CORA Cork Open Research Archive
Cartlann Taighde Oscailte Chorcaí

Title	Cyber as an enabler of terrorism financing, now and in the future
Authors	Carroll, Paul;Windle, James
Publication date	2018-08-20
Original Citation	Carroll, P. and Windle, J. (2018) 'Cyber as an enabler of terrorism financing, now and in the future', Journal of Policing, Intelligence and Counter Terrorism, 13(3), pp. 285-300. doi: 10.1080/18335330.2018.1506149
Type of publication	Article (peer-reviewed)
Link to publisher's version	http://www.tandfonline.com/10.1080/18335330.2018.1506149 - 10.1080/18335330.2018.1506149
Rights	© 2018 Department of Security Studies and Criminology. This is a pre-print of an article published by Taylor & Francis in Journal of Policing, Intelligence and Counter Terrorism, on 20 August 2018, available online: http://www.tandfonline.com/10.1080/18335330.2018.1506149
Download date	2026-10-18 00:56:36
Item downloaded from	https://hdl.handle.net/10468/7649

UCC
University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

Carroll, P., & Windle, J. (2018). Cyber as an enabler of terrorism financing, now and in the future. *Journal of Policing, Intelligence and Counter Terrorism*, *13*(3), 285-300. Pre-print

Cyber as an enabler of terrorism financing, now and in the future

Paul Carroll and James Windle

The final version of the paper as published in the print edition can be found at: https://www.tandfonline.com/doi/abs/10.1080/18335330.2018.1506149

Abstract

The objective of this paper is to conduct a critical analysis of whether there is, or could be an incremental use of cyber in the raising and transfer of terrorism finance, compared against traditional terrorism finance practices already in place. Data was collected through semi-structured interviews with subject matter experts. They were initially dismissive of any significant use of cyber within terrorism finance, whilst acknowledging that the lack of quality data means that there may be more terrorism finance activity within the cyber domain than is empirically known. Some participants offered examples of how cyber might be utilised by providing impromptu 'what if' scenarios. We suggest that this may be symbolic of how primitive the thought process around the current and future use of cyber in terrorism finance is. It was also acknowledged that the current gap in empirical data might be addressed through bespoke training of both security services personnel and wider organisations in identifying terrorism finance 'red flag' indicators.

Keywords: Terrorist financing; cyber; cryptocurrency; Dark Web; ISIL

Introduction

While Gabriel Weimann (2004) identified fund raising as one of eight ways in which terrorists could use the internet, our understanding of the extent of cyber use by terrorist financers is underdeveloped. As cyber-related criminality is growing, and terrorists have historically

borrowed fundraising techniques from criminals (Windle et al., 2018), it is an issue warranting greater attention within terrorism studies. The key objective of this research is to establish if there is an appetite by Islamist terrorist organisations to utilise cyber, and more specifically cryptocurrencies, to raise and transfer finance, now and in the future.

To do this we interviewed four subject matter experts. They were initially dismissive of any significant use of cyber within terrorism finance,[1] whilst acknowledging that the lack of quality data means that there may be more terrorism finance activity within the cyber domain than is empirically known. Some participants offered examples of how cyber might be utilised by providing impromptu 'what if' scenarios. We suggest that this may be symbolic of how primitive the thought process around the current and future use of cyber in terrorism finance is.

As cyber involves a shift, in part or full, from traditional terrorist financing sources, the next section provides a foundation for analysis by briefly reviewing the traditional sources that cyber may replace. The relatively scant cyber-terrorist financing literature is then reviewed, followed by our methodology and the interview results.

[1] Terrorism finance refers to any finance raised for the purpose of terrorism, whether it be for the direct funding of a terrorist attack or to finance the day to day operational functions and materials of the organisation and its members. This definition centres upon how we define terrorism, here defined as 'the use of violence or the threat of violence with the primary purpose of generating a psychological impact beyond the immediate victims or object of attack for a political motive'. This definition sets specific parameters, while including state and non-state actors (Richards, 2014:24; see Wittig, 2011).

Literature review: Weighing the benefits of traditional against cyber terrorist financing

While most terrorist attacks are relatively cheap - as reflected in the recent attacks carried out in Manchester, New York and London - running a terrorist organisation can be costly; especially if groups engage in prolonged campaigns or assume state functions in areas under their authority (Windle, forthcoming/2018; see Silke, 1998). For example, leaked documents suggest that, in 2014, the Islamic State of Iraq and the Levant (ISIL) required around US$5 million per month to operate (Cooper, 2017).

Terrorists have traditionally raised revenue from five main sources: Legitimate investments, state sponsorship, donations/extortion, charities and crime (Windle, forthcoming/2018). While some cells or individuals may concentrate on just one or two sources, larger organisations will often diversify. For example, Irish Loyalist paramilitaries raised finance through donations, extortion, robbery, smuggling, counterfeiting and a range of legitimate businesses, including drinking clubs which defrauded the exchequer. The drug trade became a core source of revenue for some; partially as a response to more stringent regulation of drinking clubs, which had been a primary source of income (Windle, forthcoming/2018; Hourigan et al., 2018; Silke, 2000).

While some argue that terrorists are increasingly involved in criminality (Makarenko, 2004), the 'most resilient and well-organized' terrorist groups invest in legitimate business (Passas, 2007) and collect charitable donations (Rudner, 2010). Both of which can be low risk, non-suspicious and difficult to trace (see Napoleoni, 2007; Raphaeli, 2003; Rudner, 2010). Hezbollah, for example, claim that the majority of their income comes from their own investment portfolio (Levitt, 2007); a significant amount also comes from a transnational

network of charities tasked with collecting donations. That a portion of these donations are channelled back into society makes it difficult to differentiate between funds being spent on terrorism or social goods; especially if the money does not pass through financial institutions and regulatory frameworks (Rudner, 2010).

