International Institutions: An Underutilized Tool for Combating the Financing of Terrorism

Cody Wilson

Northeastern University

Abstract:

During the 1980s, the pace of globalization increased dramatically. The world shrunk in size as companies opened up factories in other countries, new trade agreements went into effect, and global prosperity was promised for all. The world continued shrinking in the 1990s when the Internet sped up the forces of globalization even more. However, globalization also mobilized backlash in the form of radical fundamentalist groups like Al-Qaeda. Over the last thirty years, Al-Qaeda globalized as well. Today, it has affiliates in dozens of countries, and it has used the infrastructure built by the forces of globalization to create a worldwide financing network. This network takes advantage of the international banking system, informal remittances, donations, and more. Since the 9/11 attacks, national governments and their regional partners have tried to combat the financing of terrorism, but Al-Qaeda has simply altered its financing strategy to circumvent these measures. The limited cooperation at the international level has allowed Al-Qaeda to continue raising millions of dollars per year, and emerging technologies have gotten Al-Qaeda's attention as a further source of funding, planning, and communication. These globally connected technologies now threaten to allow Al-Qaeda and others to "go dark" while expanding their financial resources as national and regional governments try to play catch up. Analysis of Al-Qaeda's financing network highlights why national and regional approaches to combating the financing of terrorism are inadequate and must be done in conjunction with international institutions.

Keywords: al-Qaeda, terrorist financing, anti-money laundering, CFT

Introduction

Between 1998 and 2005, the terrorist group Al-Qaeda carried out eight mass casualty attacks that collectively cost thousands of lives and billions of dollars in damages, yet the total expense of these attacks was estimated at just over $800,000 (del Cid Gómez, 2010). Disturbingly, during this same period Al-Qaeda was raising an estimated $30 million annually as governments haphazardly scrambled to curb terrorist financing. How did Al-Qaeda develop such a robust financial network? When Benjamin Barber wrote *Jihad vs. McWorld* in 1995, he argued there would be fundamentalist backlash to globalization (Barber, 1995). He perhaps did not imagine that when it manifested this backlash would be using globalization as a weapon. Indeed, terrorist networks all over the world are taking advantage of interconnected financial systems, trade networks, and the Internet to diffuse their fundraising channels in order to make them more robust and effective. This shift has meant that efforts to curb terrorist financing, which have mostly been done at the national and regional level, are becoming increasingly ineffective. The elusive nature of Al-Qaeda's financial network highlights why more focus must be placed on empowering international institutions with more regulatory authority aimed at combating the financing of terrorism.

Theoretical Overview

While global trade has existed for at least a millennia, the modern day liberal order did not exist until 1944 with the creation of the Bretton Woods system. Yet it was the rise of neoliberalism in the 1980s that shifted globalization into high gear with market deregulation, privatization of industries, and a heavy focus on trade liberalization (Chomsky, 1999). The ideas of neoliberalism were enshrined in policy by officials at the U.S. Treasury, the World Bank, and the International Monetary Fund (IMF) in what would be called the "Washington Consensus."

The IMF, World Bank, and World Trade Organization (WTO) were empowered to help spread the neoliberal ideal throughout the global market. The form of capitalism described by Benjamin Barber that prompted such tribal fundamentalist backlash is built upon this neoliberal tradition.

One of the core tenants of neoliberalism is market self-regulation. Buthe and Mattli have identified four types of regulatory rule-making (Buthe & Mattli, 2011). Market self-regulation constitutes type three regulation: private, market-based rules set by private industry itself. Governments make anti-money laundering (AML) rules but often expect them to be enforced by banks using this type three regulation. Type two regulation, public market-based rules, are competing rules set by national or regional governments. AML laws themselves and asset freezes are enforced by governments like the U.S. and regional bodies like the E.U. in this way. Type four regulation, private nonmarket-based rules, are set by non-governmental organizations. Possible Internet regulation over cryptocurrency and the dark web could be enforced this way through the World Wide Web Consortium and other non-governmental organizations. It is type one regulation, public nonmarket-based rules, however, that could be most effective in Combating the Financing of Terrorism (CFT) at the international level. The Financial Action Task Force (FATF) is one of the international regulatory bodies created to disrupt terrorist financing; however, its powers are quite limited. The FATF cannot disrupt terrorist financing alone. Amartya Sen, Robert Keohane, and Bruce R. Scott all argue that properly administered international institutions can be used to solve global challenges like poverty and climate change (Sen, 2002; Keohane, 1998; Scott, 2001). International rule setting is the mechanism for overcoming these global challenges, and it can be used to close loopholes through superseding regulation and apply international pressure on a persistent international problem like terrorist financing as well.

