The Centre for the Study of Terrorism and Political Violence
Journal of Terrorism Research

Striking at their Core – De-funding the Islamic State of Iraq and Syria

by Alessio Shostak

Abstract

The fundraising efforts of the Islamic State of Iraq and Syria (ISIS) have impressed academics, journalists, and government officials alike. The literature has thus far explored the methods via which ISIS acquire funds and transfer their proceeds across international borders. This article aims to expand upon these entries by analysing the failures of EU and US policy to counter terrorist financing since the 9/11 attacks, particularly with regards to the inability of both entities to adjust to digital transfer methods. The value of military operations will also be discussed within the context of halting the Islamic State's fundraising capabilities.

Keywords: *ISIS; Terrorist Financing; Transfer Methods; CFT; War on Terror; Iraq; Syria*

Introduction

Recent terrorist attacks across the Western world have placed the spotlight on the threat of terrorism as a whole, and the Islamic State in Iraq and Syria (ISIS) in particular. ISIS has been described by David Cohen (2014), a leading official in the US Department of the Treasury, as "the best funded terrorist organisation we have come across". Indeed, in 2015 their estimated asset pool was valued at $2 billion; greater than the GDP of many small nations (Fowler, 2015). Media outlets have dedicated countless hours to covering the ongoing military struggle waged by the international community against ISIS. However, to date there has been relatively scant coverage of the group's ability to raise and move funds in order to finance their terrorist activities and maintain an infrastructure necessary to sustain their caliphate. Terrorist financing has been coined by Raphaeli (2003) as "an octopus with tentacles spreading across vast territories" (p.59), and a key portion of this paper will be dedicated to analysing ISIS's sources of revenue. It will also discuss ISIS's methods of transferring funds, with an emphasis placed on what the Financial Action Task Force (FATF) refer to as "emerging terrorist financing risks" such as virtual currencies and prepaid cards (FATF 2015: 4). The bulk of this paper will then be reserved for addressing (a) the measures the international community – particularly the EU and the United States – has taken to counter the financing of terrorism (CFT) since the 9/11 terrorist attacks, (b) whether these measures have been successful, and (c) what measures and approaches should be taken in the future. Finally, this paper will adopt a broader focus by outlining the indispensable role of private-public sector cooperation to combatting terrorist financing while stressing the interconnectedness of military and non-military measures in the fight against ISIS.

Expenditures

Terrorists require funds for a myriad of purposes. The most evident use of funding is for 'operational costs' in order to directly plan and carry out terrorist attacks; this includes the potential costs associated with the falsification of documents, the purchasing of weapons, and the use of vehicles for transportation. However,

Biersteker and Eckert (2008) note that only approximately 10% of funds are allocated to operational costs (p.8). Indeed, the direct expenses of conducting terrorist attacks tend to be quite low; for instance, the cost of the 2004 Madrid bombings for Al Qaeda was approximately $100,000 (Gomez, 2010: 4). The vast majority of funds are allocated by terrorist groups towards what Biersteker and Eckert (2008) describe as "infrastructure" (p.8) in order to sustain and expand the organisation. These include paying members' salaries, providing ideological and military training, and recruitment and propaganda costs. ISIS additionally fund social welfare programs in their occupied territories in order to create the perception that their rule is legitimate. This involves the creation of police forces, the subsidizing of schools and the provisioning of basic necessities such as food and electricity. ISIS have also overseen numerous "state-building activities" such as the establishment of a "court of grievances", a body empowered to process civilian complaints against ISIS officials (Stergiou, 2016: 198). Overall, terrorist organisations must incur substantial costs in order to function, irrespective of their vast network of fundraising sources.

Sources of Funding

ISIS have utilized their territorial control to develop self-sufficient fundraising methods which would be, in Cronin's (2015) words, "unthinkable for most terrorist groups". Chief among these is revenue from the sale of 'domestic' petroleum and refined petroleum products to individuals in ISIS-held territory and several entities abroad, ranging from the Syrian government to criminal elements in Turkey. The US Treasury (2015) estimates that ISIS accrued $100 million in revenue from petroleum and petroleum-related products in 2014. Despite this, numerous sources indicate that the rate of oil extraction has declined precipitously in recent years, dropping from 80,000 barrels per day (bpd) in August 2014 to 20,000 bpd in November 2014 (Levitt, 2014). This has mainly been attributed to the persistent effects of US-led coalition airstrikes on mobile oil refineries. Most significantly, revenues from petroleum and petroleum products have also plummeted, with some positing as much as an 80% decrease between October 2014 and April 2015 (Bahney and Johnston, 2014). This has largely been due to (a) the aforementioned airstrikes, (b) Turkey's enhanced border security measures, and (c) the recent fall in oil prices. Several authors have suggested that these revenues have reached a peak, and that from now on ISIS will rely more heavily on other sources of funding.

