REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
04-05-2016	Master's of Military Studies	SEP 2015 -APR 2016

4. TITLE AND SUBTITLE
A WICKED PROBLEM: TRANSNATIONAL TERRORIST FINANCING AND THE TRILLION-DOLLAR DILEMMA

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
LCDR JUSTIN D. GUITERMAN, USNR

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES
NONE

14. ABSTRACT
Government officials and stakeholders in the financial industry trying to counter transnational terrorist financing face a wicked problem. This problem is ill-defined, with multiple causes and uncertainly on whether the solutions implemented to combat this threat are effective. It is a problem further complicated by the convergence of globalization, digitalization and introduction of disruptive financial technologies, which further enables distributed terrorist financing.

15. SUBJECT TERMS
ANTI MONEY LAUNDERING, TERRORIST FINANCING, WICKED PROBLEM, DISTRIBUTED TERRORIST FINANCING, COUNTER TERRORIST FINANCING, DISTRIBUTED OPERATIONS, VIRTUAL CURRENCY, DIGITALIZATION, GLOBALIZATION, FINANCIAL TECHNOLOGIES

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC Command and Staff College
U	U	U	UU	64	19b. TELEPHONE NUMBER *(Include area code)* (703) 784-3300 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

A Wicked Problem: Transnational Terrorist Financing
And the Trillion-Dollar Dilemma

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR: LCDR Justin D. Guiterman, USNR

AY 15-16

Mentor and Oral Defense Committee Member: Marc Lorince Antonoff
Approved:
Date: 5/2/16

Oral Defense Committee Member: Michael Lewis
Approved:
Date: 5/2/2016

EXECUTIVE SUMMARY

Title: A Wicked Problem: Transnational Terrorist Financing and the Trillion-Dollar Dilemma

Author: Lieutenant Commander Justin D. Guiterman, USNR

Thesis: Government officials and stakeholders in the financial industry trying to counter transnational terrorist financing face a *wicked problem.* This problem is ill-defined, with multiple causes and uncertainty on whether the solutions implemented to combat this threat are effective. It is a problem further complicated by the convergence of globalization, digitalization and introduction of disruptive financial technologies, which further enables *distributed terrorist financing*.

Discussion: The acquisition and use of illicit funds is a vital function for any transnational terrorist organization. Along with personnel and materials, money represents a critical component in the execution of violent activities. Government and financial industry stakeholders since the 1970s, and particularly after the events of 9/11, attempted to detect and stop this nefarious activity. Despite tactical level successes and making the operating environment more difficult for transnational terrorist organizations, the macro level problem persists at levels exceeding $1 trillion USD annually.

Simultaneously the convergence of globalization, digitalization and introduction of disruptive financial technologies are enabling transnational terrorist organizations to further distribute their acquisition, transmission and storage activities. By employing *distributed terrorist financing*, these groups engage in a form of offense designed to circumvent and overwhelm the defensive measures in place, and disperse the acquisition and transmission of illicit funds. Altogether the macro-level state of transnational terrorist financing, along with distributed terrorist financing, create a *wicked problem* that is never solved, but resolved over and over again.

Conclusion: Government and financial industry stakeholders should accept transnational terrorist financing as a *wicked problem,* as this can help foster development of a strategic mindset focused on more effective CTF resolutions. This will require a continuous effort on the part of all stakeholders, with hard, but necessary, choices around risk tolerance and the restoration of trust and confidence.

DISCLAIMER

ILLUSTRATIONS

TABLES

TABLE OF CONTENTS

LIST OF ACRONYMS AND ABBREVIATIONS

ACAMS	**ASSOCIATION OF CERTIFIED ANTI-MONEY LAUNDERING SPECIALISTS**
AML	**ANTI-MONEY LAUNDERING**
AQ	**AL QAEDA**
CTF	**COUNTER TERRORIST FINANCING**
EU	**EUROPEAN UNION**
FATF	**FINANCIAL ACTION TASK FORCE**
FINCEN	**FINANCIAL CRIMES ENFORCEMENT NETWORK**
FINTECH	**FINANCIAL TECHNOLOGIES**
FIU	**FINANCIAL INTELLIGENCE UNITS**
FTF	**FOREIGN TERRORIST FIGHTER**
HSBC	**HONG KONG AND SHANGHAI BANKING CORPORATION**
IS	**ISLAMIC STATE**
ISIL	**ISLAMIC STATE OF IRAQ AND THE LEVANT**
ISIS	**ISLAMIC STATE OF IRAQ AND SYRIA**
IT	**INFORMATION TECHNOLOGY**
MVTS	**MONEY VALUE TRANSFER SYSTEM**
NTFRA	**NATIONAL TERRORIST FINANCING RISK ASSESSMENT**
SAG	**SURFACE ACTION GROUP**
SAR	**SUSPICIOUS ACTIVITY REPORT**
TF	**TERRORIST FINANCING**
USA	**UNITED STATES OF AMERICA**

USD	**UNITED STATES DOLLAR**
UN	**UNITED NATIONS**

ACKNOWLEDGEMENTS

I would like thank the faculty and staff of Marine Corps University, Command and Staff College for assisting me through the study of a serious, transnational threat to US economic and national security. Dr. Anne Louise Antonoff, who was my mentor in this project, guided me in our conversations about my thesis and how transnational terrorist financing is "a *wicked problem*." Your input over the six months I researched and wrote this thesis was invaluable. Because of your help, I was able to define the problem and highlight the consequences of *distributed terrorist financing* that globalization and digitalization enable. I would also like to acknowledge Professor Michael Lewis and Lieutenant Colonel William "Punchy" Chesarek, USMC, who attended my oral defense and provided important feedback on my work.

I would also like to thank my leadership and colleagues at EY (Ernst & Young) LLP, my civilian employer. When I received the message the Navy wanted me to attend the service college program with the Marines in Quantico, you gave me unconditional support as a Navy Reserve Officer. My special thanks goes to Ron Giammarco, Erin McAvoy, Joe McHugh, Tony Klimas, Rob Mara, Jake Jacobson, Patrick Pfeil, Jason Wingo (the best counselor one could ask for), Orlando Lopez, Nik Walser, Charles Dotter, Carl Case (GO NAVY!), Christina Rasch (BEAT ARMY), Adam Meshell, Greg Capece and numerous others who helped me learn and navigate the world of financial consulting and anti-money laundering/counter terrorist financing.

Finally, I want to thank an alumna of the Command and Staff College and fellow surface warfare officer, my wife Lieutenant Commander Bree Adams Guiterman. She gave me all of the support a husband can ask. Whether by picking up our son so I could spend more time at the library, to reviewing my thesis as a sanity check (all while pregnant!!!), she motivated me to keep going on researching this complicated topic. GO NAVY!