Methodology

In order to properly highlight the inadequacy of the current national and regional focus of CFT efforts, this project presents a deeper look at Al-Qaeda's complex financing network and how it has evolved to circumvent CFT counter-measures. The findings below draw upon the extant literature on terrorist financing, financial crimes datasets, federal indictments, Congressional testimony, as well as governmental and intergovernmental reports. For the purposes of these findings, Al-Qaeda will refer exclusively to the central group led and organized by Ayman al-Zawahiri and, formerly, Osama bin Laden. Loosely affiliated offshoots and splinter groups like Syrian-based Hay'at Tahrir al-Sham are not included in the discussion of Al-Qaeda.

Al-Qaeda's Financial Network

It is a myth that Osama bin Laden single-handedly funded Al-Qaeda (9/11 Commission, 2004). Osama bin Laden's money certainly got Al-Qaeda started, but it was a sophisticated financial network with multiple revenue streams that allowed the group to begin raising millions of dollars per year. Al-Qaeda's financial network can be sub-divided into four distinct domains. For the sake of unity, each domain has been identified as its own "economy." They are: the Traditional Economy, the Grey Economy, the Dark Economy, and the Cyber Economy.

The Traditional Economy

The Traditional Economy is the part of Al-Qaeda's financial network that focuses on exploitation of the international and Islamic banking systems as well as legitimate and illegitimate business operations. Since 9/11, most CFT efforts have revolved around disrupting this economy. However, the implementation of existing policies leaves many loopholes available for exploitation.

Before 9/11 the leadership of Al-Qaeda did not place much trust in the international banking system. However, offshore bank accounts and banking secrecy allowed their supporters to funnel money to the organization effectively and without raising suspicion until it was already too late (Stiglitz, 2004). Despite Al-Qaeda's preference for other forms of financing, their money eventually returns to the formal financial system in the lead up to an attack, so the robustness of these CFT policies, which serve as a last line of defense before would-be attackers withdraw money from their accounts, is imperative (U.S. House of Representatives, 2016). The U.S. and E.U. have frozen Al-Qaeda assets in their own jurisdictions, and organizations like the FATF have recommended that their 37 signatories follow suit (Financial Action Task Force, 2017). However, the global deregulation of the financial sector has allowed terrorist capital to enter into the market through other channels (Basile, 2004). Al-Qaeda has adopted a variety of methods to move money in and out of the financial sector, these include: bribing bank officials, opening accounts at deregulated offshore Central Banks, using financiers not known to governments and banks, opening accounts under stolen identities, as well as using correspondent banking, wire transfers, and shell companies (Clarke, 2015; U.S. House of Representatives, 2012).

When the international banking system fails to produce results, Al-Qaeda relies on the Islamic banking system. Islamic banks operate under *sharia* law, do not allow interest to be earned, are found around the world, and are heavily integrated into the formal financial sector (Zulkhibri, 2016). Profits and interest at these banks must be used for internal projects only; however, these funds have, at times, disappeared into suspicious client accounts due to a lack of oversight in the distribution of these funds in some cases and simple corruption in other cases. Additionally, because the banks are integrated into the global financial market, Al-Qaeda uses

Islamic banks to move funds around the world before using correspondent banking to transfer these funds back into the formal financial sector (Basile, 2004).

Lastly, Al-Qaeda and its supporters have raised funds through both legitimate and illegitimate businesses. Following the model of multinational corporations, Al-Qaeda uses a network of legitimate companies in a variety of industries in an estimated 40 countries around the world to funnel business profits into their terrorist operations (Clarke, 2015). Many of these businesses are intermingled with illegitimate front businesses to make detection more difficult. One such front business was the Benevolence International Foundation (BIF). Enaam Arnaout established this fake charity organization, which was located in the U.S. but had offices around the world, to buy equipment for Al-Qaeda as well as funnel $1.4 million through a Swiss bank account to the group (*United States v. Arnaout*, 2002). The front was so good that Microsoft, U.P.S., and Hewlett Packard allegedly donated to BIF before Arnaout's arrest (Raphaeli, 2003).