One such base of funds is the extortion racket run by the Islamic State within their territory. Involuntary taxation is derived from all manner of sources, some of which include a 5-10% tax on all cash withdrawals, customs taxes on vehicles entering and exiting ISIS territory, and so-called 'jizya' taxes on religious minorities. Another key fundraising source is the sale of cultural artefacts on the black market. ISIS have occupied over 4,500 archaeological sites, and some sources estimate that sales of artefacts have garnered "tens of millions of USD" from Syria alone (FATF, 2015: 16). Despite only contributing to 5% of ISIS's total revenue, Stergiou (2016) projects that external contributions from wealthy patrons – particularly from Gulf States such as Qatar and Kuwait–are projected to increase in importance given the dwindling fundraising potential of oil reserves in ISIS-held territory (p.204).

Transfer Methods

Traditional Methods

The use of standard wire transfers via the formal financial system has become troublesome for terrorists–and

particularly for ISIS–due to the policies enacted by the international community in order to identify and freeze suspicious transactions. Consequently, terrorist groups have shifted to unconventional methods to transfer funds across their vast networks. Chief among these is the use of informal value transfer systems (IVTS), most notably of 'hawala' networks. These networks are characterized by their ability to transfer funds across borders without the physical movement of these funds via a complex process involving several intermediaries. Hawalas play a key role in the economy, having traditionally served as remittance systems for migrants to transfer money back to their families residing in developing nations without a reliable banking system. However, as Berti (2008) claims, "the very characteristics that account for hawala's success have made it an impenetrable haven for illicit and criminal transactions" (17). Chief among these is the lack of a transparent audit trail, as hawala operators are unlikely to keep extensive transaction records or to verify customer identity. The key policy challenge for lawmakers and regulators has been to strike a balance between mitigating TF risks while also preventing excessive compliance regulation. However, the severe lack of recent documented cases involving hawalas suggests that terrorist organisations such as ISIS have transitioned away from these traditional transfer methods towards novel, 'emerging' methods in order to globally transfer their funds.

Emerging Methods

Financial innovation has produced a wide variety of payment methods and services. Although it is indisputable that each of these advances has had positive ramifications on society as a whole, they have unfortunately raised numerous potential anti-money laundering (AML)/CFT vulnerabilities which policymakers ought to address. At the outset, it is important to note that concrete examples of these systems being used to finance terrorist activities are few and far between; indeed, in a recent report the FATF (2015) claimed that "the actual prevalence and level of exploitation of these technologies by terrorist groups and their supporters is not clear at this time and remains an ongoing information gap to be explored" (p.6). However, the FATF also stressed the probability of terrorists having adapted to using these services after heightened AML/CFT regulations elsewhere. The subsequently outlined threats should therefore be placed highly on any nation's counter-terrorism agenda.

Cryptocurrencies are one of the novel methods of transferring funds that are subject to TF risks. Cryptocurrencies are virtual currencies, which are defined as "digital sources of value that can be digitally traded" (FATF, 2014: 4). On one hand, virtual currencies such as Bitcoin have various legitimate uses; for instance, experts claim that bitcoin could reduce transaction costs and facilitate micro-transactions (FATF, 2014). However, the TF risks associated with these currencies are substantial, not least among which is the greater anonymity offered by cryptocurrencies relative to other non-cash methods of money transfer; browser extensions such as Dark Wallet obscure the source of Bitcoin transactions, while Bitcoin accounts do not require identity verification. The decentralized nature of cryptocurrencies implies the lack of a central administrator to monitor transactions – this increases the difficulty of any potential enforcement efforts by eliminating the focal point of any asset seizing measures that might be implemented. Policy solutions must counterweigh the benefits and drawbacks of these cryptocurrencies. In the absence of a central administrator, the IMF have advocated for the imposition of AML/CFT regulations (such as customer due diligence requirements) on the institutions – known as 'covered entities'–facilitating the exchange of Bitcoin into fiat currency (IMF, 2016). However, legislation to this effect is in its infancy in most jurisdictions; indeed, the EU has no regulations in place whatsoever with respect to virtual currencies.