I. INTRODUCTION

When describing illicit financing's importance to transnational terrorism, deceased *Al Qaeda* (AQ) financial chief Sa'id Al-Masri put it best when he stated, "Without money, jihad stops."[1] He and his associates knew this, as they were responsible for a $30 million USD annual budget, financing activities prior to the 9/11 attacks.[2] Without funding, the approximately $500,000 USD spent by the 9/11 hijackers to plan and execute their now infamous attacks would not have been possible.[3] In the case of AQ, the terrorist group succeeded in acquiring funds through the illicit use of *zakat*, which is the call of Islamic charitable giving, private patronage and Taliban financial support in Afghanistan.[4] Furthermore, they transferred money using a trust-based, informal remittance system called *hawala*[5], avoiding the formal, global banking system until the hijackers were physically in the United States.[6] By then the small, incremental volume of their transactions made detection of suspicious activity difficult, as the primary focus of financial institutions and U.S. Treasury regulators at the time was on international fraud and drug trafficking.[7] The end results were thousands murdered, billions of dollars in economic damage, the World Trade Center's destruction and an on-going war.

Since the 1970s and particularly after 9/11 (see Appendix A for US AML/CTF regulations overview), government officials and stakeholders in the financial industry have attempted to solve problems caused by the likes of Sa'id Al-Masri: detect and stop illicit financial activity

---

[1] U.S. Department of Treasury. *National Terrorist Financing Risk Assessment: 2015.* Washington, DC: U.S. Department of Treasury, 2015. 14

[2] Commission, 9/11. *The 9/11 Commission Report.* Commission Report, Washington, DC: National Commission on Terrorist Attacks Upon the United States, 2004. 170

[3] 9/11 Commission, *The 9/11 Commission Report*. 172

[4] 9/11 Commission, *The 9/11 Commission Report*. 171

[5] Patrick M. Jost, Harjit Singh Sandhu, "The Hawala Alternative Remittance System and its Role in Money Laundering," *Financial Crimes Enforcement Network and INTERPOL.* 6

[6] 9/11 Commission, *The 9/11 Commission Report*. 171

[7] 9/11 Commission, *The 9/11 Commission Report*. 172

from exploiting a complex, globalized system configured to maximize access, efficiency and speed. His statement on money's importance demonstrates a common denominator for AQ and similar entities: "The lifeblood of [many] violent, non-state organization is its ability to generate funds."[8] Transnational terrorist financing is not static, however, as these groups repeatedly demonstrated an agile ability to adapt and exploit new methods for achieving their intended ends.[9] They include a desire for monetary profit, political gain or ideological supremacy. Paralleling this situation, the financial industry itself continues to experience large-scale transformation due to the continuing effects of globalization, increased digitalization and introduction of disruptive, financial technologies (e.g. virtual currencies). Nefarious actors now have an increased ability to distribute the acquisition and transmission of illicit funds further.

In the end, government officials and stakeholders in the financial industry trying to counter terrorist financing (CTF) face a "*wicked problem.*" [10] This term denotes an ill-defined problem with multiple causes and uncertainty as to whether the solutions implemented to combat this threat are effective. The problem itself defies single, permanent solutions as it frequently takes new forms. The convergence of globalization, digitalization and introduction of disruptive financial technologies further complicate CTF and results in *distributed terrorist financing*. This term borrows from a concept prevalent in military thinking, *distributed operations*, and intended to allow forces to evade the ever more precise and all-seeing surveillance and targeting systems of the 21st Century. More granularly, distributed terrorist financing leverages the concept of *distributed lethality* developed by the United States Navy. Its focus is to add more firepower to all manner of Navy vessels and operate them in a way that would spread thin enemy defenses. In

---

[8] Colin P. Clarke, *Terrorism, Inc. The Financing of Terrorism, Insurgency and Irregular Warfare*, Praeger: Santa Barbara, 2015, 1

[9] Colin P. Clarke, , *Terrorism, Inc. The Financing of Terrorism, Insurgency and Irregular Warfare*, 172

[10] Camillus, John C, "Strategy as a Wicked Problem," *Harvard Business Review*, May 2006, accessed 19 March 2016, https://hbr.org/2008/05/strategy-as-a-wicked-problem

the case of terrorist financing, transnational terrorist and criminal organizations can utilize multiple mechanisms that spread the resources thin of those attempting to detect and stop this illicit activity. By complicating enemy targeting with multiple, simultaneous avenues of approach in very small units, *distributed operations* aim to improve survivability and effectiveness, with each unit operating on its own initiative but under the intent of the overall command. *Distributed terrorist financing* replicates this capability in the digital, globalized system of modern money, and epitomizes the constant mutation and creative audacity inherent in *wicked problems*.

This paper will explore this national security issue in the following four steps:

1. Review the current, macro-level state of transnational terrorist financing and appreciate the holistic, global scale of this problem. Gaining a fundamental grasp of the issue is necessary to understand a systemic perspective.
2. Define *distributed terrorist financing* and the impact of globalization, digitalization and disruptive financial technology enablers. This section builds off the previous review by identifying the newest aspects of the transnational terrorist financing problem. It will also underscore the need for a systemic view beyond the linear focus of key stakeholders in government and the financial industry. Historically, these groups would use discrete measures to precise, past behaviors, rather than considering the conceptual intent behind the behavior and trying to get into the minds of the perpetrators. As opposed to their money, the mind brings a virtually unlimited source of innovation, whereas the money has the illusion of being a fixed, definable problem at any given moment. It questions whether money interdiction is the proper metric of success.

3. Why is it necessary to understand transnational terrorist financing as a *wicked problem*? Despite a series of seemingly tactical AML/CTF successes, this did not add up at the operational or strategic level. Despite the implementation of numerous solutions, the illicit acquisition and movement of funds continues, though more difficult but largely unabated.
4. Provide macro-level recommendations for government and financial industry stakeholders to consider for more effectively approaching CTF. Recognizing transnational terrorist financing is a *wicked problem* can provide a foundation for developing a strategic mindset and trust across multiple stakeholders, and tackle the highly difficult attempt of a cost-benefit analysis.

This paper does not attempt to solve the multiple, complex causes of why individuals and groups engage in transnational terrorist financing, nor does it propose micro-level resolutions. Additionally, it acknowledges that "tremendous progress has been made in combating the financing of terrorism, insurgency and irregular warfare"[11] since 9/11. Unfortunately, despite successes against individuals or groups, the larger, systemic problem remains a serious threat to US national security and economic well-being. What CTF needs, therefore, is a holistic understanding of the problem in descriptive systemic terms, conveying the overarching dynamic and character of the problem from the terrorist standpoint as much from the counter-terrorist standpoint, not prescriptive tactical solutions devised one at a time in pursuit of an adversary in constant metamorphosis.