The Grey Economy

The Grey Economy is the part of Al-Qaeda's financial network that focuses on exploitation of donations, informal remittances, money laundering, and fraud. Current CFT policies focus heavily upon disrupting money laundering and fraud. However, the current national and regional approach does nothing to disrupt donations or remittances. In fact, one primary form of funding is donation from state sponsors. Without international pressure, it is highly unlikely that this potent form of financing will dry up.

Charitable donations constitute a major revenue stream for Al-Qaeda. In Islam, *zakat* is an annual obligatory donation of 2.5% of an individual's wealth (del Cid Gómez, 2010). In some cases, sympathetic individuals choose Al-Qaeda as their *zakat* recipient and donate through the Internet (MEMRI Cyber & Jihad Lab, 2015). However, it is more common for these individuals

to contribute *zakat* through charitable organizations or non-profits. The vast majority of non-profit organizations are legitimate; however, groups like the International Islamic Relief Organization give money to Al-Qaeda overtly along with the Saudi-based Al Haraman Islamic Foundation (Clarke, 2015). Other groups like Lajnat al Daawa Al Islamiya have been linked to Al-Qaeda but also provide legitimate services. Worldwide, non-profits receive $1.3 trillion annually, so even a small fraction of that could provide a great deal of funding to groups like Al-Qaeda (van de Does de Willebois, 2010). Perhaps the most potent form of *zakat* is that from wealthy donors and government officials in the Gulf States which have reliably provided Al-Qaeda with millions of dollars per year (Soufan, 2017). Even when Saudi Prince Mohammed bin Nayyef outlawed donations from Saudis patrons, neighboring Qataris and Emiratis continued to donate several million dollars per year (Levitt & Bauer, 2017).

In parts of the world where the international banking system has not yet established itself, informal transactions and money service businesses take place between individuals without regulation or oversight. These remittance transactions are known as *hawala*, and *hawaladars,* or *hawala* dealers, have played a large part in allowing Al-Qaeda to move money discreetly (9/11 Commission, 2004). A client simply approaches a *hawaladar* with money he or she wishes to transfer elsewhere. The *hawaladar* takes the money, calls another *hawaladar* at the money's destination, and instructs that *hawaladar* to dispense the money to the client's intended recipient, minus a transaction fee. Often these transactions take place without any record of their existence which makes them very hard to regulate or stop. It is estimated that in South Asia, the black market fueled by *hawala* is 30-50% the size of the regular economy (U.S. Department of Treasury, 2010).

Prevention of money laundering and fraud is the primary focus of current CFT efforts. It is estimated that as much as ten percent of global GDP is laundered money (Reuter & Truman, 2004). Cooperation between the U.S. and E.U. has drastically cut down on traditional money laundering efforts (Kingah & Zwartjes, 2015). However, without a unified policy on AML, banks often must enforce regulations themselves, and this is done at the expense of effectiveness in favor of efficiency (Bures, 2012). Additionally, Al-Qaeda has shifted into trade based money laundering focused around used cars and consumer goods to get around stronger banking scrutiny, but it is unclear how much money this method has generated the group (U.S. House of Representatives, 2016). A different tactic of Al-Qaeda is to commit bank fraud by acquiring loans and credit cards, quickly spending the money, and then defaulting on the payments (Clarke, 2015). Other tactics include stealing credit card information, stealing identities, and committing tax fraud.