The type of funding source used is context dependent, influencing factors can include: opportunities, group size, member's skills/expertise, law enforcement priorities, competition, start-up costs, ideological and political considerations, and geography (see Asal et al., 2015; Picarelli & Shelley, 2007; Windle, 2018/forthcoming). The choice of both legitimate and less legitimate enterprise will, for example, depend upon the start-up capital and skills available to the group. Primarily working class Irish paramilitaries ran traditional working class enterprises such as pubs, building firms and taxi hire companies (Silke, 2000; Windle, forthcoming/2018; see also Comras, 2007). Some smaller terrorist cells have raised money through small-scale welfare frauds or retail drug dealing, while others engaged in larger-scale drug trafficking.

Opportunities can be presented by geography, existing markets and, member's skills and position in social networks. The PKKs involvement in heroin distribution, for example, resulted from Turkey's geographical position on a traditional smuggling route linking South Asian opium fields to Europe, coupled with logistical support provided by large numbers of members and sympathisers living across Europe (Roth & Sever, 2007). Irish paramilitaries involvement in fuel laundering and tobacco smuggling resulted from opportunities presented by tax differentials between Northern and Southern Ireland (Hourigan et al. 2018), while ISIL has been able to exploit oil fields and antiquities in areas under their control (Johnston, 2014).

Some organisations, such as Al-Qaeda and Hezbollah, enjoy international reach. While others, such as ISIL utilise locally sourced finances from the territories they occupy (Cooper, 2017). That ISIL have been able to sustain this finance locally, and without extensive involvement in international financial systems, will be important to note throughout this study: If access to local funds 'dry up' and finance needed to be raised further afield, then ISIL may adapt towards cyber, in a similar way that Loyalist paramilitaries adapted from drinking clubs to the illicit drug trade. And terrorists are very good at adapting; whether to new opportunities or in response to law enforcement or preventive interventions. As such, effective policies must acknowledge and plan for potential future threats.

A final consideration, that may limit the utility of cyber, is that any one enterprise can have multiple objectives beyond the financial. Any one enterprise may try to accumulate multiple sources of capital - financial but also political, social and religious or cultural – and serve strategic purposes (Windle, forthcoming/2018; see Felbab-Brown, 2010). For example, firms providing income (no matter how legitimate) in high unemployment areas can strengthen a group's political and social capital; extortion signals a group's authority over a community, while using a portion of the extorted revenue for social goods is symbolic of the group's ability to undertake state functions; and legitimate enterprises can offer fronts for the smuggling of goods or people.

Cyber: Raising money

Cyber has provided a 'virtual bridge' across borders, allowing criminality to be conducted on a larger scale, at greater pace and with potential for greater return. Consequently, the extent of cyber victimisation and, online contraband sales are significant and growing. Cyber has been used for: credit card fraud (Kim et al., 2011), drug trafficking/dealing (Barratt et al., 2014) and

cultivation (Windle, 2017), extortion (Hampton & Baig, 2015), unlawful purchase of arms and ammunition (Paoli et al., 2017), identity theft (Finch, 2003), money laundering (Filipkowski, 2008) and, online grooming and control of vulnerable peoples for exploitation in criminal activity (Storrod & Densley, 2017). Ross Anderson and colleagues (2013), however, reject categorising cybercrime as a new crime type, instead suggesting it be used to describe traditional crimes now carried out online (also Wall, 2005).[2] Indeed, the offline version of each of the offences mentioned earlier in this paragraph have been used by terrorists for operational or financial purposes.

Dovetailing illicit enterprise, there is some evidence of terrorists creating or exploiting legitimate internet companies or charities in much the same way they would in the offline world. For example, paralleling usage by non-violent political and civil organisations, there is 'huge potential for increased financial donations' by inviting visitors to terrorist websites to donate money or buy goods through their online stores (Conway, 2006:285; also Weimann, 2004). While the move from offline to online could attract a wider pool of potential donors it remains dependent on geography. For example, it is relatively simple to collect and move charitable donations in Mosul. Whereas, the terrorist sympathiser living in London may be unwilling to attend a function where money is collected yet feel more confident donating from the anonymity of their home computer. This said, many 'donations' are essentially a version of extortion and cyber may dilute the potential social and/or physical threat of refusing

[2] We should differentiate here between 'cyber-enabled' crime (i.e. a crime that might also be carried out independently of a cyber-element, but is enhanced by it) and 'cyber-dependent crime' (i.e. a crime that is impossible to carry out without a cyber related infrastructure, such as large-scale malware attacks).

'donation' demands. The point, however, is that many traditional methods can be enabled and enhanced through the use of cyber, context dependent.

A benefit to cyber is that dual objectives of raising finances and disrupting national economic infrastructure can be achieved in one operation. The 'SWIFT attack' on the Bangladesh Central Bank, for example, offers insight into not only the potential for cyber-crime to raise funds and attack economic infrastructures, but also human elements of cybercrime. In 2016, hackers utilised malware to steal US$101 million from the Bangladesh Central Bank (Mallet & Chilkoti, 2016). The Banks lack of simple cybersecurity measures was an influencing factor in the hacker(s) successful access to the bank's system: The 'bank lacked a firewall and used second-hand, $10 electronic switches to network those computers' (Finkle, 2016). The 'SWIFT attack' demonstrates the potential scale, speed and global reach of a single cyber-attack upon an organisation that might appeal to terrorists. The initial investment and skillset coupled with the potential risk of being identified may not, however, represent a worthwhile investment. Especially when there are well-grounded fundraising tools already in place.

Cryptocurrencies: Moving money

A key element of cybercrime is the use of cryptocurrencies, such as Bitcoin, to buy and sell contraband and services on the Dark Web. Michael Jacobson (2010) and Gabriel Weimann (2016) suggest that the Dark Web would appeal to terrorists, given the geographical scope, speed and degree of anonymity that it provides. The Dark Web is not, however, risk free. Cryptocurrencies provide increased, rather than complete, anonymity as they are added to blockchains which can be used to trace the originating electronic wallet from which the cryptocurrency was sent. Even with more sophisticated techniques of hiding transactions the

money is, according to Meiklejohn, 'going to be [in the blockchain] forever, so you're giving law enforcement a lot of time to figure it out' (cited in Dunietz, 2017).