Therefore, the aim is to present an alternate view on a persisting danger, and provide a catalyst for new, creative thinking. Enacting new laws and regulations, or requiring the financing industry to meet those obligations, is not sufficient while there is a lack of a strategic understanding of transnational terrorist financing. Nor will the blunt use of US national power

[11] Colin P. Clarke, *Terrorism, Inc. The Financing of Terrorism, Insurgency and Irregular Warfare.* 171

suffice only, as demonstrated by recent US military actions against Islamic State [IS]. This risks providing a false sense of achieving a solution, as follow on evidence will establish that transnational terrorist (and criminal) financing is as robust as ever. At the very least, the goal is to have stakeholders in government and the financial industry pause and ask a straight forward and potentially uncomfortable question: Are our efforts, including time, manpower and billions in CTF compliance and law enforcement costs, working to successfully counter this threat?

II. MACRO-LEVEL STATE OF TRANSNATIONAL TERRORIST FINANCING

Dr. Colin P. Clarke, an Associate Political Scientist at the RAND Corporation, recently authored a book examining the financing of terrorist and insurgency groups. In *Terrorism, Inc.* he defines terrorist financing as, "the process of raising, storing and moving funds obtained through legal or illegal means for the purpose of terrorist acts or sustaining the logistical structure of an insurgent organization."[12] Transnational terrorist groups wanting to engage in violent activities are, "as needing three essential components: men, money and munitions…with the money the less high profile," [13] and historically receiving less attention as compared to the other two items. Generating and transmitting funds to pay personnel and supply them, across nation-state borders, is a critical function for any group, including violent, non-state organizations. The end result is transnational terrorist financing.

If there is at least one consistency across any entity, it is the requirement to acquire and transmit funds. The US government, as an example, legally levies taxes and fees to finance federal government expenditures. Without funding agencies and departments, such as the Department of Defense (DoD) or Federal Bureau of Investigations (FBI), will lack the means to pay salaries, procure equipment and execute operations. Transnational terrorist organizations engaged in financing face this similar, minimum financial requirement. A key difference, however, is the necessity to conceal or legitimize their acquisition and transmission activities.

Dr. Clarke in *Terrorism Inc.* developed a useful framework to understand how transnational terrorists and insurgents fund their organizations: *the gray and dark economies*. One should not

[12] Colin P. Clarke, *Terrorism, Inc. The Financing of Terrorism, Insurgency and Irregular Warfare*, 1
[13] Nick Ridley, *Terrorist Financing: The Failure of Counter Measures,* Edward Elgar: Northampton, 2012. 1

confuse these terms with an informal economy or black market, as those typically are associated with unregulated financial activities. Instead, these two economies consist of the following:

	Definition	Financing Methods and Techniques	Identified by FATF	Identified by NTFRA
Gray Economy	A "combination of licit and illicit activities perpetrated by terrorist and insurgent groups for monetary gain, and not entirely illegal."[14]	Diaspora support	Yes, with support coming via private donations or the abuse and misuse of non-profit organizations (NPOs)	Yes
		Charities	Yes, with support coming via private donations or the abuse and misuse of non-profit organizations (NPOs)	Yes
		Fraud	Yes, but with non-violent criminal activities such as insurance and credit card fraud	Yes
		Legal Businesses	Yes, either through the use of trade-based financing or shell companies (e.g. car dealerships)	Yes, identifying trade-based financing, or securities trading (e.g. microcap stocks)
		Money Laundering	Not a method for raising funds, but rather concealing	Not a method for raising funds, but rather concealing
Dark Economy	Economic activity that is "entirely illicit and illegal, with little room for interpretation."[15]	Kidnapping for Ransom	Yes, and identified as a growing source of TF revenue	Yes
		Armed Robbery and Theft	Yes	Yes
		Smuggling, Trafficking and Counterfeiting	Yes	Yes
		Natural Resources, Gems, and Precious Metals	Yes	Yes, through extortion
		Extortion and Protection Payments	Yes	Yes
		External State Support	Yes, identified as state sponsorship of terrorism	Yes

Table 1: Gray and Dark Economy Terrorist Financing

Operating in these two economies, transnational terrorist organizations are able to generate funds, transmit and integrate them through the money laundering process (if necessary), and eventually store for future use. The Financial Action Task Force (FATF) outlined in a 2015 report, "in general, previous research has shown that terrorist organizations rely on numerous sources of income and that they use a range of methods to move funds, often internationally, to

[14] Colin P. Clarke, *Terrorism, Inc. The Financing of Terrorism, Insurgency and Irregular Warfare, 5*
[15] Colin P. Clarke, *Terrorism, Inc. The Financing of Terrorism, Insurgency and Irregular Warfare, 8*

their end point without being detected."[16] These activities provide the necessary funding for transnational terrorist organizations to achieve their end, and highlight an important point: they will use more than one financing method, in a ***distributed*** fashion.

Acquiring and transmitting illicit funds presents elevated vulnerability for terrorist organizations, as they risk detection and have varying levels of control until the funds reach their intended beneficiary. One of the primary methods used to mitigate this risk is the *money laundering* process. The U.S. Department of Treasury defines money laundering as, "financial transactions in which criminals, including terrorist organizations, attempt to disguise the proceeds, sources or nature of their illicit activities."[17] Money laundering "is not an end in and of itself, but a method that is best conceived of as an illicit support activity."[18] It takes *dirty* proceeds and makes it appear legitimate, or *clean*. The process entails three primary steps recognized by the government and financial industry:

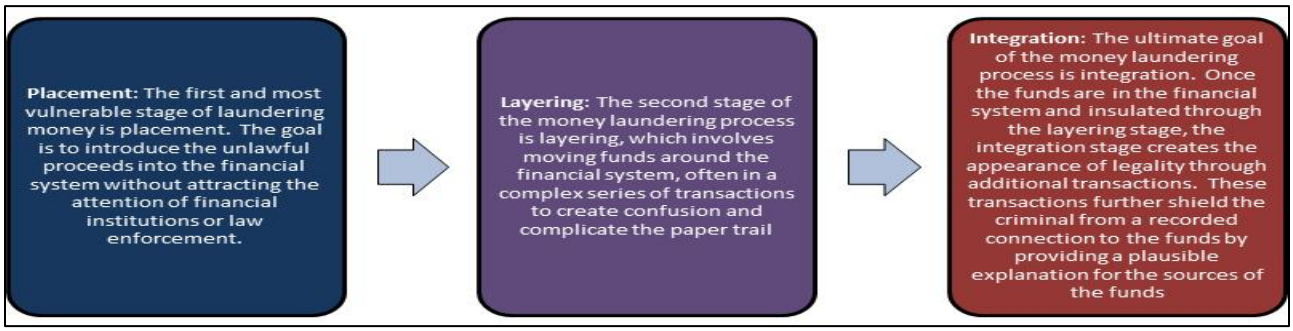


Illustration 1: Three Money Laundering Steps[19]

