ways of transferring money.

Although terrorists used the Internet for coordinating funds, cases in which the whole plot was coordinated online – like El Bahnasawy, Haroon, and Salic's – were still rare. It was much more common for individuals that had preexisting offline networks to use the Internet to help coordinate payments. This is in line with the broader research on terrorists' use of the Internet which posits the Internet as a facilitator of offline social networks rather than as a replacement.[93] While social media does offer the ability to help coordinate the movement of money around the world, often beyond the reach of the security services, for little cost, there do not seem to be many cases in which it is used by individuals that have no previous connection. Rather, online and offline behaviors are often inseparably intertwined.

One noticeable absence is *hawala* and other similar service providers. There are some clear examples of this, such as the case of Mohamed Naji, mentioned above, which involved his unindicted girlfriend sending money to a third party in Yemen, who then brought the cash to him.[94] Less clear are the cases in which the court documents outline instances of individuals transferring money to third parties in the Middle East or South East Europe, implying that it is intended to reach a specific individual.[95] In these cases, a reasonable assumption is that this money makes its way to the intended individual within IS territory. However, given the final step is informal and takes place outside of US jurisdiction, the court documents cannot easily include it. Much of the academic literature suggests that these types of movements are still commonplace,[96] so the most reasonable interpretation from this study is that it cannot capture this data point with sufficient accuracy.

RQ2: What Technology Do Terrorists Use to Make Purchases in Pursuit of Their Plots?

The actors in this sample made 319 purchases, of which 170 could be determined to be either online or offline and the distinction between the two domains is split roughly down the middle – 47% and 53% respectively. It is difficult to estimate a base rate for all purchases in the US, it has been suggested that e-commerce accounts for around 11% of the total amount purchased in dollars. Going deeper into the type of seller, the most popular was offline licensed traders such as Walmart (9 purchases) as well as various home improvement stores, which accounted for 42% of sales. Next were online traders, who accounted for 40% of purchases, including eBay (33 purchases) and Amazon (6 purchases). These online platforms were popular for the purchase of attack materials, such as Ahmad Khan Rahimi, who over June-August 2016 used eBay to purchase a range of bomb-making materials including circuit boards, citric acid, ball bearings, and fireworks ignitors,[97] or Esaamah Abdullah Rahim, who ordered three knives from Amazon, one of which he would eventually use in his attempted attack on Boston police officers in June 2015.[98] The US Government was the next most frequent seller at 10% – this is almost entirely made up of purchases or renewals of passports or other travel documents, and finally, FBI undercover agents accounted for 7%, for example in setting up sting operations that involved selling illicit materials. An example of this is the case of Mufid Elfgeeh, who via an undercover source purchased a selection of handguns, silencers, and ammunitions before immediately being arrested by the FBI.[99]

In the 108 transactions in which the method of payment can be identified, there is prevalence toward the banking sector with debit and credit card payments accounting for 57%. The Federal Reserve estimates that debit cards account for roughly three-quarters of all noncash payments in 2018, which is somewhat higher this sample.[100] Cards were used for a wide variety of purchases including flights,[101] firearms and ammunition,[102] storage,[103] and even a drone.[104] The next most popular type of payment was cash, which accounted for 23%. Although it is difficult to estimate the broader use of cash among the US population, this is in line with an ever-lowering figure at the expense of card payments.[105] The use of cash includes the purchase of fake passports[106] and hotel rooms.[107] After this were online payment systems, mostly PayPal, at 18%, followed by 2% of cases which were conducted by bank wire. Of the 37 actors that made these 108 transactions, no actor made more than 1 different type of purchase. In other words, individuals stuck to what they knew rather than using a multiplicity of different methods to purchase goods and services.

As noted above, there is little in the way of existing empirical literature on this topic. The results of RQ2 suggest that when it comes to purchases, terrorists opt for simplicity. Although around half the transactions took place online, this is a very common occurrence in the present day and roughly in line with what would be expected given a random sample of individuals, or even more so given the cohort's median age was 26. Similarly, actors tended to use debit and credit cards for purchases more than any other system of payment, which also holds true with the general population. As with RQ1, the findings suggest that terrorists tend to rely on tried and trusted methods without resorting to any highly sophisticated methods of paying for items related to their plots.

RQ3: Does the Technology That Terrorists Use Affect Their Chances of Success?

Much of the counter terror finance literature uses the language of "vulnerabilities" of certain types of payment or sector.[108] Therefore, it is worthwhile to examine the relationship between different types of financial technologies and the success of terrorist plots. To begin, each of the types of movement transaction (cash, MSB, bank transfer, online payment system, cryptocurrency, and non-crypto virtual currency) are converted into binary dummy variables so they can be tested against whether the actors' events are successful using chi-square tests. The results show that only one type of transaction – using an MSB to move funds – holds a significant relationship; those that did were 2.9 times more likely to be successful than those that did not.

This finding is important in itself; although different types of movement require degrees of sophistication, for the most part, it does not affect plot success. At the simpler end of the technological spectrum, one might be inclined to suggest that cash offers a covert way of moving money without detection from law enforcement as it is much harder to trace, while at the other, it is claimed that electronic payment systems offer a distinct threat because they do not have the same level of CTF regulations as brick and mortar banks.[109] It is worth noting that the small sample of cryptocurrencies make it difficult to draw any meaningful conclusions. Given that it is still a relatively new phenomenon which is not yet heavily used by terrorists, one must instead look at case studies – like that of Shahnaz – qualitatively to draw hypotheses for future analysis.