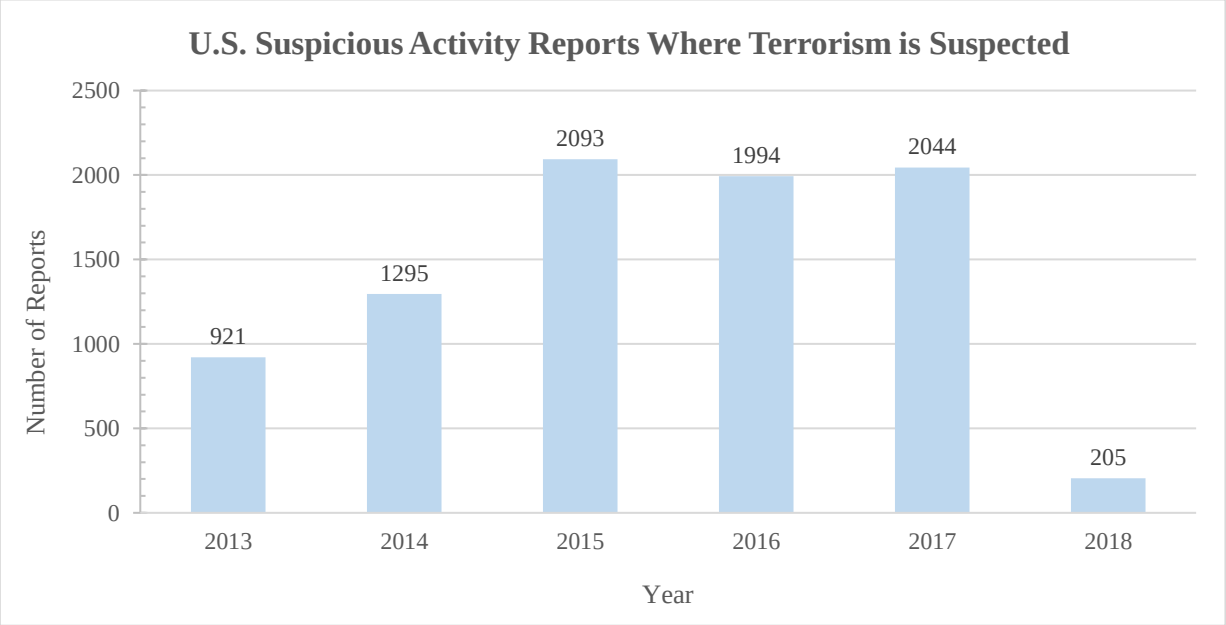

Figure 1. *Suspicious Activity Reports filed with the Financial Crime Enforcement Network from 2013 to present. Data: U.S. Department of the Treasury. (2018). "Suspicious Activity Report Statistics". Retrieved from https://www.fincen.gov/reports/sar-stats. Graph: Cody Wilson.*

Much of the resulting anti-fraud and money laundering measures have increased due diligence standards for banks. Figure 1 shows the number of suspicious activity reports relating to terrorism that U.S. banks filed with the Financial Crime Enforcement Network of the U.S. Department of the Treasury between 2013 and 2018. There are 8,552 cases thus far. Table 1 at the end of the paper shows the full break down of the data by industry and type of activity reported.

The Dark Economy

The Dark Economy is the part of Al-Qaeda's financial network that focuses on exploitation of ransoms from kidnapping, smuggling and trafficking, as well as partnering with organized crime syndicates. Due to the focus of current CFT policies on Traditional and Grey Economy activities, Al-Qaeda has increasingly turned toward this economy to evade disruption. This is an area where even robust international regulation may struggle to be effective.

Kidnapping for ransom (KFR) has been one of the most powerful tools for Al-Qaeda's financing efforts in the post-9/11 world. In fact, both U.N. and U.S. officials have identified ransoms as "the main source of funding for al-Qaeda-related groups in Yemen and North Africa, and as an important source of funding for such groups in Syria and Iraq" (Weinberg, 2015). Between 2008 and 2014, Al-Qaeda was paid $125 million in ransoms from kidnappings. Just a single ransom can make the group millions of dollars. In 2014, the Italian government reportedly paid almost $14 million for the return of two Italian aid workers (Keatinge, 2015). Military efforts have been made to rescue hostages; however, these efforts have had mixed success which means KFR will remain a potent financing tool going forward.

One of the side effects of pushing terrorists deeper underground is that they must engage in more traditional criminal behavior in order to raise funds. As such, Al-Qaeda has expanded

into counterfeiting, smuggling, and trafficking. In the Middle East, selling counterfeit goods represents a low risk-high reward arrangement as fines and prison sentences are small, yet profits can be very high. Counterfeiting costs intellectual property rights holders an estimated $200-250 billion per year worldwide (Raphaeli, 2003). Additionally, Al-Qaeda engages in the trafficking of antiquities looted from conflict zones as well as valuable materials such as gold, diamonds, and other precious gems, often purchased from corrupt governments in Africa (Weinberg, 2015; Clarke, 2015; Raphaeli, 2003). Al-Qaeda is estimated to have invested between $20-50 million in the trafficking of these goods, especially so-called blood diamonds. Meanwhile, the smuggling of hundreds of cartons of cigarettes from tax-free locations to other countries can generate the group upwards of $500,000 per week (University of Maryland, 2014).