The United Nations Office on Drugs and Crime (UNODC) **conservatively estimated** in one year, "money laundered globally…is 2-5% of global GDP [gross domestic product], or **$800**

[16] Financial Action Task Force, *FATF Report: Emerging Terrorist Financing Risks*. Paris, 13.
[17] "Resource Center: Money Laundering," US Department of Treasury, accessed January 11, 2016, https://www.treasury.gov/resource-center/terrorist-illicit-finance/Pages/Money-Laundering.aspx
[18] Colin P. Clarke, *Terrorism, Inc. The Financing of Terrorism, Insurgency and Irregular Warfare,* 7
[19] Federal Financial Institutions Examination Council (FFIEC), *Bank Secrecy Act/Anti-Money Laundering Examination Manual 2014*, November 17, 2014. 7

billion - $2 trillion in current US dollars [USD]."[20] This is a staggering amount when put into context. If one were to use the **lower** estimate, the value is larger than the market capitalization of the world's largest corporation according to *Forbes*: Apple, Inc. with $741.8 billion USD.[21] Compared to a different entity, the IMF estimated "Indonesia's gross domestic product, in current prices, at $888.648 billion USD."[22] If criminal and terrorist enterprises were hypothetically a single entity, their *minimum* entire proceeds would approach the size of the world's fourth most populous country. When examining the United States exclusively, the US Treasury "estimates that about $300 billion is generated annually in illicit proceeds."[23] What exact percentage of these proceeds directly connects to terrorist activities is not precise but the, "UNODC estimates illicit drug sales were $64 billion…putting the proceeds for all other forms of financial crime in the United States at $236 billion, most of which is attributable to fraud."[24]

While fraud and the narcotics trade frequently identify with criminal activity, "in recent years, some analysts have identified a series of potentially disturbing trends that have hastened the expansion of the relationship between terrorist and transnational crime groups."[25] The *Congressional Research Service* (CRS) in 2010 summarized this finding, with research indicating transnational terrorist organizations are exploiting:

---

[20] "Money Laundering and Globalization," UNODC, accessed December 28, 2015. https://www.unodc.org/unodc/en/money-laundering/globalization.html
[21] "The World's Most Valuable Brands," *Forbes,* October 2015, accessed January 23, 2016, http://www.forbes.com/companies/apple/
[22] "World Economic Outlook Database, October 2015," International Monetary Fund, accessed January 27, 2016, http://www.imf.org/external/pubs/ft/weo/2015/02/weodata/weorept.aspx
[23] U.S. Department of Treasury, *National Money Laundering Risk Assessment: 2015*, U.S Department of Treasury, June 12, 2015. 2
[24] U.S Department of Treasury*, National Money Laundering Risk Assessment*, 11
[25] John Rollins and Liana Sun Wyler, *Terrorism or Transnational Crime: Foreign Policy Issues for Congress,* Congressional Research Service: Washington, DC, 2013. 5

1. The growing size of criminal syndicates, as globalization extended their transnational reach and exploit vulnerabilities in the area of cybercrime, credit card fraud and trade-based money laundering.
2. A religious rather than a nationalist or ethnic separatist imperative that prevailed prior to the 1980s motivates terrorist organizations. This enables increased cross-border appeal.
3. Transnational terrorist groups are more resilient to financial destruction, either due to state sponsorship (i.e. Hezbollah and Iran), or entrepreneurial expansion into profitable criminal activities (i.e. Taliban and Afghan opium production).[26]

[26] John Rollins et al, *Terrorism or Transnational Crime: Foreign Policy Issues for Congress,* 2

III. DISTRIBUTED TERRORIST FINANCING: THE IMPACT OF GLOBALIZATION, DIGITALIZATION AND DISRUPTIVE TECHNOLOGIES

What is *distributed terrorist financing*? The term borrows from recent discussions in the United States Navy involving *distributed lethality*, which is, "The condition gained by increasing offensive power of individual components of the surface force and then employing them in dispersed offensive formations known as 'hunter-killer SAGs' (surface action groups)."[27] It is a concept centered on finding the most effective and efficient method for offensive sea control, while countering enemy anti-access/anti-denial (A2/AD) defensive measures. Using this framework and outside the military context, *distributed terrorist financing* is the condition gained by individual transnational terrorist (and criminal) organizations that enable the acquisition, transmission and use of illicit funds through multiple mechanisms simultaneously. In this situation, government and financial industry personnel deploy policies, procedures and infrastructure to prevent access to the global financial system (i.e. know your customer requirements). If nefarious actors circumvent these countermeasures, the same government and financial industry personnel attempt to detect and stop illicit activity, with the ultimate goal of denying exploitation of the global system. By employing *distributed terrorist financing*, transnational terrorist organizations engage in a form of offense designed to circumvent and overwhelm the defensive measures in place, and disperse the acquisition and transmission of illicit funds. This further adds to the complexity existing within the *wicked problem* the next section will examine.

[27] Vice Admiral Thomas Rowden USN, Rear Admiral Peter Gumataotao USN, Rear Admiral Peter Fanta USN, "Distributed Lethality," *Proceedings Magazine*, January 2015 Volume 141/1/1.343, accessed 21 March 2016, http://www.usni.org/magazines/proceedings/2015-01/distributed-lethality

The question immediately following this concept is how do transnational terrorist organizations employ *distributed terrorist financing*? FATF identified several terrorist financing trends in their 2015 report demonstrating this. More importantly, there are three elements fostering this situation: globalization, digitalization and the introduction of disruptive financial technologies. This section will examine these three factors, how they contribute to *distributed terrorist financing*, and ultimately the *wicked problem*.

Globalization

In 2008 the IMF defined economic globalization as, "the increasing integration of economies around the world, particularly through the movement of goods, services, and capital across borders."[28] Starting with the Bretton Woods system, established under United States' leadership after World War II to help stabilize currencies and promote growth, the global economy experienced a period of trade liberalization, increased cross-border capital flows and foreign direct investment. As a result of this and as the 2010 CRS report identifies, globalization and the financial system's integration, "in recent years has enabled illicit actors to place and move money, hide assets, and conduct transactions anywhere in the world, exposing financial centers to exploitation and abuse."[29]

Globalization Case Study: Global Remittance

Remittance payments serve as an excellent example of cross border capital flows and their resilience following the global financial crisis. As a money value transfer system (MVTS), "the remittance sector has been exploited to move illicit funds and is also vulnerable to terrorist financing."[30] In 2009, "the economic crisis in a major migrant destination country (i.e. France) was expected to adversely affect migrants' income and employment opportunities and hence