A central thesis of the terror finance literature that the small amounts of money moved through MSBs poses a risk because they are not detectable.[110] Therefore, it is instructive to assess whether transaction size has an effect on plot success. However, because of the high variance between different transfers (from $20 to $100,025), this variable will be unsuitable as the unit of measurement is very small compared to the size of a meaningful change (the result is a significant correlation but an odds ratio of 1.000 with a 95% CI of 1.000–1.001). Therefore, it is recoded into a series of dichotomous variables below and above certain thresholds. It is important to include multiple thresholds that are theoretically justified because, as Ranganatham, Pramesh, & Aggarwal note, it is not good practice to have arbitrary cutoffs when conducting multivariate analysis.[111]

The first is $800, which is chosen because it is outlined by the US Department of Treasury as the threshold for which the vast majority (94%) of suspicious activity reports are filed.[112] Chi-square analyses reveal that transactions of over $800 are 3.88 times more likely to be successful than those under. The second threshold is the mean transaction amount ($2,264), which holds no significant correlates, and finally, the third threshold is $3,000, given that this is the figure for which MSBs are required by law to collect personal information on individuals sending money.[113] Again, chi-square tests show that sending more money is indicative of success; transactions above $3,000 are 3.27 times more likely to be successful that those under that figure. Despite repeated claims to vulnerability due to small amounts of money being moved without detection, the data presented in this study suggest that higher amounts of money are associated with event success. An explanation for this could be that, regardless of CTF regulations, plots are simply more likely to be successful if they have more funding at their disposal, although this would somewhat go against the notion that

low-cost attacks such as lone-actor knife or vehicle attacks pose a greater risk than better funded cell activity.

Given that the use of MSBs is strongly related to event success, it is prudent to test whether it predicts success by conducting a binary logistic regression. The transaction threshold ($800) is chosen as a control variable because it is shown to have a strong relationship with event success. These variables are tested for collinearity, with each of their variance inflation factors coming in around 1.000, which is well under the acceptable threshold, which suggests no biasing effects. The results of the regression (Table 1) show that when transferring money via MSBs predicts the success of terrorist plots, even when controlling for the amount sent. Note that because there were more unsuccessful events than successful, the former is chosen as the baseline, so the relative risk – Exp(B) – of .269 suggests that plots that used MSBs were 3.717 times more likely to be successful.

Discussion

Low Tech Financial Technologies

The findings of this study point to a relative degree of simplicity when it comes to terror finance, supporting the existing literature.[114] Terrorists go with what they know, using cash, the banking system, and MSBs to move money as well as cash and card to purchase goods and services. Moreover, cases which employ sophisticated financial mechanisms with multiple methods seem to be in the minority. This is particularly interesting given that research has often posited terrorists as early-adopters of technology particularly in the case of social media and messaging platforms.[115] These findings suggest that this may not be the case for the financing of plots.

When exploring why this is the case, one can draw from six attributes offered by Freeman & Ruehsen which help to dictate terror finance: Volume, risk, convenience, simplicity, costs, and speed.[116] In terms of volume, the terrorists in this sample had relatively low amounts of money to be moved and low costs for goods and services – the average amount of money moved was around $2,200, which is below the $3,000 threshold for which ID must be legally collected by MSBs – although many do collect at lower levels than this.[117] In short, for the amount of money in question, technologically simple methods such as cash, card, and MSBs are sufficient. When considering risk, the actors seemed to have little trouble sending, receiving, and purchasing without setting off too many red flags. There are cases like Mohamed Elshinawy, in which a $1,000 Western Union payment alerted the FBI to his plot,[118] but volume seems to have little to do with this. The US Treasury notes that of the approximately 3,600 Suspicious Activity Reports from 2015–17 that were related to terrorism, "were filed

Table 1. Binary logistic regression.

	Binary logistic regression – event success				95% CI for Exp(B)	
Behavior	B(SE)	*df*	Sig.	Exp(B)	Lower	Upper
MSB	1.313(.379)	1	.001	.269	.128	.566
Amount transferred	1.581(.318)	1	.000	.206	.110	.384
Constant	2.178(.401)	1	.000	8.832		

based on derogatory information regarding the sender or recipient, rather than based on suspicious activity associated with the transaction."[119]

Freeman & Ruehsen also highlight the importance of convenience, noting that using the banking system may not be suitable if one was trying to transfer cash to war-torn areas. This is an interesting point because a sizable number of movement transactions are sent to individuals in the caliphate. However, the typical route for this is to transfer funds to third parties via MSBs in surrounding countries. An example of this is Abdullahi Ahmed Abdullahi and his coconspirators, who sent money to Gaziantep, a Turkish town close to the Syrian border.[120] Presumably – although it is not explicitly stated – an individual then took this into the caliphate. In other words, MSBs and a degree of coordination are still convenient enough to move cash into war-torn areas. The next factor is simplicity; Freeman and & Nuehsen note that "terrorists would prefer methods that require the fewest number of steps, the lowest level of technology, and the least amount of skill."[121] As this research shows, not only do terrorists stick to simple technologies like MSBs, cash, and cards over more technical solutions such as cryptocurrencies, but regardless of the level of technology used, they also tend to utilize only one type rather than mixing a number of different methods.