There has been much debate over the past few decades about convergence between terrorist groups and organized crime syndicates; however, the evidence seems to suggest that groups like Al-Qaeda are working with and adopting tactics from the world of organized crime. Due to CFT measures, terrorist groups are becoming more reliant on the illicit networks and drug markets built by criminal organizations (Picarelli, 2012). This change has also meant that when the crime-terror nexus forms, the relationship is longer lasting due to more overlap in the threat environment to both groups. A 2009 arrest of three Al-Qaeda operatives by the U.S. Drug Enforcement Administration confirmed that Al-Qaeda had indeed branched into using organized crime for its financing. The three men were charged with conspiring to smuggle several hundred kilograms of cocaine from North Africa into Colombia to be sold by the FARC and local drug cartels (*United States v. Issa, et al.,* 2009).

The Cyber Economy

The Cyber Economy is the emerging part of Al-Qaeda's financial network that focuses on exploitation of the dark web and online black markets, as well as virtual currency. Due to its distributed nature, the Internet has increasingly been a tool of financing because it is inherently difficult to disrupt with current CFT efforts. However, this is an area where even type one governmental regulation may struggle, but it is possible type four regulation by international, Internet-focused nongovernmental organizations could prove effective against this economy.

The forces of globalization brought the world much closer together, but with the rise of the Internet in the 1990s the world truly flattened, and Thomas Friedman's technology driven "Globalization 3.0" began (Friedman, 2005). The diffuse, almost unregulated nature of the Internet has been of interest to Al-Qaeda since as far back as the early 2000s, but recent technological advances are making it possible to interact on the Internet with relative anonymity. This problem has more recently taken the name "Going Dark" as more Internet traffic becomes encrypted. Some government efforts have been aimed at taking down terrorist websites; however, groups like Al-Qaeda have increasingly moved to the so-called dark web.

The deep web and dark web refer to parts of the Internet that are not indexed by search engines. The dark web is a segment of the deep web that can only be accessed through The Onion Router (TOR) or Invisible Internet Project (I2P) software designed to anonymize web traffic by moving through multiple servers or nodes (Weimann, 2016). The websites on the dark web often contain illegal material and are inaccessible unless an individual knows the actual address of the website. A vast number of traditional websites still host terrorist material because many followers may not know how to operate on the dark web. However, the dark web allows Al-Qaeda access to many advantages including online black markets where they can sell illicit materials like opium or buy supplies for attacks, hidden online forums for planning operations,

marketplaces to sell jihadist literature and other paraphernalia, and an even more diffuse network of *zakat* contributions (Weimann, 2016; Rudner, 2017).

One of the primary ways that money changes hands on the dark web is through virtual currency, like Bitcoin, sometimes referred to as crypto-currency due to the cryptographic "block-chain" algorithm that allows the currency to be generated through "mining" which is, put simply, the computational factoring of increasingly complex prime numbers. The creation of Bitcoin exchanges and Bitcoin ATMs that allow real money to be converted into Bitcoin and visa-versa threaten the current CFT and AML regulatory frameworks because money can now be laundered through these new currencies and used to purchase goods and services through online black markets on the dark web (Salami, 2017). In 2017, there was an estimated $8 billion of Bitcoin in existence, but that number fluctuates quite dramatically as value of the currency has not settled (Vovchenko, Tishchenko, Epifanova, Gontmacher, 2017). Due to the growth of Dark Wallets that anonymize crypto-currency transactions and the fact that new currencies are emerging almost weekly, it is unclear how much virtual currency Al-Qaeda is seeking out or has acquired. However, activities by the once allied Islamic State may provide clues, and evidence strongly suggests that the Islamic State has already used Bitcoin to partially fund attacks in Europe and Indonesia (Irwin & Milad, 2016). Additionally, a New York woman was indicted in December 2017 for allegedly defrauding over $85,000 from financial institutions before laundering the money via Bitcoin and transferring it to a Bitcoin wallet operated by the Islamic State (*United States v. Shahnaz*, 2017).