[28] IMF, "Globalization: A Brief Overview." http://www.imf.org/external/np/exr/ib/2008/053008.htm
[29] U.S Department of Treasury, *National Terrorist Financing Risk Assessment*, 46
[30] FATF, *FATF Report: Emerging Terrorist Financing Risks*. 21

willingness and ability of migrants to stay in their host countries and continue to remit funds. Nevertheless, it was remarkable that remittance flows to developing countries fell only 5.2 percent in 2009, providing to be significantly more resilient than private capital flows, which declined precipitously."[31]

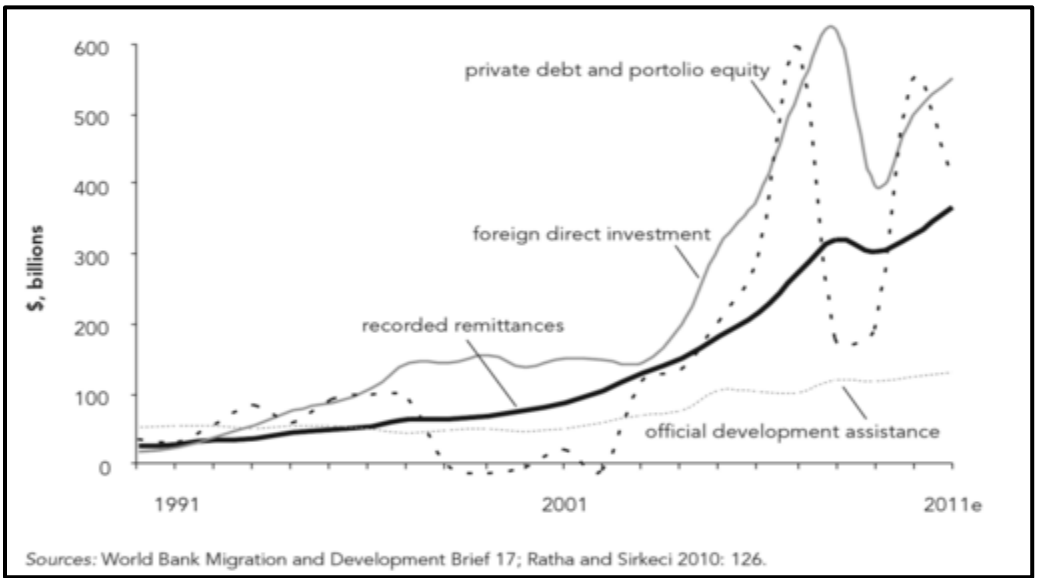


Illustration 2: Resilience of Remittances Compared to Other Financial Flows to Developing Countries[32]

By 2014, personal remittance reached approximately $510 billion USD, and this figure does not include flows to failed or failing nation-states such as Syria or Iraq.[33] What does this all mean? It is not a secret that transnational terrorist organizations utilized cross-border remittance payments for raising and transmitting funds. In fact, the key point to make is this is but one tool in the tool box for nefarious groups and individuals. The takeaway is the quantity of remittance payments, and the multiple avenues available to execute these types of transactions. It is also important to note that the above figures do not include informal exchanges, such as a *hawala*. It

[31] Ibrahim Sirkeci, Jeffery H. Cohen, Dilip Ratha, *Migration and Remittances During the Global Financial Crisis and Beyond*, The World Bank, Washington, 2012, 3.
[32] Sirkeci et al, *Migration and Remittances During the Global Financial Crisis and Beyond,* 2.
[33] "Personal remittances, received (current US$), The World Bank, accessed 21 March 2016, http://data.worldbank.org/indicator/BX.TRF.PWKR.CD.DT/countries/1W?order=wbapi_data_value_2014%20wbapi_data_value%20wbapi_data_value-last&sort=desc&display=default

also does not imply that remittance payments are bad. On the contrary, it is a legitimate, vital service for millions of people daily as the below illustrations demonstrate:

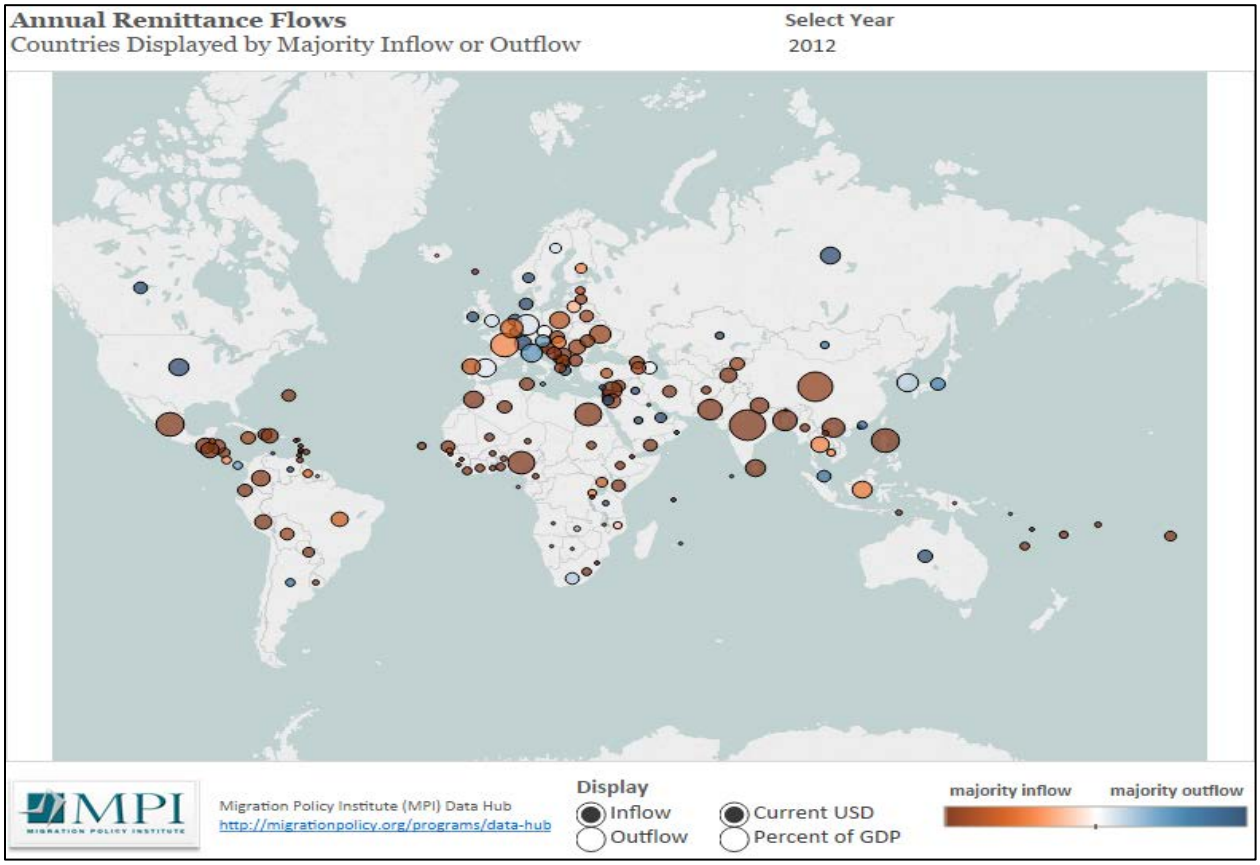


Illustration 3: 2012 Global Remittance Inflow (Source: Migration Policy Institute). The larger the circle indicates a higher USD quantitative value.