Looking at costs is more difficult as the data do not reveal the amount of money that MSBs or banks charged actors to move money around. Freeman & Ruehsen note that MSBs like Western Union or MoneyGram can charge between 1 and 10% depending on the amount of money being transferred.[122] However, given the relatively small amounts of money at stake, these costs are likely to be negligible. Finally, when considering speed, there are relatively few barriers when using the popular methods of payments; cash can be transferred immediately, card payments are instantaneous, and MSBs can transfer money around the world within minutes – Western Union has a "Money in Minutes" service in which an individual can pick up cash immediately.[123] Zoobia Shahnaz again provides an example of taking advantage of quick transactions; on 30 May 2017, she withdrew $22,000 cash through 3 withdrawals and immediately sent $17,000 to third parties in Pakistan from an MSB in Queens, NY.[124]

When considering why terrorists in this sample did not adopt more sophisticated financial technologies, perhaps the adage of "if it ain't broke, don't fix it" is appropriate. As shown by the discussion of Freeman and Ruehsen's six factors, the low-tech means that were used were seemingly adequate to fulfill the needs of the terrorists in this sample. Moreover, multivariate analysis shows that one method of moving money – using MSBs – is predictive of the success of the overall plot, even when controlling for the amount of money sent. If, hypothetically, terrorists were purely rational thinkers, favoring MSBs over other ways of moving money, either locally, nationally, or globally, would be a justified decision.

The data presented in this study show that terrorists do, at times, opt for online technologies. This was highlighted in two important ways: Firstly, although they tend to move money using the traditional banking sector, the Internet is often used to coordinate these transactions. Keatinge & Keen warn that CTF has neglected the important role of social media platforms, which is important given platforms are not subject to the same regulation as the traditional financial sector.[125] Secondly, this research found that around half of all purchases were made online, utilizing platforms such as eBay, Amazon, as well as travel search engines for flight tickets. These findings

further strengthen the idea that terrorists opt for simplicity; the types of online platforms that are used represent some of the largest and most popular platforms on the Internet. There is little evidence in this sample – beyond a small number of outliers – to suggest that terrorists are using more sophisticated financial technologies than the public at large.

A Crypto-Based Future?

This study finds that terrorists are largely not using cryptocurrencies, which also conforms with the existing academic literature.[126] However, the concern over their use has continued to grow for understandable reasons. They offer the possibility to bypass the regulated financial sector and, if used with other technologies, they can be used with a high degree of anonymity. Furthermore, we know that terror organizations are attempting to solicit funds using them.[127] Moreover, the majority of cases in this sample were taken from the mid-2010s, which represents is a long time ago in the adoption and growth of cryptocurrencies. Given these factors, it is prudent to probe whether this is a technology that could be presently being exploited by terrorists, or if not, whether it is likely in future.

It is often noted that the reason that terrorists have not yet adopted cryptocurrencies and other sophisticated financial technologies because there are still relatively high barriers to entry.[128] Gartenstein-Ross, Clarke, & Shear provide an instructive four-step model for terrorist innovation which can be used as a lens with which to view this problem.[129] In the first step is the "Early Adoption" of a new technology in which groups and individuals tend to underperform. This is followed by "Iteration" in which the commercial technology undergoes consumer-focused improvements, which advances into a "Breakthrough" in which terrorists become more successful, before "Competition" in which stakeholders develop counter-measures and then both terrorists and stakeholders spin off into adaption and counter-adaption.

There are two ways to interpret this theoretical model onto these findings. The first is by looking specifically in the context of cryptocurrencies, which should be seen at the "Early Adoption" phase – there is little reason to suggest they are being used in a widespread way and groups seem to be underperforming at using them to fundraise. The literature suggests that this is because there are high barriers to entry to utilize it to its full potential.[130] Dion-Schwarz and colleagues argue that a key challenge for terrorists is that it is difficult to use and there are several potential pitfalls such as re-using public keys and the use of TOR with Bitcoin.[131] Importantly, they note that if a terrorist makes a small mistake, they may not know that they have not been successful at staying anonymous.[132] Brantly echoes this point, noting that although Bitcoin is relatively straightforward, maintaining anonymity requires substantial effort and technical skill, which poses a problem that a single unsophisticated use may reduce the anonymity of a whole network.

However, these barriers to entry could dissolve as cryptocurrencies become more mainstream. In a recent report, Eisermann suggests that terrorists *are* becoming more sophisticated at using this technology and that the situation is dynamic, and the potential risk is considerable.[133] Gartenstein-Ross, Koduvayur, and Hodgson find three

ways in which US white supremacists have used cryptocurrencies in recent years: donations to support digital content; paying for merchandise; and making general donations. They highlight several instances of individuals using the platform "DLive" to stream and solicit donations, including of the 6 Jan Capitol Riot.[134] It is worth noting that these individuals are not individuals that have conducted terror plots, but rather part of the wider extremist milieu. That being said, these contemporary cases do suggest that the barriers to entry may not be the same as they once were and we could be entering the "Breakthrough" phase.