Policy Considerations

Much of the existing CFT framework operates through a combination of type two and type three regulation, that is, at the national and regional level as well as the private enterprise

level. The participants and stakeholders of current CFT efforts have disproportionately been the U.S. and Europe and the companies which operate in their jurisdictions. Strong AML rules are set at both the national and regional levels by the U.S. and E.U., but often day to day compliance enforcement falls to the banks themselves. The banks, however, are under pressure to keep costs low, so they prioritize efficiently implementing AML rules instead of effectively implementing them (Bures, 2012). This means that while 8,552 reports of suspicious activity have been caught in recent years it is highly likely that there are thousands more that are missed due the focus on profits not security. Essentially, implementation of type two regulation at the type three level often means that the banks have neither the resources nor the motivation to effectively counter terrorist financing. Even when banks do their due diligence, however, the lack of a global AML policy, as well as other CFT policies, means that money can just enter the financial sector through other channels. In effect, the national and regional approach is just like playing a very dangerous game of "Whac-A-Mole" where Al-Qaeda just relocates to an area with less regulation. The lead taken by the West has also made other possible partners less likely to assist in these efforts due to suspicion over the West's motives, so a stronger international focus emphasizing collective cooperation will be less likely to be interpreted as interference and bullying by the West.

As has been alluded to in the sections above, certain financing economies would be more hard hit by effective international institutions than others. The Dark Economy, for example, relies mostly on criminal activity which is, of course, hard to disrupt and immune to regulation. However, international institutions can at least apply pressure on domestic governments to not give carte blanche to such activity and provide these governments assistance when necessary. Furthermore, some major donors to terrorist groups are states themselves. If the WTO

approached combating terrorist financing with as much vigor as it approaches enshrining neoliberalism, it could much more effectively pressure state sponsors like Saudi Arabia and Qatar to stop trading in terrorist funding by perhaps threatening to cut off access to their sale of oil in global markets. The U.S. could not apply such leverage without damaging its relationship with these countries, but the WTO has proven time and again that it cares little about its political capital. This makes an international institution much more of an ideal candidate for such pressure.

There are, of course, challenges that must be overcome in expanding CFT efforts at the international level. One primary challenge that the U.N. has faced is definitional – some U.N. members disagree over the definition of terrorism. The cliché "one person's terrorist is another person's freedom fighter" seems to hold true for these member states, so many discussions have been halted in their infancy. Another major challenge is overcoming the "markets know best" orthodoxy of neoliberalism itself. The grip of neoliberalism was loosened in the realm of CFT after it was discovered that deregulation and banking secrecy helped Al-Qaeda fund the 9/11 attacks. However, the focus on deregulation still lingers today. Hopefully, effective international policies will win out over neoliberal ideals on merit alone before another catastrophic attack forces change, but it seems doubtful. As such, this international focus will hopefully serve as the starting point for when policy change is demanded in response to another catastrophe.

Another challenge is how to use international institutions to limit terrorist financing in culturally sensitive areas without imposing a heavy handed approach which could further serve as a tool of terrorist recruitment. In particular, imposing type one regulation over the Islamic banking system and *hawala* must be done delicately since much of the Middle East and South Asia rely on these two forms of transaction for day to day life. Perhaps international institutions

could work with their national and regional partners in more of an organizational or advisory capacity to tailor specific regulations over these transactions. Lastly, the Internet is another challenging area where perhaps type four regulatory standards may be best suited. Most of the Internet's infrastructure and protocols are already decided at this level, so debate at the World Wide Web Consortium about CFT protocols seems much less likely to stoke public backlash, like that seen over Net Neutrality, than if type one, two, or three regulation were used.

Conclusion

The goal of counterterrorism is not to prevent all terrorist attacks; its goal is to make attacks increasingly difficult to carry out. The goal of CFT is similar. It is impossible to disrupt funding entirely, so the aim is to make it as challenging and risky as possible for terrorist groups to finance themselves. Kidnapping for a ransom is dangerous and difficult for the amount of pay received; however, soliciting *zakat*, using *hawaladars*, the Islamic banking system, and the Internet is not dangerous or difficult. These areas represent gaps left by the national and regional focus of CFT. Policies at the national and regional level have had some impact, but it matters very little if terrorist groups can circumvent the policies without a lot of effort. Can all of these financing channels be eliminated by a stronger international focus? No. However, the goal of CFT and counterterrorism remains to increase the costs and risks of operating so as to dissuade the tactic of terrorism. A layered approach where national, regional, and international regulators work together, rather than separately, can more effectively dissuade terrorism by closing off more financing channels. Challenges will still remain – no institution cannot prevent terrorists from looting the coffers of failed states – but currently no institution at the national, regional, or international level can say it is doing everything in its power, using all the available tools, to protect those they serve.