Prepaid cards – cards "preloaded with a fixed amount of electronic value" – are another 'emerging' method of money transfer among terrorists (Kim-Kwang, 2008: 12). As cryptocurrencies, the positive aspects of prepaid cards are not in doubt; they are an essential component of the distribution of disaster assistance, in addition to providing an invaluable method for disadvantaged individuals to purchase goods online. However, prepaid cards pose serious TF risks; for instance, the lack of reporting requirements on international transfers of prepaid cards is a key loophole that could be used by terrorists to avoid restrictions on cash smuggling (FATF, 2015). On a broader note, a key barrier in the fight against the use of prepaid cards for nefarious purposes is the vast differences in legislation across jurisdictions, particularly with regard to regulations applied to small to medium sized card providers. This gives terrorists the freedom to purchase prepaid cards in areas where AML/CFT legislation is weakest before freely transferring these cards across international borders (FATF, 2015). The use of prepaid cards by terrorist organisations is less abstract than other methods that have hitherto been discussed; indeed, they were most notably found in the apartments of the perpetrators of the Charlie Hebdo attacks in Paris. Some legislative proposals have been brought forward to tackle the vulnerabilities associated with these cards; for instance, one recent EU Communication (2016) called for amending the 4th EU AML Directive to introduce regulations on pre-paid card issuers. However, significantly more progress must be made in order to overcome the TF risks posed by this emerging method of transferring funds.

Policy Responses

International Measures

Prior to 9/11, international CFT regulations have been widely viewed as having been insufficient; by 9/11 the 'International Convention on the Suppressing of the Financing of Terrorism' – the first ever UN resolution explicitly prohibiting the financial or material support of terrorist groups – had only been ratified by four nations (Biersteker and Eckert, 2008). Despite its creation in 1989, the FATF's sole focus prior to 9/11 was on AML legislation. Following the attacks, the FATF expanded its mandate to include the battle against terrorist financing, releasing eight 'Special CFT Recommendations'. These recommendations highlighted several key issues, including the mandatory issuance of suspicious transaction reports (STRs) to "competent authorities" in suspected TF cases (FATF, 2001: 2). These eight guidelines – expanded to nine in 2004 – also endorsed UN Resolutions 1267 and 1373, two crucial CFT measures advocating for the freezing of assets belonging to designated terrorists and terrorist affiliates. These Recommendations, and all subsequent work by the FATF, have been adopted by the international community as the "international standards in the fight against terrorist finances" (Bures, 2012: 715). It is important to note, however that the success of these standards is – and will continue to be–incumbent upon the ability of legislative bodies such as the EU and US to implement these standards into law, and of regulatory agencies to enforce these laws.

The European Union

The European Union's two-pronged AML/CFT approach has been viewed by many as being strongly "in parallel with international developments in the field, in particular initiatives by the FATF" (Gilmore and Mitsilegas, 2007: 120). One aspect of this effort is the 'smart sanctions model', which calls for the full implementation of UNSCRs 1267 and 1373 (Bures, 2015). This resulted in the transposition of the terrorist blacklist developed by the 1267 Sanctions Committee into EU law. The second strand of the Union's CFT

efforts has been the 'AML FATF Model', whereby EU legislation – in the form of 'AML Directives'–has adapted over time in order to match FATF AML/CFT Recommendations (Ibid). The Third AML Directive (2005) was the first to explicitly prohibit the financing of terrorist organisations, aiming to adopt the nine Special FATF Recommendations into law. Among other measures, this Directive gave Financial Intelligence Units (FIUs)–the key CFT regulators on a national scale – full access to various nationwide databases including police records, while also expanding customer identity verification requirements via the banning of anonymous bank accounts (Gilmore and Mitsilegas, 2007). In 2015, the Fourth Directive was adopted in order to align with the revised 2012 FATF AML/CFT Recommendations. This was done primarily by increasing the flexibility of FI due diligence obligations depending on the 'risk' posed by the client.