The second way to interpret Gartenstein-Ross, Clarke, & Shear's framework is to take a step back and apply it to financial technologies more broadly. In this case, we could be seen as being in the final phase of "Competition" in which terrorists and stakeholders are engaged in adaption and counter-adaption. Scholars agree that counter-terror finance has improved substantially in the last two decades[135] and developments such as SARs and "Know Your Customer" protocols are examples of counter-adaption by government and other stakeholders. Importantly, Gartenstein-Ross, Clarke, & Shear note that the only certainty is continued innovation on the part of terrorists. Pressure from societal stakeholders can spur terrorist innovation. For example: Fisher, Prucha, & Winterbotham outline how pressure from social media companies caused jihadists to develop a complex, multiplatform ecosystem consisting of "Beacons" which direct users to material, platforms for storing content, and "Aggregators" which gather materials and provide a collection of links. It may also be useful to look at other crimes.[136] Outside of terrorism research, Horton-Eddison & Cristofaro find that the FBI's seizure of the Dark Web's Silk Road market spurred innovation and helped accelerate the adoption of innovative escrow solutions.[137] Keatinge & Danner note that there is a dearth of discussion of innovation on terror finance, but posit that groups and supporters are reactive to the hostile CTF environment in which they inhabit and necessity dictates how they adapt.[138] One reading of Gartenstein-Ross, Clarke, & Shear's model is that further improvements in CTF are likely to cause some kind of innovation by terrorists. If this happens then cryptocurrencies will be a prime candidate given the affordances they offer.

On the other hand, there are also reasons to believe that cryptocurrencies may not be the next innovation in terror finance. Beyond the points relating to the technical sophistication of users outlined above, there may be other reasons which block their emergence. Dion-Schwarz and colleagues offer six features of cryptocurrencies (anonymity, usability, security, acceptance, reliability, and volume) and five needs of terrorists (fundraising, gun and drug trafficking, remittance, attack funding, and operational funding).[139] Although they find that many of the features involved may aid terrorists, there are no cryptocurrencies that can address all these needs. Carroll & Windle make a similar point; although crypto has a number of uses, needs such as living expenses, wages, and pensions are not met, although they note that this could change if bitcoin becomes more mainstream.[140] Finally, Whyte notes the main shortcomings of cryptocurrencies. Firstly, control difficulties – organizations may lose control of individual actors to affect the control of assets. Secondly, the speculative nature of the technology; this relates to both the volatile value of currencies as well as possible regulation from governments.[141] Ultimately, there will always be a high degree of conjecture when

attempting to make predictions, but it is worth noting that there are reasons beyond terrorists' innovation which may stop cryptocurrencies becoming the financial method of choice in future.

Conclusion

This study sought to explore the role of financial technologies in contemporary cases of terrorism using a database of 231 IS actors in the US. The empirical findings are largely congruent with the existing literature on the topic of CTF; terrorists tend to opt for technological simplicity when moving money and making purchases. This may be related to the relatively small amounts of money that are involved in plots. There is little evidence of widespread exploitation of online payment technologies – either platforms such PayPal or digital assets such as cryptocurrencies. Instead, terrorists engage in cash transactions (including depositing and withdrawing money from the banking sector) or use MSBs.

Despite most transactions taking place offline, this research does suggest that the Internet plays an important role in two ways. Firstly, almost half of all purchases that were deemed to be relevant to terrorists' plots took place online. This includes flights to the caliphate, weaponry, and bomb-making materials and was done on platforms such as Amazon and eBay. Secondly, actors used the Internet to communicate and facilitate offline transactions using mainstream social media platforms, messaging services, and email. This helps highlight the growing literature which suggests that the online/offline dichotomy may be a difficult one to draw in many cases; terrorist actors' behavior is often intertwined between the two domains.

This study also found that one method of moving money – utilizing MSBs – significantly predicted the success of plots, even when controlling for how much money is moved. These results should be taken tentatively, particularly as the sample of some technologies (cryptocurrencies in particular) is small and therefore it is difficult to draw firm conclusions. This, too, is congruous with existing literature which suggests that MSBs may be vulnerable to exploitation from terrorists and are an easier way of moving money than the banking sector.

Moreover, cryptocurrencies were not regularly exploited by terrorists in this sample. However, it is prudent to consider why this is the case and whether this trend will continue in future. One way of interpreting this is that that law enforcement crackdowns has spurred technological innovation in the future and as CTF controls become stricter, and barriers to entry to cryptocurrencies become smaller, that one may expect their usage to increase in future. However, this technology is not, at present, a panacea for terrorists. They have many needs that cannot currently be met by cryptocurrencies and the next step in innovation may lay somewhere else.

Notes

1. Lorenzo Vidino, Jon Lewis, and Andrew Mines, "Dollars for Daesh Analyzing the Finances of American," *Program on Extremism*, September 2020.
2. *The 9/11 Commission Report*, 2004.