In Mexico alone, overseas remittance inflow payments totaled $24.8 billion USD in 2014,[34] with most of the funds coming from family members working outside of the country. What this above chart illustrates is the global nature of this payment system. The following chart illustrates outflow payments:

[34] Associated Press, "Mexico Got More Money from Remittances Than from Oil Revenues in 2015," *NBC News*, 3 February 2016, accessed 10 April 2016, http://www.nbcnews.com/news/latino/mexico-got-more-money-remittances-oil-revenues-2015-n510346

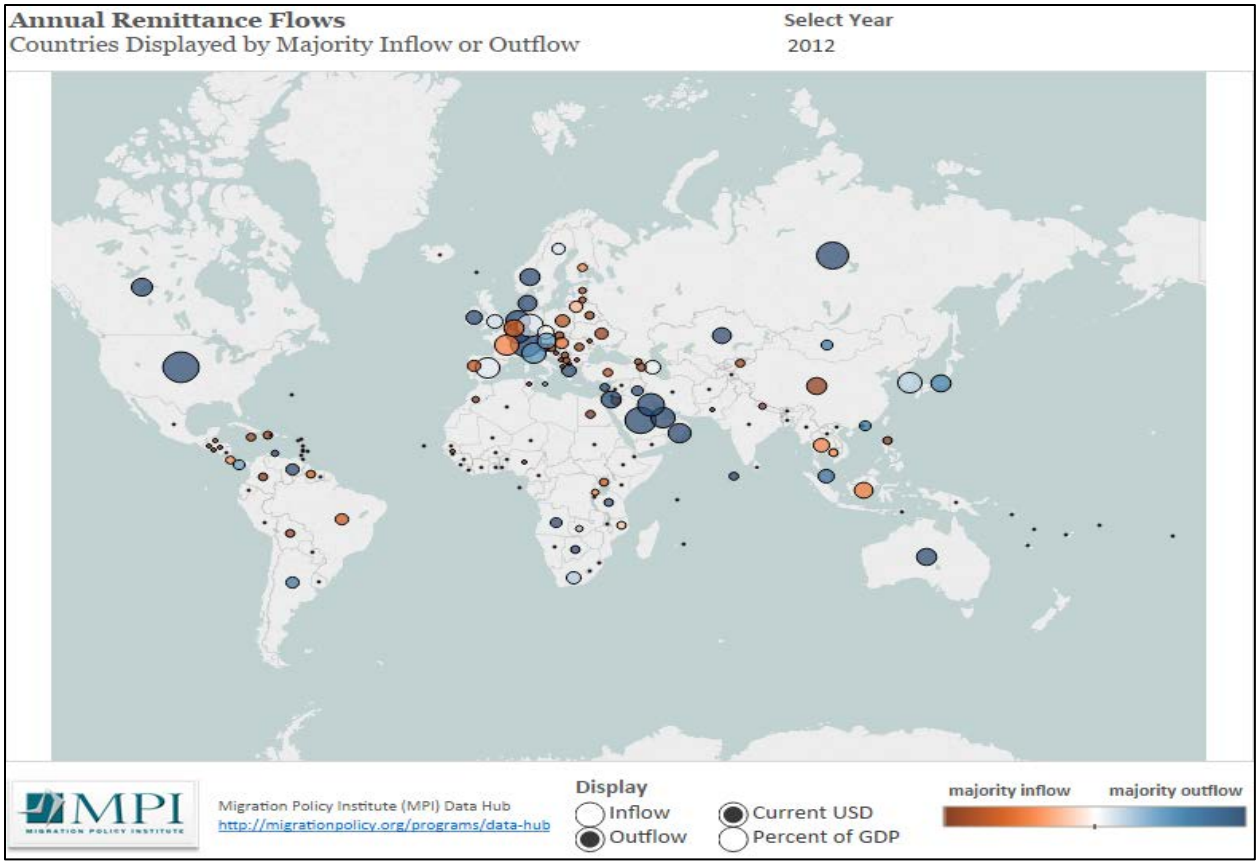


Illustration 4: 2012 Global Remittance Outflow (Source: Migration Policy Institute). The larger the circle indicates a higher USD quantitative value.

As the two illustrations demonstrate, global remittance outflow and inflow payments take place in nearly every nation-state. Within each are varying degrees of AML/CTF controls, corruption and other elements that can potential enable transnational terrorist financing. Since the payments are cross-border, however, the originating or beneficiary country is inherently dependent on the other. Traditionally dominated by such household names like Western Union and MoneyGram, new digital technologies have the potential to disrupt the remittance payment industry and further complicate AML/CTF efforts.

Digitalization and Disruptive Financial Technologies:

Concurrently with globalization, two other significant events are having a profound impact on the financial services industry, and challenging government's ability to keep up with the

changing landscape: digitalization and the introduction of disruptive financial technologies. With respect to digitalization, there are numerous definitions on how to define this term. To put it simply, it is the transition from analog to digital. The following case study is an example of the convergence of digitalization and the use of disruptive financial technologies:

Digitalization and Disruptive Technologies Case Study - Ransom at the Point of a Keyboard

Administrators, nurses and other medical employees of Hollywood Presbyterian Medical Center discovered they were victims of a cybercrime on 5 February 2016. A ransomware attack infected the hospital's information technology (IT) infrastructure, with a hacker(s) holding the hospital ransom by locking electronic access to critical information such as patient electronic medical records. Facing a dangerous and potentially life-threatening situation because of their dependency on digital information for patient care, Hollywood Presbyterian agreed to pay the approximately $17,000 USD ransom, and received the unlocking decryption key designed by this industrious individual or group. More interestingly was the chosen payment method dictated by the perpetrator: 40 bitcoin.[35] This is an extraordinary development. An unknown individual or entity was able to not only hold an institution hostage electronically, but also anonymously receive its ransom by utilizing a new financial instrument now widely available to the public: **virtual currencies**.