While investigating cryptocurrencies can be difficult, security agencies have used them to build a picture of cryptocurrency users' behaviour and routine financial activity. Cryptocurrencies are, however, in their infancy and could become more secure and even harder to trace,[3] further reducing the risk to terrorist financers. At present, however, maintaining anonymity requires time and skill, and mistakes by 'novice users' can compromise all those involved in that chain of transactions; which could potentially expose the locality of a terrorist network (Brantly, 2014; Dunietz, 2017). This may be a key reason why the use of cryptocurrencies by terrorist organisations has not been in sync with their incremental use by organised crime groups (Brantly, 2014); and even organised criminals' uptake of cryptocurrencies have been slow (Carlisle, 2017).

Cryptocurrency profits will often never leave the Dark Web: they will be used to buy goods and services rather than converted to fiat currency. While Weimann (2016) suggests that the Dark Web could be a 'treasure trove' for terrorists, Zachery Goldman and colleagues (2016) highlight that terrorists often need fiat currency to be spent locally or moved to cells planning attacks in distant locations. As such, many terrorists rely on local cash based funding sources: cash being a much more useful commodity and far more difficult to trace than an electronic transfer (also Wittig, 2011). While a terrorist may find cryptocurrencies useful for buying fake documents or weapons, much of a terrorist organisations expenditure goes on expenses which

[3] For example, 'dark wallets' are being designed which camouflage illicit transactions within licit transactions (Brantly, 2014:4).

require fiat currency - such as living expenses, wages and pensions - and the process of converting into fiat currency might prove an unnecessary identifying risk (Goldman et al., 2016). This said, as cryptocurrencies become more understood and trusted, more retailers may accept them as currency.[4] These circumstances could increase the usefulness of cryptocurrencies for terrorists, while reducing the risk of their financial activity and location being tracked. This sits well with the Routine Activity Approach (Cohen & Felson, 1979): As technology makes it easier to use and access cryptocurrencies and the Dark Web, they become a more routine aspect of our lives and, these changes to our lifestyle increase criminal opportunities.

This said, should they wish to transfer funds, at present, Hawala and similar systems are predictable, tested and trusted methods which retain high-levels of anonymity (de Goede, 2003:514). While Brantly challenges the benefits of Hawala in an age where there is a requirement to quickly transfer funds further afield (Brantly, 2014), terrorists favour simplicity and reliability over profit maximisation: the presence of often 'dramatic price swings' of cryptocurrencies 'may prove unattractive beyond occasional, one-off use' (Carlisle, 2017:18).

There is evidence of cryptocurrencies being used by terrorist organisations to move or raise money (Goldman et al., 2016; Weimann, 2016), or buy goods (Paoli et al., 2017). The evidence has, however, tended to be 'generally unconfirmed and anecdotal' (Carlisle, 2017:viii; also Paoli et al., 2017) and cases cited are relatively scarce and involve relatively small amounts of

[4] A small number of offline and surface web retailers have started accepting Bitcoins as currency and Bitcoin ATMs have been introduced where fiat currency can be converted into Bitcoin (Macadam & Palumbo, 2017).

income. This said, that many examples are of online forums being used by 'more technical' extremists to 'educate their peers on the use of virtual currencies' (Goldman et al., 2016:12; also Jacobson, 2010)[5] may suggest a new generation of extremists with increased awareness of online security and, not only an appetite to utilise online systems, but greater familiarity and capability with online tools.

Furthermore, as Wall (2005:81) notes, the internet shifted the organisational nature of criminal activity by empowering 'lone offenders … to carry out incredibly complex and far-reaching tasks that can be repeated countless times over a global span bordered only by levels of online use and language'. As such, it's possible that we may see an emergence of what could be termed lone-wolf cyber-financers: individuals otherwise unconnected to any physical terrorist cell raising money through criminal activity in aid of terrorism.

Geography is a key influencing factor in not only the decision to utilise cryptocurrencies, but also the profitability and anonymity of using cyber (Goldman et al., 2016). Many cybercriminals are based in developed countries with existing infrastructure to support cyber (Carlisle, 2017; also Klausen, 2015). In contrast, terrorist organisations such as ISIL and Hezbollah are not based in areas enriched with such technical infrastructure and expertise, which may present a barrier to utilising cryptocurrencies to any significant scale (Brantly, 2014). Even in the US, which possesses sophisticated cyber-infrastructures, the 'predominate'

[5] For example, there have been a number of online guides on how to fund Islamic terrorism via the Dark Web, including, one document, which guides readers on how to use bitcoins to buy weapons for the mujahedeen (Weimann, 2016).

methods of moving money remains smuggling and 'the movement of funds through the banking system' (Department of Treasury, 2015).

This section has explored how cyber can be usefully employed to raise potentially substantial finances, move money and purchase goods and services. The usefulness of cyber to terrorist organisations has, however, been challenged in the existing literature which has tended to portray cyber as too resource intensive, risky and failing to provide the non-monetary benefits of other enterprises. Furthermore, evidence of the use of cryptocurrencies to raise funds by terrorist organisations appears, in the main, to be anecdotal. This said, there has been cyber activity amongst terrorist cells, and this could become more common as cryptocurrencies become more user friendly to a new generation of terrorists with greater cyber familiarity.

Methodology

Using a grounded theory approach (Corbin & Strauss, 2001), the lead author conducted open-ended interviews with four subject matter experts. Participants were specifically selected for their professional knowledge of terrorism finance, organised crime and the use of cyber to commit criminality, and from varied sectors to allow differing insights and perspectives. The four participants were: P1. A lead government cyber security professional; P2. A Detective Inspector and Deputy Director of the Economic Crime Academy, City of London Police; P3. A financial crime compliance director in the banking sector; P4. A researcher at a major policy think tank and former investment banker.

Participants were identified and contacted through the lead authors professional contacts. Interviews lasted an average of 45 minutes. Ethical approval was provided by the University

of East London Research Ethics Committee. Three interviews were held at the participant's place of work and one by telephone.