3. Iwa Salami, "Terrorism Financing with Virtual Currencies: Can Regulatory Technology Solutions Combat This?" *Studies Conflict and Terrorism* 41, no. 12 (2018): 968–89, https://doi.org/10.1080/1057610X.2017.1365464.
4. Emilie Oftedal, "The Financing of Jihadi Terrorist Cells in Europe," *Forsvarets Forskningsinstitutt*, 2015, https://www.ffi.no/no/Rapporter/14-02234.pdf.
5. Alexander Meleagrou-Hitchens, *Incitement: Anwar Al-Awlaki's Western Jihad* (Cambridge, MA: Harvard University Press, 2020).
6. Bürke Uğur Basaranel, "Online Terrorist Financing," in *Terrorists' Use of the Internet: Assessment and Response*, ed. Maura Conway and others (Amsterdam: IOS Press, 2017), cxxxvi, 95–108, https://doi.org/10.3233/978-1-61499-765-8-95.
7. Aaron Brantly, "Financing Terror Bit by Bit," *CTC Sentinel* 7, no. 10 (2014): 1–4; Christopher Whyte, "Cryptoterrorism: Assessing the Utility of Blockchain Technologies for Terrorist Enterprise," *Studies in Conflict & Terrorism* (2019): 1–24, https://doi.org/10.1080/1057610X.2018.1531565; Cynthia Dion-Schwarz, David Manheim, and Patrick B Johnston, *Terrorist Use of Cryptocurrencies* (Santa Monica, CA: RAND Corperation, 2019); Daniel Eisermann, "Cryptocurrencies as Threats to Public Security and Counter Terrorism: Risk Analysis and Regulatory Challenges," *Counter Extremism Project*, April, 2020.
8. Tom Keatinge and Florence Keen, "Social Media and (Counter) Terrorist Finance: A Fund-Raising and Disruption Tool," *Studies in Conflict and Terrorism* 42, no. 1–2 (2019): 178–205, https://doi.org/10.1080/1057610X.2018.1513698; The Camstoll Group, "Use of Social Media By Terrorist Fundraisers and Financiers," April 2016.
9. U.S. Department of Treasury, *National Terrorist Financing Risk Assessment*, 2018.
10. Magnus Ranstorp, "Microfinancing the Caliphate: How the Islamic State Is Unlocking the Assets of European Recruits," *CTC Sentinel* 9, no. 5 (2016): 11–5.
11. Lorenzo Vidino, Jon Lewis, and Andrew Mines, "Dollars for Daesh Analyzing the Finances of American," *Program on Extremism*, September 2020; Tom Keatinge and Florence Keen, "Lone-Actor and Small Cell Terrorist Attacks. A New Front in Counter-Terrorist Finance?, *Royal United Services Institute for Defence and Security Studies*, 2017; Kacper Rekawek and others, *Who Are the European Jihadis?*, *Globsec: Defence & Security Programme*, 2018.
12. Tom Keatinge and Kerstin Danner, "Assessing Innovation in Terrorist Financing," *Studies in Conflict & Terrorism*, 2019, https://doi.org/10.1080/1057610X.2018.1559516.
13. For example, see: Oftedal; Vidino, Lewis, and Mines.
14. Michael Freeman and Moyara Ruehsen, "Terrorism Financing Methods: An Overview," *Perspectives on Terrorism* 7, no. 4 (2013): 5–26, http://www.terrorismanalysts.com/pt/index.php/pot/article/view/279/562.F
15. Defined by the US Department of Treasury as: "any person doing business, whether or not on a regular basis or as an organized business concern, in one or more of the following capacities: (1) Currency dealer or exchanger; (2) Check casher; (3) Issuer of traveler's checks, money orders or stored value; (4) Seller or redeemer of traveler's checks, money orders or stored value; (5) Money transmitter; and (6) U.S. Postal Service".
16. U.S. Department of Treasury.
17. U.S. Department of Treasury
18. UN Security Council, "Joint Report of the Counter-Terrorism Committee Executive Directorate and the Analytical Support and Sanctions Monitoring Team Pursuant to Resolutions 1526 (2004) and 2253 (2015) Concerning Islamic State in Iraq and the Levant (ISIL) (Da'esh), Al-Qaida An," June 2020, https://doi.org/10.1017/S0020818300002435.
19. Financial Action Task Force, "Emerging Terrorist Financing Risks," *Emerging Terrorist Financing Risks FATF Report*, October 2015, 47, http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf.
20. Lorenzo Vidino, Jon Lewis, and Andrew Mines, "Dollars for Daesh Analyzing the Finances of American," *Program on Extremism*, September 2020.
21. N.S. Jamwal, "Hawala-the Invisible Financing System of Terrorism," *Strategic Analysis* 26, no. 2 (2002): 181–98.
22. Salami, p. 971.