Despite the success of the directives at transposing UN resolutions and FATF Recommendations into EU legislation, evidence suggests that the implementation of these laws has occurred slowly and is, as yet, incomplete. This slow implementation has primarily been linked to the differences in the perceived threats of a terrorist attack among member states, as nations who view an attack as unlikely are susceptible to become 'free-riders' in order to avoid bearing the costs of implementation (Clunan, 2006). One instance of this is the lack of asset freezing arrangements within certain EU member states. Moreover, a recent EU Communication (2016) outlined the necessity of amending the 4th EU AML Directive to monitor virtual exchanges and increase regulations on pre-paid card issuers; in my view, the slow speed at which this issue is being addressed could potentially be due to the 'free-rider' problem, particularly because of the high suspected costs of implementing these high-tech solutions. Overall, a key issue for the EU to consider should be the uniform implementation across all member states of the global CFT standards endorsed by the international community; as the aforementioned discussion regarding prepaid cards indicates, the success of terrorists in financing their operations is likely to be determined by "the weakest link in the international cooperation frameworks" (Bures, 2015: 209).

The effectiveness of the EU's efforts has been historically difficult to measure; indeed, the EU Commission has itself claimed that "it is rather difficult to establish whether the aforementioned measures have had 'a significant impact on terrorists' ability to carry out attacks'" (Ibid: 224). The reasoning behind this is that each of the candidates which could be used as the criteria for success are imperfect measurements. Firstly, the amount of terrorist funds frozen cannot be used as a proxy for success; on one hand, a high value of frozen assets could nevertheless coexist with the fact that several terrorist attacks – such as the 2004 Madrid bombings–have been carried out using small sums of money which would not have been frozen under existing legislation. Inversely, a lack of frozen funds might imply that terrorists have shifted their focus away from formal financial institutions towards transferring their proceeds using informal channels. The quantity of STRs filed by financial and non-financial institutions is another misleading barometer of success. One of the key themes of the recent literature is the lack of public-private sector communication regarding the exact AML/CFT measures that private institutions must follow. Due to their lack of knowledge regarding the exact measures they must implement, and because of the heavy penalties they face for non-compliance, private actors tend to file an excessive amount of STRs. Therefore, a high amount of STRs does not necessarily indicate any sort of success; on the contrary, the dilution of legitimate and frivolous reports increases the difficulties faced by FIUs in determining which transactions pose a serious threat (Bures, 2012). Indeed, evidence suggests that the number of STRs resulting in TF prosecutions are negligible at best, and that most terrorist financing investigations come to light during unrelated investigations.

The United States

A key branch of US CFT regulations stems from the pre-9/11 US sanctions regime. The 1977 International Emergency Economic Powers Act enabled the Treasury to place financial sanctions on nations which threatened US national interests, freezing their assets and thus impeding them from using the international financial system. The 1996 'Anti-terrorism and Effective Death Penalty Act' expanded the targets of these sanctions to include terrorist groups and their financial supporters. However, Eckert claims that until the 9/11 attacks, these asset freezing measures were a "little known and understood tool of policy-makers" which had effectively "done little or nothing against terrorist financing" due to the low priority placed upon financial intelligence gathering by the US government (Eckert, 2008: 214). This changed after 9/11 with the issuance of Executive Order 13224, which greatly expanded the US Treasury's ability to strategically freeze the assets of terrorist organisations and their financiers, whist prohibiting US individuals from transacting with these designated parties. Ryder (2015) estimates that $135m worth of assets have been frozen from the bank accounts of approximately 1439 suspected terrorists as a result of this order (Ryder, 2015: 82). Despite this, several authors question the effectiveness of the US sanctions regime in combatting TF; firstly, evidence shows that the rate of asset freezes greatly diminished following the first months after 9/11 (Ibid). Furthermore, Eckert (2008) notes that the "evidentiary foundations" (p.215) for several designations were "quite weak" (p.215), and that many terrorism charges were dismissed due to a lack of evidence. Most crucially, terrorists have perfected other means of transferring funds without the use of the formal financial system.