A guided interview method was adopted: questions were provided to the participant to generate themes around which they could apply their knowledge, while allowing participants space to develop their ideas. By not applying a rigid question/answer process, the researcher was able to collate data in furtherance of the research, while capturing unexpected information which might dictate new directions of enquiry. This allowed our participant to discuss themes of significance to them, rather than the interviewer. The interview schedule was designed around three research themes aimed at scoping the potential of cyber as a terrorism finance tool both now and in the future:

1. Could and have terrorist organisations become more inclined to utilise cyber-enabled means above more conventional methods of raising finance?
2. Could more contemporary methods of raising, transferring and laundering funds leave terrorist groups more open to infiltration by the security services?
3. Could cryptocurrencies provide terrorist organisations with a more secure / anonymous means of raising, transferring and laundering finance on a global scale and have there already been notable examples of its use by terrorist organisations?

These questions are rooted in the authors observations of the increased use of cyber to commit criminality; identified through the academic literature and, for the lead author, as a law enforcement professional with a working understanding of cryptocurrencies, acquired during professional training and practice. This said, the grounding of 'the theory in reality' allowed

data collection and analysis to be steered by the data rather than the preconceptions of the researcher (Corbin & Strauss, 2001).

Research limitations

Our research was carried out using opportunity sampling and recruited a small sample. While small opportunity samples are common in terrorism and organised crime research, they do limit the generalizability of the findings (Silke, 2001). The present study was designed, however, as an exploratory foray into an emerging area which drew from participants who are particularly well positioned to provide insightful accounts. Furthermore, as Becker (2012) suggests, and as is apparent below, a small number of well-placed participants can demonstrate the complexity of the phenomena.

Results

This section explores the observations and opinions of four subject matter experts. They reflect on the criminal use of cyber to raise finance, how useful this is to terrorist organisations and whether cryptocurrencies have, or could in the future, prove fortuitous to terrorism finance. Four subordinate categories have been identified which best encapsulate the findings of this research: current demand and capability of cyber, future potential of cyber, cryptocurrency use and the use of data to counter terrorist financing. Each subordinate category is addressed within this section.

Demand and capability

Jacobson (2010:353) has argued that Islamist terrorist groups make 'extensive use of the Internet to raise and transfer funds' because it offers 'broad reach, timely efficiency, as well as a certain degree of anonymity and security for donors and recipients' (see also Weimann,

2004). All participants in this study, conversely, agreed that there is currently a lack of appetite by Islamic terrorist organisations to adopt largescale cyber-scams to raise finance.[6] So far there are only a few examples of virtual currencies being used in terrorist attacks and, as P4 suggested, people tend to point to the same example of Indonesia in 2016. This lack of appetite may be because, as P1 suggested, sustained cyber-attacks and cyber-scams require vast resources and may heighten the risk of identification; risks and expenditures which may not be reflected in the rewards.

The lack of demand may also be due to the infrastructure and technical capability lacking in the host states (Brantly, 2014). This said, P2 and P3 argued that even Islamic terrorist cells located in the West - which could capitalise on the infrastructure and their own computer literacy - have so far tended to focus on more traditional finance raising methods of welfare fraud and charitable donations: which are relatively low risk and require few start-up costs. Two participants suggested that cyber may currently be better deployed for propaganda (P1) or recruitment (P3) purposes (see also Klausen, 2015; Stohl, 2007); rather than the raising of finance. All participants did, however, recognise the potential for terrorist organisations to utilise the cyber domain more so in the future, though there is uncertainty as to the form that will take.

Future potential

P1 - a lead government cyber security professional - reflects on the SWIFT attack as a template to attack other financial systems:

[6] P1 moved beyond terrorist financing to acknowledge 'we have never seen cyber-terrorism on any kind of scale' (see Jarvis et al., 2014).

> I'm not saying you could hack them, but just imagine if you did, what you could do, because trillions of dollars go through that every single day, trillions. One extra transaction, would anybody notice? (P1).

P1 and P2, however, pondered how this might be achieved without the technical knowhow or infrastructure to support a hack into the system. They suggested that it may be easier, safer and potentially more effective to 'have someone in one of the data centres install something for you' (P1) through either a form of tiger kidnapping (P1) or corruption (P2). Indeed, corruption of insiders could mitigate the need to utilise cyber to access systems, especially in weak states where officials' poor pay opens the door to corruption (see Rotberg, 2002).

This said, as the interview progressed, P1 identified a generational uplift of 'bright people' with cyber-related specialism within terrorist organisations, and suggested they could bear the fruits of what could be a largescale cyber-attack or -fundraising:

> You see ISIL's mediumship is an online mediumship. It is entirely cyber, there is nothing else to it. Right if you look at their dissemination model and all of that, there are some pretty bright people behind that (P1).

Indeed, ISIL have exploited social media and, developed a computer game (*Saleel Alsvarm*) and mobile application (*Fajr Al-Bashayer*), as part of their recruitment and propaganda campaigns (Sardarnia & Safizadeh, 2017; also Jacobson, 2010).

P2 considered how a state sponsored cyber-attack could be 'massive' by referring to the WannaCry attack on the NHS and the reputed links to North Korea (see Hern & MacAskill, 2017). While few terrorist groups have the capacity for largescale attacks (P1), many states have existing expertise and resources with which to launch or support largescale cyber-attacks or cyber-scams. It might be difficult to identify or trace financial flows moving from states to terrorists. States have, in the past, supported terrorists and insurgents by providing training, logistical support, equipment, weapons and/or finance (see Levitt, 2007) and if cybercrime is traditional crimes carried out online, then there is a potential threat of state or state-sponsored cyber-terrorism.

In summary, according to our participants, Islamist terrorists are not presently utilising cyber platforms to raise finances or conduct attacks to any significant extent, and there is a general consensus that traditional methods are currently the preferred option. There does, however, appear to be an unsettling rumbling that the growth in cyber-related acumen within these organisations might presuppose a future where cyber becomes a, if not the, preferred channel for raising finance. In this regard, our participants conflict with scholars, such as Jacobson (2010) and Weimann (2004, 2016), who suggest that terrorists are already extensively using cyber to raise funds; although their views on potential future usage are more closely aligned.

Cryptocurrency use

The general opinion of participants was that cryptocurrencies are not quite established enough to veer terrorist organisations away from traditional methods of moving money or purchasing goods and services. As P1 notes, most terrorist organisations prefer to operate in cash and would need to convert cryptocurrency into cash for many expenses: families of imprisoned

terrorists are unlikely to welcome Bitcoin pensions, nor can the building of mosques or schools be paid for online. This said, P1's thoughts on the topic shifted as the interview progressed:

> I think terrorist use of cyber to get finance has some limits …. they're not going to go using Bitcoins to buy stuff on the Dark Web, like credit card numbers. Oh my, that's not actually a bad thing, using credit card numbers to cash out on the ATM, that would work (P1).