23. Freeman and Ruehsen.
24. For example, see: Keatinge and Danner; Nikita Malik, "Terror in the Dark: How Terrorists Use Encryption, The Darknet, and Cryptocurrencies," *Henry Jackson Society*, 2018; Whyte.
25. Financial Action Task Force, *Terrorist Financing Risk Assessment Guidance*, 2019, www.fatf-gafi.org.
26. Europol, *Terrorism Situation and Trend Report*, 2020.
27. Fabian M. J. Teichmann, "Financing Terrorism Through Hawala Banking in Switzerland," *Journal of Financial Crime* 25, no. 2 (2018): 287–93.
28. Fabian M. J. Teichmann and Marie-Christin Falker, Money laundering via underground currency exchange networks, *Journal of Financial Regulation and Compliance*, 2020.
29. UN Security Council.
30. Oftedal.
31. Europol, *Terrorism Situation and Trend Report*; Financial Action Task Force, *Terrorist Financing Risk Assessment Guidance*.
32. Michael Jacobson, "Terrorist Financing and the Internet," *Studies in Conflict and Terrorism* 33, no. 4 (2010): 353–63, https://doi.org/10.1080/10576101003587184.
33. Basaranel, cxxxvi.
34. U.S. Department of Treasury.
35. UN Security Council.
36. Oftedal.
37. U.S. Department of Treasury; Keatinge and Danner.
38. Keatinge and Keen, "Social Media and (Counter) Terrorist Finance: A Fund-Raising and Disruption Tool."
39. The Camstoll Group.
40. Malik; Salami.
41. Keatinge and Danner.
42. Maura Conway, "Violent Extremism and Terrorism Online in 2018: The Year in Review," *Vox Pol*, 2018; Malik.
43. Keatinge and Danner.
44. Dion-Schwarz, Manheim, and Johnston.
45. Eisermann.
46. For example, see: Vidino, Lewis, Mines; Keatinge and Keen; Eisermann; Dion-Schwarz, Manheim, and Johnston; Salami.
47. Salami.
48. U.S. Department of Treasury.
49. Paul Gill and others, "Terrorist Use of the Internet by the Numbers: Quantifying Behaviors, Patterns, and Processes," *Criminology and Public Policy* 16, no. 1 (2017): 99–117, https://doi.org/10.1111/1745-9133.12249; Jytte Klausen, "Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq," *Studies in Conflict & Terrorism* 38, no. 1 (2015): 1–22, https://doi.org/10.1080/1057610X.2014.974948.
50. Joe Whittaker, "The Online Behaviors of Islamic State Terrorists in the United States," *Criminology & Public Policy* 20, 177–203; Michael Jensen and others, "The Use of Social Media by United States Extremists," *National Consortium for the Study of Terrorism and Responses to Terrorism*, 2018, http://www.start.umd.edu/data-
51. U.S. Department of Treasury.
52. Keatinge and Keen, "Lone-Actor and Small Cell Terrorist Attacks. A New Front in Counter-Terrorist Finance?"
53. U.S. Department of Treasury.
54. Whittaker.
55. At the time of the end of data collection in May 2020.
56. Program on Extremism, "ISIS in America: The Cases." George Washington University," https://extremism.gwu.edu/cases
57. Alexander Meleagrou-Hitchens, Seamus Hughes, and Bennett Clifford, "The Travelers: American Jihadists in Syria and Iraq," *Program on Extremism, George Washington University*,

2018; Seamus Hughes, Emily Blackburn, and Andrew Mines, "The Other Travelers: American Jihadists Beyond Syria and Iraq," *Program on Extremism*, 2019.

58. START, "Global Terrorism Database," https://www.start.umd.edu/gtd/
59. For example, see: Audrey Alexander, "Cruel Intentions: Female Jihadists in America," *Program on Extremism*, 2016; Bennett Clifford and Seamus Hughes, "United States vs. Aws Mohammed Younis Al-Jayab: A Case Study on Transnational Prosecutions of Jihadi Foreign Fighter Networks," *CTC Sentinel*, December 2018, 26–30; Jytte Klausen, "A Behavioral Study of the Radicalization Trajectories of American "Homegrown" Al Qaeda-Inspired Terrorist Offenders," 2016; Jytte Klausen and others, "Towards a Behavioral Model of "Homegrown" Radicalization Trajectories," *Studies in Conflict & Terrorism* 39, no. 1 (2016): 67–83, https://doi.org/10.1080/1057610X.2015.1099995; Jytte Klausen, *The Role of Social Networks in the Evolution of Al Qaeda-Inspired Violent Extremism in the United States, 1990-2015*, 2016.
60. Paul Gill, "The Data Collection Challenge: Experiences Studying Lone-Actor Terrorism," *Resolve Network: Researching Violent Extremism Series*, February 2020.
61. START, "Profiles of Individual Radicalization in the United States (PIRUS) Codebook," 2018, www.start.umd.edu.
62. Vidino, Lewis, and Mines, "Dollars for Daesh Analyzing the Finances of American."
63. USA v. Mohamed Amiin Ali Roble, Criminal Complaint, Case 0:16-mj-00584, United States District Court for the District of Minnesota, 2016.
64. Klaus Krippendorff, *Content Analysis: An introduction to its Methodology* (Thousand Oaks, CA: Sage, 2004).
65. Paul Gill, "Online Behaviours of Convicted Terrorists," *Vox Pol*, 2016.
66. Whittaker.
67. The sample includes only three actors under the age of 18 because they were tried as adults. The standard procedure for minors is to seal the document and leave the actor unnamed. Minors that successfully traveled to the Iraq or Syria were not included. This means that the distribution and average age is probably somewhat lower than presented above
68. Rachel Bryson, *For Caliph and Country* (London, 2017).
69. 6 I follow the lead of the George Washington University's Program on Extremism, who record life sentences (in this sample n = 6) as 470 months, as per United States Sentencing Commission practice. Glenn R. Schmitt & Hyun J. Konfrst, Life Sentences in the Federal System. United States Sentencing Commission, 2015.
70. Keatinge and Keen, "Lone-Actor and Small Cell Terrorist Attacks. A New Front in Counter-Terrorist Finance?"; U.S. Department of Treasury; Financial Action Task Force, *Terrorist Financing Risk Assessment Guidance*.
71. Rekawek and others; Keatinge and Keen, "Lone-Actor and Small Cell Terrorist Attacks. A New Front in Counter-Terrorist Finance?"; Vidino, Lewis, and Mines, "Dollars for Daesh: The Small Financial Footprint of the Islamic State's American Supporters."
72. U.S. Department of Treasury.
73. John Horgan and others, "Actions Speak Louder than Words: A Behavioral Analysis of 183 Individuals Convicted for Terrorist Offenses in the United States from 1995 to 2012," *Journal of Forensic Sciences* 61, no. 5 (2016): 1228–37, https://doi.org/10.1111/1556-4029.13115.
74. Karen J. Greenberg and Seth Weiner, "The American Exception: Terrorism Prosecution In the United States – The ISIS Cases – March 2014 – August 2017," *Center on National Security At Fordham Law*, 2017.
75. Human Rights Watch, *Illusion of Justice: Human Rights Abuses in US Terrorism Prosecutions*, 2014, http://www.hrw.org/node/126101. Huma
76. U.S. Department of Treasury; UN Security Council; Financial Action Task Force, *Terrorist Financing Risk Assessment Guidance*.
77. Vidino, Lewis, and Mines, "Dollars for Daesh: The Small Financial Footprint of the Islamic State's American Supporters"; Oftedal; U.S. Department of Treasury.
78. Paul Carroll and James Windle, "Cyber as an Enabler of Terrorism Financing, Now and in the Future," *Journal of Policing, Intelligence and Counter Terrorism* 13, no. 3 (2018): 285–300, https://doi.org/10.1080/18335330.2018.1506149; Keatinge and Danner; Salami.