Another regulation that has garnered much attention is the 2001 USA PATRIOT Act, which greatly enhanced the administrative CFT burden placed on both formal and informal financial institutions. This act required them to enact know your customer mechanisms and establish minimum due diligence procedures, while empowering the Treasury to sanction foreign FIs if they are suspected of having participated in ML/TF. The PATRIOT Act also facilitated increased sharing of financial intelligence between the public and private sectors regarding suspicious individuals. Despite these overarching measures, however, there are several reasons to doubt the effectiveness of the PATRIOT Act in curbing the transfer of terrorist funds. Primary among these is the difficulties of AML measures such as the PATRIOT Act to take into account the differences between the mechanisms involved in money laundering versus terrorist financing. As a result, several authors have called for alternative measures for focusing on CFT apart from the AML extensions which have hitherto been adopted (Ibid). One potential flaw is the high minimum requirement for currency transaction report (CTR) filings, which has led many to suggest that terrorists could simply break up their transactions into several smaller increments in order to evade these measures (Ibid). Moreover,–similarly to the European situation outlined above – various authors point to the failed communication between the private and public sectors as a key factor in the failure of CFT efforts (Ibid). Revealingly, Ryder (2015) and Bures (2012) both claim that 9/11 would not have been prevented even if these new regulations had been in place, while Ryder (2015) notes that these measures did not prevent the 2013 Boston Marathon terrorist attacks from occurring. Finally, new technologies such as cryptocurrencies and prepaid cards also threaten to allow terrorists to circumvent many of the existing AML/CFT provisions.

As per Cohen (2014), the US is implementing a three-pronged strategy to counter ISIS's financial network. Firstly, the Islamic State's access to the international financial system has been slowed due to a ban on wire transfers to and from bank branches within ISIS-held territory in Iraq, while banks in Syria have been subject to harsh reporting requirements. This tactic possesses several limitations; firstly – as Bahney and Johnston (2014) state – the weakness of the current Iraqi government potentially precludes the effective enforcement

of this ban. Furthermore, this strategy does not take into account alternative, 'emerging' transfer methods that ISIS could employ which are more difficult for authorities to monitor and regulate. Secondly, the US are working with Kurdish and Iraqi forces to proverbially strike ISIS at their core and disrupt the revenue gained from their sources of funding. This has involved coalition airstrikes against ISIS oil refineries, which have already proved successful in reducing oil extraction rates and revenues, particularly in Syria (Humud, Pirog, and Rosen, 2015). However, the impact of these airstrikes in Iraq has been tempered by the necessity of retaining vital oil infrastructure in order to repower the region once the government regains control (Bahney and Johnston, 2014). On a broader note, US efforts to tackle ISIS's sources of funding will never succeed without military intervention given the inescapable link between ISIS's territorial possessions and their fundraising capabilities. The US Treasury (2014) has indeed claimed that their methods are "not particularly suited to this task", and that military engagement is a necessity if the international community wishes to scale back ISIS's fundraising operations. The final weapon in America's arsenal is targeted sanctions against ISIS operators and foreign financiers. Although these donations currently constitute only 5% of ISIS revenues, the following hypothesis suggests that in the long run, these donations will grow in importance as the economic and military capacity of ISIS both decline precipitously.

The Importance of Military Action in CFT Efforts

Military force is crucial to financially crippling ISIS in the long run. The core of ISIS revenues have been derived from the selling of petroleum-based products. However, numerous factors are contributing to the decreased revenues ISIS have been able to glean from this funding source; firstly, ISIS have been unable to repair extraction infrastructure due to a lack of skilled technicians within ISIS territory. Indeed, data has shown that the productivity of oil extraction has been markedly decreasing since March 2012 (Lewis and Shapiro, 2015: 144). Rapidly declining oil prices along with coalition airstrikes have also reduced potential revenue streams. All in all, oil revenues and production possibilities are low in the long run. Moreover, ISIS's economic policies – or lack thereof – have been criticized as not being conducive to long-run growth; the excessive taxes on cash withdrawals, agriculture machinery, and fuel are typically modelled as reducing consumer incentives to save and invest, imperilling long-run growth. The lack of access to credit and private insurance markets is likely to discourage entrepreneurship, while ISIS's lack of human capital investment in the form of education and healthcare will also reduce long-term labour productivity and growth (Ibid). ISIS's long-run military prospects are also expected to be bleak. Luminosity data indicates that ISIS GDP equalled approximately $30bn in 2014 (Ibid: 148). However, Iraqi and Saudi defence spending in 2014 totalled $80bn and $9.5bn respectively – far beyond what ISIS can realistically afford (Ibid: 148). This disparity is likely to increase given ISIS's aforementioned economic difficulties. ISIS will therefore be unable to territorially expand, trapping the organisation in an area with diminishing resources. This will increase its reliance on foreign donors, enabling the international community – and especially the US Treasury – to use its sanctions regime to thwart the transfer of these funds and proverbially starve ISIS out. This long-run outlook crystallises the inextricable link between financial and military measures necessary for defunding ISIS. Evidence suggests that military action is already depleting ISIS's financial portfolio; in January 2016 it was widely reported by news outlets that ISIS had reduced their fighters' salaries by 50% as a result of coalition airstrikes (Pagliery, 2016). It is therefore essential that nations continue to coordinate military manoeuvres and share military intelligence in order to "degrade and ultimately destroy ISIL" (Obama, 2014).