What's interesting here is the rawness of the participant's response. It highlights how primitive current understanding and forethought is of how cryptocurrencies could be utilised to the benefit of terrorist organisations in the future.

P1 thoughts developed further by referring to current cyber-related crime trends which are less resource intensive and might rationalise a use for cryptocurrency by terrorist organisations. For example, there's a lot of anecdotal evidence of online extortion, such as where criminals demand a thousand Bitcoins in exchange for a company's data log to be released (Baig & Hampton, 2015). Cryptocurrencies are chosen partly because they are far more difficult to trace (P1). Furthermore, in some instances, the offender might not actually have carried out a full infiltration of a company's network. Rather an old fashioned lie can do the trick: A terrorist need only access a sample of data to dupe a company into believing all data has been breached and pay out the requisite amount of cryptocurrency because, not only do 'people always assume that criminals tell the truth', but identifying this deceit can be time consuming (P1). P1 then began considering how malware could be used to mine cryptocurrencies and generate real cash.

Then, having originally pondered how converting cryptocurrencies to cash might deter their use by terrorists, P1 highlights the ease with which this may be done, and how terrorist financers may draw from their offline experiences of laundering or moving currency. As the interview progressed P1, who had been critical of the utility of cryptocurrencies for terrorists, begins to identify how, with the right mind-set and acumen, anything's possible. P1's earlier assumption about terrorists not needing cryptocurrencies and the Dark Web may, however, be true in area such as the Tri-border Region or South Asia, where weapons and other resources can easily be purchased with cash:

> My understanding is that the Dark Web is used more by organised crime to make their purchases of guns, particularly of ammunition.... So I think in more sophisticated societies, in more cyber dependent societies, the Dark Web is going to be something that is used more. I think in cash rich societies like Pakistan, there's no evidence that it's used (P.2).

This argument could be extended further than a Global South/North divide: Strict firearm regulations in Europe could result in more significant usage of the Dark Web compared with more relaxed regulatory regimes (i.e. the USA). Paoli and colleagues (2017) suggest that the purchase of weapons and ammunition on the Dark Web may be more beneficial to those without the smuggling infrastructure to support the acquisition of arms, such as lone wolf actors or smaller cells. This harks back to Wall's (2005) observation of the internet's empowerment of lone criminals to reinforce our earlier suggestion of the potential rise of lone-wolf cyber-financers.

P1 considered the level of anonymity that Bitcoin has to offer, clarifying that there has been nothing by which this has been truly tested, but that on the whole it appears to be quite good. P4 is, however, far more sceptical as to whether there could be enough trust in the value of the currency, or the aptitude to use it. Indeed, he notes that cryptocurrencies can be awkward and time consuming to use and tend not to be 'as anonymous as people think' (P4).

This argument might not stand the test of time, as rapid advancements in cyber technology and growing normalisation of cryptocurrencies could increase the ease and reduce the risk of terrorist utilisation of cryptocurrencies, in much the same way that the evolution of the mobile phone changed the structure of criminal markets. Indeed, P2 brings to focus the dynamism of terrorists to adapt to their surroundings: 'I think you will see the changing face of funding, as we have for all areas of crime. I think the terrorists will make best use of these systems that we introduce' (P2).

P4, who initially reflected on the success of traditional methods, also warns that we should tread carefully, avoid becoming too routed in the finance models of 9/11 and remember how adaptive terrorists can be. That while 'much of today's response to terrorist fundraising is a function of … the funding model that Al Qaeda were using at the time [of 9/11], so donors and charities' we need to monitor for future financial opportunities, which may include the cyber domain (P4).

As the P1 and P4s interview progressed, both participants' sceptical reflection on the use of cryptocurrencies began to change and they began considering the wider use of cyber and potential avenues of use by terrorists. Overall, our participants were sceptical, yet agreed that

to rule out the use of cryptocurrencies, and cyber more generally, would be detrimental to efforts in identifying and tracking terrorism finance.

Data

Participants' responses direct focus to how data might be retrieved and managed to deliver more effective information and intelligence feeds. P1 - a lead government cyber security professional - asserted a lack of confidence in methods applied to data collation:

> The reports that are published show a rise in the use of cyber to commit criminality, absolutely. [However] I am not convinced the data we have is good data. The way that we collect that data is not great (P1).

The lack of data regarding the use of cryptocurrencies by terrorist cells, or potential for their use, does not serve well in initiating any action from the banking sector, to implement compliance around their use. Indeed, P3 - a financial crime compliance director in the banking sector - suggested that banks are not focused on cryptocurrencies:

> I think unless it's a clear risk that the banks or the government says, you know, we know bank x y z in Spain, the terrorists are using cryptocurrency, unless there's a clear methodology or typology that the financial community observes, that's something they haven't gotten to. There are so many other things to comply with, that creating compliance around cryptocurrency; it's just that most people aren't there yet (P3).

These statements from P1 and P3, when connected to the shifts in thinking around how cyber could be utilised by terrorists discussed above, lead to questions around whether we are looking for the correct data and, whether the use of cryptocurrency and cyber platforms is more relied upon than is empirically known.

Both P3 and P4 considered the need for a new approach whereby, rather than trying to stop terrorism financing, we utilise the intelligence value of financial data as a counterterrorism tool. That is, financial transactions can highlight social and business network connections: 'just as the meta-data of communications is very valuable, the meta-data of finance, the value of it, I think is overlooked' (P4).

Terrorists' financial transactions are becoming more difficult to trace; such is the low cost of recent attack methodologies. Identifying the meta-data of financial flows may help determine the routines of potential terrorists and, once these routines are identified, any change of behaviour or introduction of a new financial relationship might trigger an important intelligence feed between the banking sector and law enforcement.

This flow of information would need to be fluid between both sectors, whilst remaining within lawful parameters. As such, all agencies with oversight and interest in these transactions should understand and work to the same meta-data model and respective 'red flag' triggers. Such attention to detail, however, requires dedicated resource and regular collaborative working between organisations.