The emergence of virtual currencies, most notably *Bitcoin*, potentially represents an innovation in financing. To begin with, "A virtual currency (VC) is a digital representation of a value that can be transferred, stored, or traded electronically and that is neither issued by a central bank or public authority, nor necessarily attached to a fiat currency (dollars, euros, etc…),

[35] Justin Wm. Moyer, "After computer hack, L.A. hospital pays $17,000 in bitcoin ransom to get back medical records," *Washington Post*, 18 February 2016, accessed 27 February 2016. https://www.washingtonpost.com/news/morning-mix/wp/2016/02/18/after-computer-hack-l-a-hospital-pays-17000-in-bitcoin-ransom-to-get-back-medical-records/

but accepted by people as a means of payment."[36] Virtual currencies were already used frequently by consumers over the last several decades (i.e. frequent flyer mile programs), but the key difference is that new VCs such as Bitcoin attempt to function like a fiat currency that is decentralized and exchangeable.

This anonymity is possible because the product only requires a transaction identification, user name and amount to complete the process. While not absolute, users can create random user names without having to reveal information (name, address, tax number, etc…) typically required by traditional financial institutions. In the Hollywood Presbyterian example, the hacker(s) raised illicit funds through ransom, moved them using the virtual currency Bitcoin, and can now store the proceeds virtually undetected. In this particular case, the individual(s) can either sell their bitcoins to another user for US dollars, or simply retain the currency and desire for a certain level of appreciation. If the individual elected to sell, storage is possible through a variety of methods, ranging from withdrawing and placing physical currency (i.e. US dollar bills) in a secure location, wiring money to a seemingly legitimate bank account or country domicile with weak AML/CTF controls.

What this single, micro event illustrates is nefarious, non-state organizations (and individuals) engaging in criminal or terrorist activities are exploiting digital methods and disruptive technologies for financing. Beyond virtual currencies, other forms of digital products and services are enabling disruptive financial technologies to penetrate the global financial system or enable illicit financing. As a result, transnational terrorist organizations have new mechanisms available:

---

[36] Joshua Baron, Angela O'Mahony, David Manheim, Cynthia Dion-Schwarz, *National Security Implications of Virtual Currency: Examining the Potential for Non-State Actor Deployment*, (Santa Monica: RAND Corporation, 2015), ix.

1. ***Social media communication:*** While recent advances in IT contributed to an ever increasingly globalized world, they also provide criminal and terrorist organizations new methods for fundraising and revenue generations. As a recent example, IS', "Private fundraising networks increasingly rely upon social media to solicit donations and communicate with donors and recipient opposition groups or terrorist organizations."[37] More concerning, FATF notes specific to IS that, "a number of traditional countermeasures used to deprive terrorist organizations of its funds are not applicable with respect to the new model adopted by IS."[38] The immediate fact with the Internet and social media is the increased level of anonymity provided. Additionally, "social networks are being also used to coordinate fundraising campaigns."[39] FATF documented one reason example discovered by Saudi Arabia's FIU.
2. ***"Social network fundraising with prepaid cards***: Individuals associated with IS called for donations via Twitter and asked the donors to contact them through Skype. Once on Skype, those individuals instructed donors to buy an international prepaid card (a credit for mobile phone or the purchase of an Apple or other programs or credit for playing on the internet) and send them the number of this prepaid card via Skype. Then, the fundraiser send the card number to one of his followers in a neighboring country from Syria, who would sell this card number at a lower price and give the cash proceeds to ISIL."[40]
3. ***Crowdfunding***: is an internet-based for businesses or individuals to raise money from donations or investments, and identified by FATF as an emerging terrorist financing risk. This technique represents another example of changes brought about by new information

[37] U.S. Department of Treasury. *National Terrorist Financing Risk Assessment: 2015*, 16
[38] FATF, *Financing of the Terrorist Organisation Islamic State in Iraq and Levant (ISIL)*, 42
[39] Financial Action Task Force (FATF), *FATF Report: Emerging Terrorist Financing Risks*, 31
[40] Financial Action Task Force (FATF), *FATF Report: Emerging Terrorist Financing Risks*, 33

> technology tools creating more opportunities for individuals, both legitimate and nefarious. GoFundMe.com, a major crowdfunding site, claims to have risen over $1 billion USD. Taking advantage of this new tool, terrorist organizations began to exploit this social media system to circumvent traditional anti-terrorist financing countermeasures utilized by law enforcement and financial institutions. According to FATF, Canadian FIUs have identified "instances where individuals under investigation for terrorism-related offences, including attempts to leave the country for terrorist purposes, have used crowdfunding websites prior to leaving and/or attempting to leave Canada."[41]

Beyond crowdfunding, terrorist organizations are utilizing the internet and other social media platforms to solicit donations, such as using PayPal. While it is a non-banking financial institution with an AML/CTF compliance program, "A FinCEN analysis of financial institution reporting showed individuals with alleged links to AQ, the Taliban, Hamas and Chechen Mujahedeen using personal PayPal accounts to collect funds for named causes."[42] In addition, individuals and groups utilize social media platforms such as Twitter and Facebook for advertising designated recipients of terrorist financing, with "One Kuwait based campaign claimed to have raised enough cash to arm 12,000 [IS] fighters."[43]

Methods Available for Distributed Terrorist Financing:

There exist today multiple mechanisms transnational terrorist organizations can use for the acquisition, transmission and use of illicit funds. It is important to reminder a vital point: a nefarious actor does not have to limit his financing activities to a single method. Rather, an individual(s) or group has a globalized, distributed system at their disposal to circumvent or overwhelm government and financial industry countermeasures, "While the number and types of

[41] Financial Action Task Force (FATF), *FATF Report: Emerging Terrorist Financing Risks*, 31
[42] U.S. Department of Treasury. *National Terrorist Financing Risk Assessment: 2015*, 43
[43] U.S. Department of Treasury. *National Terrorist Financing Risk Assessment: 2015*, 43

terrorist groups and related threats have changed over time, the basic need for terrorists to raise, move and use funds has remained the same. However, as the size, scope and structure of terrorist organizations have evolved, so too have their methods to raise and manage funds:"[44] The following provides an overview of some methods, but is not meant to be comprehensive. Rather, it is to illustrate the point of *distributed terrorist financing.* To start, in the *gray economy* outlined by Dr. Clarke, FATF reported continuing methods transnational terrorist groups utilize, including **but not limited to**:[45]

1. ***Private donations fundraising***: Obtained from various resources, "an analysis of terrorist financing related law enforcement cases and prosecutions in the United States since 2001 found that approximately 33% of these cases involved direct financial support from individuals to terrorist networks."[46] Private donations, from individuals and groups continue, "To provide terrorist groups with a consistent flow of funds."[47] FATF identified IS as an organization using this vehicle for revenue generation. Specifically identifying Arabian Peninsula patrons, "the case of Abd al-Rahman bin 'Umayr al-Nu'aymi, was singled out by Treasury in December 2013, who secured the transfer of over $2 million per month"[48] to IS, along with donations to other terrorist groups such as *al Qaeda in Syria* and al-Shabaab.
2. ***Non-profit organizations (NPOs)***: The exploitation and misuse of NPOs, including charities, "is a long favored fund-raising technique…often affiliated with religious groups."[49] One example of this is the *Holy Land Foundation*, where a court convicted member of the now defunct charity in 2008 of providing material support to Hamas. Charities are also suspected