References

9/11 Commission. (2004). *Staff Report to the Commission: Monograph on Terrorist Financing*. Washington, DC: U.S. Government Printing Office.

Barber, B. (1995). *Jihad vs. McWorld: How Globalism and Tribalism Are Reshaping the World*. New York, NY: Times Books.

Basile, M. (2004). Going to the Source: Why Al Qaeda's Financial Network Is Likely to Withstand the Current War on Terrorist Financing. *Studies in Conflict & Terrorism, 27*(3), 169-185.

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

Buthe, T. & Mattli, W. (2011). *The New Global Rulers: The Privatization of Regulation in the World Economy*. Princeton, NJ: Princeton UP.

Chomsky, N. (1999). *Profit Over People: Neoliberalism and the Global Order*. New York, NY: Seven Stories.

Clarke, C. P. (2015). *Terrorism, Inc: The Financing of Terrorism, Insurgency, and Irregular Warfare*. Santa Barbara, CA: ABC-CLIO.

del Cid Gómez, J. M. (2010). A Financial Profile of the Terrorism of Al-Qaeda and its Affiliates. *Perspectives on Terrorism, 4*(4), 3-27.

Financial Action Task Force. (2017). *International Standards on Combating Money Laundering And the Financing of Terrorism & Proliferation: The FATF Recommendations.* Paris, France: Organization for Economic Cooperation and Development.

Friedman, T. L. (2005, April 3). It's a Flat World, After All. *New York Times Magazine*.

Retrieved from http://www.nytimes.com/2005/04/03/magazine/its-a-flat-world-after-all.html

Irwin, A. & Milad, G. (2016). The use of crypto-currencies in funding violent jihad. *Journal of Money Laundering Control, 19*(4), 407-425.

Keatinge, T. (2015) Rampant Ransoms: Kidnapping's Economic Bubble. *Foreign Affairs, 94*(1). Retrieved from https://www.foreignaffairs.com/articles/middle-east/2015-01-26/rampant-ransoms

Keohane, R. O. (1998). International Institutions: Can Interdependence Work? *Foreign Policy, 110*, 82-94.

Kingah, S. & Zwartjes, M. (2015). Regulating money laundering for terrorism financing: EU-US Transnational policy networks and the financial action task force. *Contemporary Politics, 21*(3), 341-353.

Levitt, M. & Bauer, K. (2017). Qatar Doesn't Need a Blockade. It needs an Audit. *Foreign Policy.* Retrieved from http://foreignpolicy.com/2017/06/15/qatar-doesnt-need-a-blockade-it-needs-an-audit-al-qaeda/

MEMRI Cyber & Jihad Lab. (2015). Salafi-Jihadis Conduct Online 'Equip Us' Campaign To Raise Funds For Jihad In Gaza. Washington, DC: Middle East Media Research Institute.

Picarelli, J. T. (2012). Osama bin Corleone? Vito the Jackal? Framing Threat Convergence Through an Examination of Transnational Organized Crime and International Terrorism. *Terrorism and Political Violence, 24*(2), 180-198.

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

Reuter, P. & Truman, E. (2004). *Chasing Dirty Money: The Fight Against Money Laundering*. New York, NY: Columbia UP.

Salami, I. (2017). Terrorism Financing with Virtual Currencies: Can Regulatory Technology Solutions Combat This? *Studies in Conflict & Terrorism,* dio:10.1080/1057610X. 2017.1365464.

Scott, B. R. (2001). The Great Divide in the Global Village. *Foreign Affairs, 80*(1), 160-177.

Sen, A. (2002). How to Judge Globalism. *The American Prospect, 13*(1).

Soufan, A. (2017). *Anatomy of Terror: From the Death of Bin Laden to the Rise of the Islamic State*. New York, NY: W.W. Norton & Company.

Stiglitz, J. E. (2004). *The Roaring Nineties: A New History of the World's Most Prosperous Decade*. New York, NY: W.W. Norton & Company.

van der Does de Willebois, E. (2010). Nonprofit Organizations and the Combatting of Terrorism Financing: A Proportionate Response. *World Bank Working Papers, 208*.

Vovchenko, N. G., Tishchenko, E. N., Epifanova, T. V., & Gontmacher, M. B. (2017). Electronic Currency: The Potential Risks to National Security and Methods to Minimize Them. *European Research Studies, 20*(1), 36-48.