P3 stressed the difficulties in setting the parameters for such triggers and creating the right balance to avoid overwhelming banks with more red flags then they have the capacity to handle.

For larger banks, with a wealth of resource, implementing such measures might be achievable. Whereas lower resourced banks may struggle. As such, banks may need to work collaboratively, perhaps sharing resources where required, to avoid a two-tier response which could facilitate displacement from larger banks - with the resources to support counter-measures - to smaller establishments. Indeed, this displacement could create a worrying 'a-symmetry of information' (P4).

P3, however, clarifies that the risk–based approach applied by banks would dictate that the labour intensive process of putting in place such compliance processes, which might not be a priority for a smaller bank: If the smaller bank observes more activity aligned to fraud, then they may be more likely to align stretched resources to that greater risk. This said, P4 suggested that most banks, regardless of size, generally align greater resource to counter-fraud efforts due to its direct effect on customers. That is, incidents of fraud could result in customers moving their business elsewhere, although when illicit activities are identified they can be costly (P4) (see Arnold, 2018).

This said, some larger banks have recently refused to deal with cryptocurrencies, including banning the use of credit cards to purchase cryptocurrencies. This appears to be partly a response to regulators concerns around money laundering coupled with banks, and some governments, concerns around the volatility of cryptocurrencies (Coppola, 2018). This could, however, result in an increase flow of cryptocurrencies through smaller banks or those situated in countries with less stringent regulations.

There are also institutional barriers within law enforcement to following the data. First, international information sharing can be limited by a lack of international cooperation

(Raphaeli, 2003). Second, austerity measures have affected the ability of the police service to effectively tackle a variety of criminality (see Windle, 2017) likely including the investigation and prevention of cybercrime. Finally, the tendency to specialise police skillsets means that few are trained to counter cybercrime: 'there's this massive gap between where policing should be and where we are' (P2). During the interview, P2 reflected upon the lack of counter-terrorism finance training for fraud investigators:

> We should be identifying where [cyber is] being used for terrorism, what the red flags are and then putting that back into the training, and to my knowledge, that's not happening in any shape or form currently, which has come out of this conversation actually (P2).

While Weimann (2004, 2016) has argued that the anonymity of the Dark Web and cryptocurrencies will result in incremental usage by terrorists, overall, our participants, highlighted the value of cyber as an investigatory tool. Terrorists will, thorough human error, make mistakes; leaving a 'cyber-footprint' which provides an opportunity to identify and locate offenders. Our participants also identified a lack of preparedness and respective training regarding the use of cyber in terrorism finance and cybercrime more generally. Our participants originally rejected the use of cyber-platforms for terrorist financing, yet as interviews progressed their thoughts unfolded as raw initial concepts about how cyber could be utilised in the future. It's possible, that insufficient reflection on the future use of cyber is a key driver of this lack of training.

Conclusion

This research commenced with an overview of traditional terrorist fundraising methods to demonstrate how they may remain beneficial, regardless of geographic location. Three questions were set as a premise to this research, to establish how and whether cyber has enabled terrorist organisations to raise finance, and if this use of cyber is likely to gain momentum, perhaps replacing traditional methods. No conclusive answers have been arrived at in response to the questions posed, partly due to varied factors influencing terrorist financing decision making but also due to the lack of quality data regarding terrorists' use of cyber platforms and cryptocurrencies.

An unexpected result is that inadequate time appears to have been invested in reflecting on the role of cyber in terrorist financing. The interviews demonstrated an almost impromptu thought process of how cyber could best be utilised; moving from statements which completely ruled out the use of cyber to later identifying great potential for its use. Indeed, the interview process itself appears to have forced a reflection on the use of cyber, which led some participants to shift their thinking on its potential in terrorist financing. This conclusion parallels the 2015 US Department of Treasury (2015:58) position that while 'the possibility exists that terrorist groups may use these new payment systems to transfer funds … the degree to which this presents a residual TF [terrorist finance] risk is unclear'.

Our participants suggested that an increase in cyber capability might be influenced by greater opportunities presented by new technology and a shift to a younger generation of terrorists more adept in the use of cyber. This could be further accelerated by more transient terrorist movements (Klausen, 2015). Indeed, *if* cryptocurrencies and the Dark Web become a more

routine aspect of everyday life, then these changes to our lifestyle could increase terrorist financing opportunities (see Cohen & Felson, 1979).

The identification of future threats – including the potential for what we have termed lone-wolf cyber-financers - coupled with the lack of preparedness, suggests that bespoke training of security services and wider organisations now may put security agencies one step ahead. Fundamental gaps have been highlighted, which might prevent effective progression of counter-terrorism finance efforts, if not filled. Indeed, as P4's reflections might imply, 'counter' terrorism finance is perhaps the wrong turn of phrase, if the objective is not to counter it, but to 'use' it as intelligence to identify perpetrators and counter terrorism as a whole. As such, data collection should be a key element in the syllabus of any bespoke training.

The meta–data of cyber-terrorism finance will not be a 'one size fits all', and training needs to reflect this. Financial behaviours can vary considerably depending on local context, in particular with regards to standards of infrastructure and capability to support cyber-related enterprises. By deciphering geographic profiles of how individuals might raise, send and receive finance, more context will be provided from which to make assumptions regarding financial behaviours, and to recognise shift in methodology.[7]

[7] For example, ISIL in Syria will require a steady flow of high-income to pay for large organisational costs. Traditional methods of extortion and contraband smuggling may be preferred over cyber due to a lack of cyber infrastructure and support coupled with the requirement for cash rather than cryptocurrency. Conversely, the smaller ISIL-associated cell operating in the UK may have access to a stronger cyber skillset and infrastructure, a more

This said, while the need for anticipating future cyber threats is apparent, the development of investigation tools and training is costly. Scarce resources will need to be justified by implementing institutions; and our participants demonstrated that there is presently little evidence pointing to widespread use of this particular financing strategy and consideration of how this could develop in the future appears lacking

Paul Ekblom (2005:233) has, however, argued that governments should scan for emerging crime problems so they can be 'nipped in the bud'. Horizon-scanning methodologies can start with knowledgeable individuals 'thinking thief' (Ekblom, 2005), as did our participants when running 'what if' scenarios: during the interview process participants began identifying potential areas of concern. While this is a good start, the evidence base is still lacking and more in-depth research on the scope and nature of cyber-terrorist financing is required. This should involve interviews with a much larger sample of private and public practitioners, and, current and/or former cyber terrorist financers. Such research could illuminate the potential scope of future threats whilst providing a much needed evidence-base for training and investigative tools.