Final Thoughts

The 9/11 attacks moved terrorist financing to the forefront of global counter-terrorism efforts, as has been reflected by the innumerable strides that have made on both the national and international stages to combat TF. The FATF and the UN have been the key standard-setters with regards to CFT legislation, and the EU and the US have diligently attempted to transpose these standards into law in addition to crafting their own unique legislation to deal with this perilous threat. Despite this, several factors have conspired to thwart significant progress; for instance, the lack of communication between the private and public sectors with regards to compliance requirements has inhibited the effectiveness of increased financial sector regulations in halting the transfer of terrorist funds. Moreover, the efficacy of current regulations has been notoriously difficult to gauge due to the inadequacies of several potential proxies for success. Most importantly, tools that have hitherto been indispensable in the fight against terrorist financing are unlikely to feature as prominently against the Islamic State due to (a) the unique nature of ISIS's fundraising streams and (b) ISIS's recent shift away from traditional transfer methods in favour of 'emerging' technologies such as cryptocurrencies. It is therefore essential that nations enact legislative measures to ensure that these novel technologies are not exploited for nefarious purposes. It is also paramount that the US and EU continue to share financial and military intelligence with local forces on the ground in order to continue choking off the Islamic State's fundraising potential, in addition to cooperating on military ventures to accelerate the group's long-run decline. Overall, although CFT measures have rapidly advanced since 2001, more must be done to effectively drain the financial resources of terrorist organisations and limit their ability to wage war on their victims.

Acknowledgements

I would like to thank my supervisor Dr. William Vlcek for giving me the crucial advice and inspiration that I needed to pursue this paper. The scholarship provided by Lord Laidlaw – which allowed me to pursue the Laidlaw Undergraduate Internship in Research and Leadership – also proved invaluable.

About the author

Alessio Shostak *is a fourth-year undergraduate student studying Economics at the University of St Andrews in Scotland. He has lived a relatively nomadic lifestyle, having residing in several nations including Australia, Switzerland, and Italy.*

References

Bahney, Benjamin and Johnston, Patrick (2014), "Hitting ISIS Where it Hurts: Disrupting ISIS's Cash Flow in Iraq", RAND Corporation, [online] August 13, 2014. Available at: <http://www.rand.org/blog/2014/08/hitting-isis-where-it-hurts-disrupt-isiss-cash-flow.html>

Berti, Bernadetta (2008), "The Economics of Counterterrorism: Devising a Normative Regulatory Framework for the Hawala System', *MIT International Review*, Spring Issue 2008, pp.14-21

Biersteker, Thomas and Eckert, Sue, 'Introduction: The Challenge of Terrorist Financing' in Thomas J. Biersteker, Thomas and Eckert, Sue (eds.), *Countering the Financing of Terrorism* (New York 2008)

Biersteker, Thomas, Eckert, Sue and Romaniuk, Peter, 'International Initiatives to Combat the Financing of Terrorism' in Thomas J. Biersteker & Sue E. Eckert (eds.), *Countering the Financing of Terrorism* (New York 2008)

Bures, Aldrich (2012), "Private Actors in the Fight Against Terrorist Financing: Efficiency versus Effectiveness", *Studies in Conflict and Terrorism*, 35(10), pp.712-732

Bures, Oldrich (2015), "Ten Years of EU's Fight against Terrorist Financing: A Critical Assessment", *Intelligence and National Security*, 30(2-3), pp.207-233

Clunan, Anne (2006), "The Fight Against Terrorist Financing", *Political Science Quarterly*, 121(4), pp.569-596

Cronin, Audrey Kurth (2015), "ISIS Is Not a Terrorist Group: Why Counterterrorism Won't Stop the Latest Jihadi Threat", *Foreign Affairs,* [online] March/February 2015. Available at: <https://www.foreignaffairs.com/articles/middle-east/isis-not-terrorist-group>

Eckert, Sue (2008), 'The US Regulatory Approach to Terrorist Financing' in Biersteker, Thomas & Eckert, Sue (eds.), *Countering the Financing of Terrorism* (New York 2008)