79. For example, see: USA v. Ramiz Hodzic et al. Government's Response in Opposition to Defendant's Motion to Dismiss, Case: 4:15-cr-00049-CDP-DDN, United States District Court for the Eastern District of Missouri, Eastern Division, 2015; USA v. Abdullahi Ahmed Abdullahi, Indictment, Case 3:17-cr-00622-W, United States District Court for the Southern District of California, 2017.
80. U.S. Department of Treasury.
81. For an in-depth case study, see: Seamus Hughes, "The Only Islamic State-Funded Plot in the U.S.: The Curious Case of Mohamed Elshinawy," *Lawfare Blog,* March 7, 2018, https://www.lawfareblog.com/only-islamic-state-funded-plot-us-curious-case-mohamed-elshinawy.
82. USA v. Ramiz Hodzic et al.
83. Eisermann; Vidino, Lewis, and Mines, "Dollars for Daesh: The Small Financial Footprint of the Islamic State's American Supporters"; Malik.
84. USA v. Zoobia Shahnaz, Indictment, Case: 2:17-cr-00690, United States District Court for the Eastern District of New York, 2017.
85. USA v. Zoobia Shahnaz.
86. USA v. Lionel Nelson Williams, Statement of Facts, Case 2:17-cr-00001-AWA-LRL, United States District Court for the Eastern District of Virginia, 2017.
87. USA v. Zoobia Shahnaz.
88. USA v. Mohamed Elshinawy, Plea Agreement, Case 1:16-cr-00009-ELH, United States District Court for the District of Maryland, 2017.
89. USA v. Abdulrahman El Bahnasawy, Criminal Complaint, Case: 1:16-cr-00376, United States District Court for the Southern District of New York, 2016.
90. USA v. Russel Salic, Criminal Complaint, [No Case Number], United States District Court for the Southern District of New York, 2016.
91. USA v. Abdullahi Ahmed Abdullahi.
92. USA v. Ramiz Hodzic.
93. Sean C. Reynolds and Mohammed M. Hafez, "Social Network Analysis of German Foreign Fighters in Syria and Iraq," *Terrorism and Political Violence*, April 2017, https://doi.org/10.1080/09546553.2016.1272456; Gill and others.
94. USA v. Mohamed Rafik Naji, Criminal Complaint, Case 1:16-cr-00653, United States District Court for the Eastern District of New York, 2016.
95. USA v. Abdullahi Ahmed Abdullahi; USA v. Ramiz Hodzic.
96. Financial Action Task Force, *Terrorist Financing Risk Assessment Guidance*; Financial Action Task Force, "The Role of Hawala and Other Similar Service Providers in Money Laundering and Terrorist Financing," 2013, http://www.fatf-gafi.org/media/fatf/documents/reports/Role-of-hawala-and-similar-in-ml-tf.pdf; Malik; Normark and Ranstorp; UN Security Council.
97. USA v. Ahmed Khan Rahimi, Government's Sentencing Memorandum, Case 1:16-cr-00760-RMB, United States District Court, District of New Jersey, 2018.
98. USA v. David Wright and Nicholas Rovinski, Affidavit, Case 1:15-cr-10153-WGY, United States District Court District of Massachusetts, 2015.
99. USA v. Mufid A. Elfgeeh, Affidavit, Case: 6:15-cr-06052, Unites States District Court for the Western District of New York, 2016.
100. USA Federal Reserve, "The 2019 Federal Reserve Payments Study," 2020, https://www.federalreserve.gov/paymentsystems/2019-December-The-Federal-Reserve-Payments-Study.htm.
101. USA v. Shivam Patel, Government's Sentencing Memorandum, Case 2:17-cr-00120-MSD-DEM, United States District Court for the Eastern District of Virginia, 2018; USA v. Gregory Hubbard, Dayne Antani Christian, and Darren Arness Jackson, Criminal Complaint, Case 9:16-cr-80107, United Staes District Court for the Southern District of Florida, 2016; USA v. Abdullahi Yusuf and Abdi Nur, Criminal Complaint, Case: 14-MJ-0124, United States District Court for the District of Minnesota, 2014.
102. USA v. Noor Salman, Government's Motion for an Order Revoking Defendant's Release, Case 6:17-cr-00018-PGB-KRS, United States District Court for the Middle District of Florida, 2017.