While the findings of this paper are hampered by our small opportunity sample, they present new insights into an emerging area. Most importantly, for now, they demonstrate the complexity of the phenomena, and insight into knowledge gaps: of which there are many.

pressing need to conceal money and the purchase of arms. As such, online extortion for bitcoins, used to buy arms on the Dark Web, may be preferable to traditional methods.

Carroll, P., & Windle, J. (2018). Cyber as an enabler of terrorism financing, now and in the future. *Journal of Policing, Intelligence and Counter Terrorism*, *13*(3), 285-300. Pre-print

References

Anderson, R. Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T. and Savage, S. (2013). Measuring the cost of cybercrime. In Böhme, R. (Ed.) *The Economics of Information Security and Privacy*. Berlin: Springer.

Arnold, M. (2018). HSBC hopes to leave era of scandals behind. *The Financial Times*, 18 February 2018.

Asal, V. Milward, H. and Schoon, E.W. (2015). When terrorists go bad: Analyzing terrorist organizations' involvement in drug smuggling. *International Studies Quarterly*, 59(1), 112-123.

Barratt, M., Ferris, J. and Winstock, A. (2014). Use of Silk Road, the online drug marketplace, in the United Kingdom, Australia and the United States. *Addiction*, 109(5), 774-783.

Becker, H.S. (2012) in Baker, S.E., Edwards, R. and Doidge, M. (eds.), *How Many Qualitative Interviews is Enough?* (London: Economic and Social Research Council). Retrieved from http://eprints.brighton.ac.uk/11632/ (consulted 29th May 2016).

Brantly, A. (2014). Financing terror bit by bit. *CTC Sentinel*, 7(1), 3-4.

Carlisle, D. (2017). *Virtual Currencies and Financial Crime Challenges and Opportunities* (London: RUSI). Retrieved from https://rusi.org/publication/occasional-papers/virtual-currencies-and-financial-crime-challenges-and-opportunities (consulted 14 December 2017).

Cohen, L. and Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(9), 588-608.

Coppola, F. (2018). Why credit card users should thank banks for stopping them buying cryptocurrencies. *Forbes*, 5 February 2018. Retrieved from

Carroll, P., & Windle, J. (2018). Cyber as an enabler of terrorism financing, now and in the future. *Journal of Policing, Intelligence and Counter Terrorism*, *13*(3), 285-300. Pre-print

https://www.forbes.com/sites/francescoppola/2018/02/05/why-credit-card-users-should-thank-banks-for-stopping-them-buying-cryptocurrencies/#78278b837998 (consulted 15 July 2018).

Corbin, J. and Strauss, A. (1990). Grounded theory research: Procedures, canons and evaluative criteria. *Qualitative Sociology*, 13, 3-20.

Comras, V. (2007). Al Qaeda finances and funding to affiliated groups. In Giraldom, J.K. and Trinkunas, H.A. (Eds.). *Terrorism Financing and State Responses: A Comparative Perspective*. Stanford: Stanford University Press.

Conway, M. (2006). Terrorism and the internet: New media - new threat?" *Parliamentary Affairs*, 59(2), 283-298.

Cooper, W.H. (2017). The dark side of the economy: A comparative analysis of the Islamic State's revenue streams. *Journal of Terrorism Research*, 8(1), 34-42.

Department of Treasury (2015). *National Terrorist Financing Risk Assessment, 2015* (Washington: Department of Treasury). Retrieved from https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Terrorist%20Financing%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf (consulted 14 November 2017).

Dunietz, J. (2017). The imperfect crime: How the WannaCry hackers could get nabbed. *American Scientific*, 16 August 2017.

Ekblom, P. (2010). Designing products against crime. In Tilley, N. (Ed.) *Handbook of Crime Prevention and Community Safet*y. London: Willan.

Felbab-Brown, V. (2010). *Shooting up: Counterinsurgency and the War on Drugs*. Washington: Brookings Institution Press.

Carroll, P., & Windle, J. (2018). Cyber as an enabler of terrorism financing, now and in the future. *Journal of Policing, Intelligence and Counter Terrorism*, *13*(3), 285-300. Pre-print

Filipkowski, W. (2008). Cyber laundering: An analysis of typology and techniques. *International Journal of Criminal Justice Sciences*, 3(1), 15-27.

Finch, E. (2003). What a tangled web we weave: Identity theft and the internet. In Jewkes, Y. (Ed.). *Dot.cons: Crime, Deviance, and Identity on the Internet*. Collompton: Willan.

Finkle, J. (2016). Bangladesh bank hackers compromised SWIFT software, warning issued. *Reuters*, 25 April 2016. Retrieved from https://www.reuters.com/article/us-usa-nyfed-bangladesh-malware-exclusiv/bangladesh-bank-hackers-compromised-swift-software-warning-issued-idUSKCN0XM0DR (consulted 23rd June 2017).

de Goede, M. (2003). Hawala discourses and the war on terrorist finance. *Environment and Planning D: Society and Space*, 21(5), 513-532.

Goldman, Z., Maruyama, E., Rosenberg, E., Saravalle, E. and Solomon-Strauss, J. (2016). *Terrorist Use of Virtual Currencies - Containing the Potential Threat* (Washington: Centre for a New American Security). Retrieved from https://www.cnas.org/publications/reports/terrorist-use-of-virtual-currencies (consulted 9 July 2017)

Hampton, N. and Baig, Z.A. (2015). *Emergence of the Cyber-Extortion Menace*. Retrieved from http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1179&context=ism (consulted 9 July 2017).

Hern, A. and MacAskill, E. (2018). WannaCry ransomware attack 'linked to North Korea'. *The Guardian*, 16 June 2017.