FATF (2001), "FATF IX Special Reccommendations", FATF, [pdf] October 2011. Available at: <http://www.fatf gafi.org/media/fatf/documents/reports/FATF%20Standards%20-%20IX%20Special%20Recommendations%20and%20IN%20rc.pdf>

FATF (2014), Virtual Currencies: Key Definitions and Potential AML/CFT Risks, FATF, [pdf] June 2014. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>

FATF (2015), Emerging Terrorist Financing Risks, FATF, [pdf] October 2015. Available at: http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf

FATF (2015), Financing of the terrorist organisation Islamic State in Iraq and the Levant (ISIL), FATF, [pdf] February 2015. Available at: < http://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf>

Fowler, Jennifer (2015). U.S. Efforts to Counter the Financing of ISIL. In: Washington Institute for Near East Policy. *Taking the Fight to ISIL: Operationalizing CT Lines of Effort Against the Islamic State Group*. Washington D.C., United States of America. February 2, 2015.

Gilmore, William and Mitsilegas, Valsamis (2007), "The EU Legislative Framework against Money Laundering and Terrorist Finance: A Critical Analysis in the Light of Evolving Global Standards", *International and Comparative Law Quarterly*, 56(1), pp.119-140

Gomez, Juan Miguel Del Cid (2010), "A Financial Profile of the Terrorism of Al Qaeda and its Affiliates", *Perspectives on Terrorism*, 4(4), pp.3-28

Humud, Carla, Pirog, Robert and Rosen, Liana (2015), "Islamic State Financing and U.S. Policy Approaches", Congressional Research Service, [pdf] April 10, 2015. Available at: <https://www.fas.org/sgp/crs/terror/R43980.pdf>

IMF (2016), Virtual Currencies: Initial Considerations and Beyond, IMF, [pdf] January 2016. Available at: <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>

Johnson, Keith (2014), "Has the U.S. Turned Off the Islamic State's Oil Spigot?", *Foreign Policy,* [online] October 7, 2014. Available at: <http://foreignpolicy.com/2014/10/07/has-the-u-s-turned-off-the-islamic-states-oil-spigot/ >

Kim-Kwang, Raymond Choo (2008), "Money Laundering and Terrorism Financing Risks of Prepaid Cards Instruments?", *Journal of Asian Criminology*, 4(1), pp.11-30

Levitt, Matthew 'Terrorist financing and Islamic State – Testimony submitted to the House of Committee on Financial Services', [online] November 13 2014. Available at: <http://www.washingtoninstitute.org/policyanalysis/view/terrorist-financing-and-the-islamic-state>

Lewis, Jamie Hansen and Shapiro, Jacob (2015), "Understanding the Daesh Economy", *Perspectives on Terrorism*, 9(4), pp.142-155

Obama, Barack H. (2014), *Statement by the President on ISIL*, [press release] September 10, 2014. Available at: <https://www.whitehouse.gov/the-press-office/2014/09/10/statement-president-isil-1>

Pagliery, Jose (2016), ISIS Cuts its Fighters Salaries by 50%, *CNN Money,* [online] January 19, 2016. Available at: <*http://money.cnn.com/2016/01/19/news/world/isis-salary-cuts/*>

Raphaeli, Nimrod (2003), "Financing of Terrorism: Sources, Methods and Channels", *Journal of Terrorism and Political Violence,* 15(4), pp.59-82

Ryder, Nicholas (2015) *The Financial War on Terror: A Review of Counter-Terrorist Financing Strategies since 2001*, London: Routledge

Stergiou, Dimitros (2016), "ISIS Political Economy: Financing a Terror State", *Journal of Money Laundering Control,* 19(2), pp.189-207

The European Commission (2016), "Communication Plan from the Commission to the European Parliament and the Council: on an Action Plan for strengthening the fight against terrorist financing", The European Commission, [pdf] February 2016. Available at: <http://ec.europa.eu/justice/criminal/files/com_2016_50_en.pdf>

United States Department of the Treasury 2014, *Remarks of Under Secretary for Terrorism and Financial Intelligence David S. Cohen at The Carnegie Endowment for International Peace, 'Attacking ISIS's Financial Foundation,* [press release] March 4, 2014. Available at: <https://www.treasury.gov/press-center/press-releases/Pages/jl2308.aspx>