United States Department of the Treasury. (2010). *The Hawala Alternative Remittance System and its Role in Money Laundering.* Vienna, VA: Financial Crimes Enforcement Network/INTERPOL.

United States Department of the Treasury (2018). *Suspicious Activity Report Statistics* [data set]. Retrieved from: https://www.fincen.gov/reports/sar-stats

United States House of Representatives. (2012). *Terrorist Financing Since 9/11: Assessing an Evolving Al-Qaeda and State Sponsors of Terrorism*. Washington, DC: U.S. Government

Printing Office

United States House of Representatives. (2016). *Stopping Terror Finance: Securing The U.S. Financial Sector*. Washington, DC: U.S. Government Printing Office.

United States v. Arnaout, 282 F. Supp. 2d 838 (N.D. Ill. 2003).

United States v. Issa, et al., No. 09 Cr. 1244 (BSJ) (S.D.N.Y. 2009).

United States v. Shahnaz, No. 17 Cr. 0690 (E.D.N.Y. 2017).

University of Maryland. (2014). *Exploring the U.S. Crime-Terror Nexus: Terrorist Networks and Trade Diversion.* College Park, MD: Belli, R., Freilich, J., Chermak, S., & Boyd, K.

Weimann, G. (2016). Going Dark: Terrorism on the Dark Web. *Studies in Conflict and Terrorism, 39*(3), 195-206.

Weinberg, D. A. (2015). *Hearing before the House Committee on Foreign Affairs: "Terrorist Financing: Kidnapping, Antiquities Trafficking, and Private Donations*. House of Representatives, 114th Congress.

Zulkhibri, M. (2016). Financial inclusion, financial inclusion policy, and Islamic finance. *Macroeconomics and Finance in Emerging Market Economies, 9*(3), 303-320.

Table 1

Total Number of Reports by Industry and Type	Known Terrorist	Terrorism Suspected	Grand Total
2013	**459**	**462**	**921**
Casino/Card Club - Tribal Authorized Casino	1	2	3
Depository Institution	182	220	402
Insurance Company	1	1	2
Money Services Business (MSB)	263	154	417
Other	10	80	90
Securities/Futures	2	5	7
2014	**463**	**832**	**1295**
Casino/Card Club - Card Club	1	2	3
Casino/Card Club - State Licensed Casino	1	8	9
Casino/Card Club - Tribal Authorized Casino	1		1
Depository Institution	231	296	527
Insurance Company		2	2
Money Services Business (MSB)	202	412	614
Other	21	105	126
Securities/Futures	6	7	13
2015	**991**	**1102**	**2093**
Casino/Card Club - Card Club		1	1
Casino/Card Club - State Licensed Casino	28	7	35
Casino/Card Club - Tribal Authorized Casino	5	4	9
Depository Institution	433	371	804
Insurance Company	1	1	2
Loan or Finance Company		2	2
Money Services Business (MSB)	501	586	1087
Other	19	116	135
Securities/Futures	4	14	18
2016	**1122**	**872**	**1994**
Casino/Card Club - Card Club		2	2
Casino/Card Club - Other Casino/Card Club		2	2
Casino/Card Club - State Licensed Casino	2	47	49
Casino/Card Club - Tribal Authorized Casino	5	3	8
Depository Institution	374	404	778
Insurance Company	1	3	4
Loan or Finance Company		1	1
Money Services Business (MSB)	705	369	1074
Other	23	34	57
Securities/Futures	12	7	19
2017	**1504**	**540**	**2044**
Casino/Card Club - State Licensed Casino	27	4	31

Casino/Card Club - Tribal Authorized Casino	1	4	5
Depository Institution	379	227	606
Housing GSE		1	1
Insurance Company		3	3
Loan or Finance Company	2	1	3
Money Services Business (MSB)	1024	261	1285
Other	64	32	96
Securities/Futures	7	7	14
2018	**166**	**39**	**205**
Casino/Card Club - Tribal Authorized Casino		2	2
Depository Institution	23	19	42
Money Services Business (MSB)	135	16	151
Other	7	2	9
Securities/Futures	1		1
Grand Total	**4705**	**3847**	**8552**

Source: U.S. Department of the Treasury. (2018). "Suspicious Activity Report Statistics". Retrieved from https://www.fincen.gov/reports/sar-stats. Table: Cody Wilson