Hourigan, N., Morrison, J.F., Windle, J. and Silke, A. (2018). Crime in Ireland, North and South: Feuding gangs and profiteering paramilitaries. *Trends in Organized Crime*, 21(2), 126-146.

Carroll, P., & Windle, J. (2018). Cyber as an enabler of terrorism financing, now and in the future. *Journal of Policing, Intelligence and Counter Terrorism*, *13*(3), 285-300. Pre-print

Jacobson, M. (2010). Terrorist financing and the internet. *Studies in Conflict & Terrorism*, 33(4), 356-372

Jarvis, L., Macdonald, S. and Nouri, L. (2014). The cyberterrorism threat: Findings from a survey of researchers. *Studies in Conflict & Terrorism*, 37(1), 68-90.

Johnston, P.B. (2014). *Countering ISIL's Financing.* (California: RAND Corporation). Retrieved from http://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT419/RAND_CT419.pdf (consulted 11 June 2017).

Kim, W., Jeong, O., Kim C. and So, J. (2011). The dark side of the internet: Attacks, costs and responses. *Information Systems*, 36(3), 675-705.

Klausen, J. (2015). Tweeting the Jihad: Social media networks of Western foreign fighters in Syria and Iraq. *Studies in Conflict & Terrorism*, 38(1), 1-22.

Levitt, M. (2007). *Hamas*. New Haven: Yale University Press.

Macadam, D. and Palumbo, D. (2017). What is Bitcoin. *BBC News*, 11 December 2017. Retrieved from http://www.bbc.com/news/business-42150512 (consulted 11 December 2017).

Makarenko, T. (2004). The Crime-terror continuum: Tracing the interplay between transnational organised crime and terrorism. *Global Crime*, 6(1), 129-145.

Mallet, V. and Chilkoti, A. (2016). How cyber criminals targeted almost $1bn in Bangladesh bank heist. *Financial Times*, 18 March 2016.

Napoleoni, L. (2007). Terrorism financing in Europe. In Giraldom, J.K. and Trinkunas, H.A. (Eds.). *Terrorism Financing and State Responses: A Comparative Perspective*. Stanford: Stanford University Press.

Carroll, P., & Windle, J. (2018). Cyber as an enabler of terrorism financing, now and in the future. *Journal of Policing, Intelligence and Counter Terrorism*, *13*(3), 285-300. Pre-print

Paoli, G., Aldridge, J., Ryan, N. and Warnes, R. (2017). *Behind the Curtain: The Illicit Trade of Firearms, Explosives and Ammunition on the Dark Web* (California: RAND Corporation). Retrieved from https://www.rand.org/pubs/research_reports/RR2091.html (consulted 11 December 2017).

Passas, N. (2007). Terrorism financing mechanisms and policy dilemmas. In Giraldom, J.K. and Trinkunas, H.A. (Eds.). *Terrorism Financing and State Responses: A Comparative Perspective*. Stanford: Stanford University Press.

Picarelli, J.T. and Shelley, L.I. (2007). Organized crime and terrorism. In Giraldom, J.K. and Trinkunas, H.A. (Eds.). *Terrorism Financing and State Responses: A Comparative Perspective*. Stanford: Stanford University Press.

Richards, A. (2014). Conceptualizing terrorism. *Studies in Conflict & Terrorism*, 37(3), 213-236.

Raphaeli, N. (2003). Financing of terrorism: Sources, methods, and channels. *Terrorism & Political Violence*, 15(4), 59-82.

Rotberg, R. (2002). Failed states in a world of terror. *Foreign Affairs*, 81(4), 127-140.

Roth, M.P. and Sever, M. (2007). The Kurdish Workers Party (PKK) as criminal syndicate: Funding terrorism through organized crime, a case study. *Studies in Conflict & Terrorism*, 30(10), 901-920.

Rudner, M. (2010). Hizbullah terrorism finance: Fund-raising and money-laundering. *Studies in Conflict & Terrorism*, 33(8), 700-715.

Sardarnia, K. and Safizadeh, R. (2017). The Internet and Its Potentials for Networking and Identity Seeking: A Study on ISIS. *Terrorism & Political Violence* (online first).

Carroll, P., & Windle, J. (2018). Cyber as an enabler of terrorism financing, now and in the future. *Journal of Policing, Intelligence and Counter Terrorism*, *13*(3), 285-300. Pre-print

Silke, A. (2000). "Drink, drugs, and rock'n'roll: Financing loyalist terrorism in Northern Ireland — part two. *Studies in Conflict & Terrorism*, 23(2), 108-132.

Silke, A. (2001). The Devil you know: Continuing problems with research on terrorism. *Terrorism & Political Violence*, 13(4), 1-14.

Stohl, M. (2007). Cyber terrorism: A Clear and Present Danger, the Sum of all Fears, Breaking Point or Patriot Games? *Crime, Law and Social Change*, 46(4-5), 223-238.

Storrod, M.L. and Densley, J.A. (2017). 'Going viral' and 'going country': The expressive and instrumental activities of street gangs on social media. *Journal of Youth Studies*, 20(6), 677-696.

Wall, D.S. (2005). The internet as a conduit for criminals. In Pattavina, A. (Ed.) *Information Technology and the Criminal Justice System*. Thousand Oaks: Sage.

Weimann, G. (2004). *www.terror.net: How Modern Terrorism uses the Internet*. Washington: United States Institute of Peace.

Weimann, G. (2016). Going dark: Terrorism on the dark web. *Studies in Conflict & Terrorism*, 39(3), 195-206.

Windle, J. (2017). The impact of the Great Recession on the Irish drug market. *Criminology & Criminal Justice* (online first).

Windle, J. (forthcoming / 2018). Fundraising, organised crime and financing terrorism. In Silke, A. (Ed.). *The Routledge Handbook of Terrorism and Counter-Terrorism*. Abingdon: Routledge.

Windle, J., Morrison, J.F., Winter, A. and Silke, A. (2018). *Historical Perspectives on Organised Crime and Terrorism*. Abingdon: Routledge.

Wittig, T. (2011). *Understanding Terrorist Finance*. Basingstoke: Palgrave Macmillan.