103. USA v. Yousef Mohammad Ramadan, Criminal Complaint, Case 2:17-cr-20595-MOB-EAS, United States District Court for the Eastern District of Michigan, 2017.
104. USA v. Ikaika Erik Kang, Affidavit in Support of Criminal Complaint, Case 1:17-mj-00767-KJM, United States District Court for the District of Hawaii, 2017.
105. Andrew Perrin, More Americans are Making No Weekly Purchases with Cash, *Pew Research*, December 12, 2018, https://www.pewresearch.org/fact-tank/2018/12/12/more-americans-are-making-no-weekly-purchases-with-cash/
106. USA v. Mohamed Abdihamid Farah et al, Criminal Complaint, Case 0:15-cr-00049, United States District Court for the District of Minnesota, 2015
107. USA v. Fabjan Alameti, Government's Sentencing Memorandum, Case 2:19-cr-00013-DLC, United States District Court for the District of Montana, 2019.
108. U.S. Department of Treasury; Financial Action Task Force, *Terrorist Financing Risk Assessment Guidance*; UN Security Council.
109. U.S. Department of Treasury.
110. Keatinge and Keen, "Lone-Actor and Small Cell Terrorist Attacks. A New Front in Counter-Terrorist Finance?"
111. Priya Ranganatham, C.S. Pramesh, & Rakesh Aggarwal, Common Pitfalls in Statistical Analysis: Logistic regression, *Perspectives in Clinical Research,* 8. 2017.
112. U.S. Department of Treasury.
113. U.S. Department of Treasury.
114. Vidino, Lewis, and Mines, "Dollars for Daesh: The Small Financial Footprint of the Islamic State's American Supporters"; U.S. Department of Treasury; Financial Action Task Force, "Emerging Terrorist Financing Risks."
115. UN CTED, *Analysis and Recommendations with Regard to the Global Threat from Foreign Fighters*, 2015; B. Levin, "The Original Web of Hate: Revolution Muslim and American Homegrown Extremists," *American Behavioral Scientist* 59, no. 12 (2015): 1609–30, https://doi.org/10.1177/0002764215588815; Mia Bloom, Hicham Tiflati, and John Horgan, "Navigating ISIS's Preferred Platform: Telegram," *Terrorism and Political Violence*, 2017, 1–13, https://doi.org/10.1080/09546553.2017.1339695.
116. Freeman & Ruehsen.
117. U.S. Department of Treasury.
118. Hughes "The Only Islamic State-Funded Plot in the U.S.: The Curious Case of Mohamed Elshinawy."
119. U.S. Department of Treasury, p. 16.
120. USA v. Abdullahi Ahmed Abdullahi
121. Freeman and Ruehsen, p. 7.
122. Freeman & Ruehsen.
123. Western Union, "When Will My Receiver Get the Money?," https://wucare.westernunion.com/s/article/When-can-the-receiver-pick-up-the-money-I-sent?language=en_US#:~:text=Direct%20to%20Bank%20deposit%20typically,%E2%80%93%20generally%20delivered%20within%20minutes*.
124. USA v. Zoobia Shahnaz.
125. Tom Keatinge and Florence Keen, "Social Media and Terrorist Financing What Are the Vulnerabilities and How Could Public and Private Sectors Collaborate Better ?," *Global Research Network on Terrorism and Technology* 10 (2019).
126. Keatinge and Danner; Malik; Dion-Schwarz, Manheim, and Johnston; U.S. Department of Treasury.
127. Eisermann; Europol, "Terrorism Situation and Trend Report (TE-SAT)," 2019, https://doi.org/10.2813/788404; Conway.
128. Dion-Schwarz, Manheim, and Johnston; Brantly; UN Security Council.
129. Daveed Gartenstein-Ross, Colin P. Clarke, & Matt Shear, Terrorists and Technological Innovation, *Lawfare Blog*, February 2, 2020, https://www.lawfareblog.com/terrorists-and-technological-innovation
130. Dion-Schwarz, Manheim, and Johnston.

131. Dion-Schwarz, Manheim, and Johnston.
132. Brantly.
133. Eisermann.
134. Daveed Gartenstein-Ross, Varsha Koduvayur, and Samuel Hodgson, Crypto-Fascists: Cryptocurrency Usage by Domestic Extremists, *Valens Global,* 2022 https://www.fdd.org/analysis/2022/03/15/crypto-fascists/.
135. Salami; Oftedal.
136. Ali Fisher, Nico Prucha & Emily Winterbotham, "Mapping the Jihadist Information Ecosystem: Towards the Next Generation of Disruption Capability," *Global Research Network on Terrorism and Technology* no. 6 (2019).
137. Martin Horton-Eddison & Matteo di Cristofaro, "Hard Interventions and Innovation in Crypto-Drug Markets: The escrow example," *Global Drug Policy Observatory*, 2017.
138. Keatinge & Danner.
139. Dion-Schwarz, Manheim, and Johnstonl.
140. Carroll & Windle.
141. Whyte.

Acknowledgements

I would like to thank Joe Rees for his hard work in coding this data for inter-coder reliability. I would also like to thank Dr. Daveed Gartenstein-Ross for his helpful feedback in preparing this article. I am also grateful for feedback received from the Swansea University's Cyber Threats Research Centre (CYTREC) research seminar on 18 November 2020.

Disclosure Statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by the Swansea University's Paid Internship Network (SPIN).

ORCID

Joe Whittaker http://orcid.org/0000-0001-7342-6369