[44] Financial Action Task Force (FATF), *FATF Report: Emerging Terrorist Financing Risks*, October 2015. 5
[45] Financial Action Task Force (FATF), *FATF Report: Emerging Terrorist Financing Risks*, 24
[46] Financial Action Task Force (FATF), *FATF Report: Emerging Terrorist Financing Risks*, 13
[47] U.S. Department of Treasury. *National Terrorist Financing Risk Assessment: 2015*, 16
[48] Matthew Levitt, "*Countering ISIL Financing: A Realistic Assessment*" (Speech), February 2, 2015
[49] Colin P. Clarke, *Terrorism, Inc. The Financing of Terrorism, Insurgency and Irregular Warfare*, 6

of providing financial support, "In the ongoing Syrian conflict," where organizations "from Kuwait and Qatar have allegedly funneled money to Salafist jihadist organizations."[50] Transnational terrorist networks utilize "couriers, wire transfers, hawalas and exchange houses to move funds to Syria, as an example."[51]

Transnational terrorist organizations, as Dr. Clarke identified, do not restrict their activities to the *gray economy*. As the CRS noted, these individuals and groups are increasingly embracing the use of criminal and other illegal activities for the express purpose of generating funds. FATF documented several trends that support their [CRS] conclusions of *dark economy* economic activity:

1. ***Generating revenue from criminal activities (i.e. production and sale of illegal narcotics)***: Criminal and terrorist organizations will engage in illegal activities for revenue, with the sale of narcotics a prominent example. The latest estimate from the UNODC is the global drug trade alone is worth around $435 billion USD annually.[52] Specific to terrorist financing, FATF recently studied the opiate trade in Afghanistan. Research found, "that the multi-million dollar profits of drug trafficking networks have leaked into the funds of terrorist organizations, and according to the United Nations, "out of the total 2011/2012 budget of the Taliban of USD 400 million – one third was raised from the poppy trade."[53] Beyond the narcotics trade, often forms of criminal activity utilized for transnational terrorist financing include credit card fraud (which can bleed over into the gray economy).
2. ***Kidnapping for ransom (KFR)***: KFR remains a growing source of revenue for transnational terrorist organizations, including IS. FATF notes several key points associated with this

[50] Colin P. Clarke, *Terrorism, Inc. The Financing of Terrorism, Insurgency and Irregular Warfare*, 6
[51] U.S. Department of Treasury. *National Terrorist Financing Risk Assessment: 2015*, 16
[52] Holly Ellyatt, "Global Drugs Trade As Strong As Ever As Fight Fails, CNBC, 13 August 2013, Accessed 24 March 2016, http://www.cnbc.com/id/100957882
[53] Financial Action Task Force (FATF), *FATF Report: Emerging Terrorist Financing Risks*, 16

revenue source, highlighting the, "US government estimates that, between 2008 and 2014, terrorists including AQ, ISIL and both affiliates and allies, generated at least USD 222 million in ransom payments."[54] Complicating this situation further, terrorist groups often require the physical delivery of cash through couriers, or use of alternative remittance systems such *hawalas*.

3. ***Nation-state sponsorship***: The United States and other countries, over the last several decades, attempted to use diplomatic efforts and economic sanctions to restrict state financial sponsorship of criminal and terrorist organizations. Despite these efforts, "states continued to directly fund terrorist groups."[55] Iran and their patronage of Hizballah serve as a primary example, with the latter receiving hundreds of millions of dollars in financial support. Additionally, researchers in the area of terrorist financing conclude insurgencies receiving external support are substantially more likely to outlast counterinsurgency efforts and ultimately overthrow incumbent regimes or force concessions than those without a foreign patron. This can apply to other methods of criminal or terrorist financing, but state sponsorship provides a consistent stream of funding.
4. **"Foreign terrorist fighters (FTFs)**: FTFs present a growing and dangerous emerging method of transnational terrorist financing, as they often rely on small, individual contributions or self-funding. The risk associated with FTFs is the small amount of funding these individuals require. Even within global financial institutions themselves, the quantity is often too low for detection, or appears as legitimate financial activity. FATF notes that foreign fighters are not a new phenomenon, but its scale dramatically increased with the recent fighting taking place in Syria and Iraq. More importantly, "While FTFs are not

[54] Financial Action Task Force (FATF), *FATF Report: Emerging Terrorist Financing Risks*, 18
[55] U.S. Department of Treasury. *National Terrorist Financing Risk Assessment: 2015*

presently considered to be a significant source of funding for IS or Al-Nusrah Front (ANF), they contribute to the larger TF threat posed by these groups…and are considered one of the main forms of material support to terrorist groups."[56] Additionally, FTFs are frequently self-funded individuals, meaning that they do not require the tradition forms of terrorist financing. These fighters simply can utilize legitimate sources of income, in the gray economy, for supplies and travel to a particular combat zone. Beyond legal income means, FATF also identified other revenue streams utilized specifically by ISIL FTFs:

- "Proceeds of robbery and drug trafficking
- Social benefits, from unemployment to family allowances
- Non-paid off consumer loan, below 10,000 euros, withdrawn in cash
- Opening several bank accounts and use of bank overdraft limit to withdraw cash
- Donations by family, friends and supporters, raised through social media (addressed in next topic), and sent by cash or wire transfers"[57]

As one example out of potentially thousands, Terri Nicholson, "from the [London] Metropolitan Police's counter-terrorism command unit said **that taxpayers' money was being claimed** frequently and used by terrorists in countries such as Iraq and Syria."[58]

[56] Financial Action Task Force (FATF), *FATF Report: Emerging Terrorist Financing Risks*, 24
[57] FATF, *Financing of the Terrorist Organisation Islamic State in Iraq and Levant (ISIL)*, 22
[58] Peter Dominiczak, Christopher Hope and Tom Whitehead, "Jihadists Funded by Welfare Benefits, Senior Police Warns," *The Telegraph*, 26 November 2014. Accessed on 20 March 2016, "http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/11256882/Jihadists-funded-by-welfare-benefits-senior-police-officer-warns.html

IV. UNDERSTANDING TRANSNATIONAL TERRORIST FINANCING AS A WICKED PROBLEM

The next step in this paper's discussion is connecting the macro-level state of transnational national terrorist financing and *distributed terrorist financing*, and demonstrating how it links to the concept of a *wicked problem*. Are the efforts by government and the financial industry working to counter transnational terrorist financing, or is new thinking required? Nick Ridley, Senior Lecturer in Policing and Security at the London Metropolitan Police, states in his book *Terrorist Financing: The Failure of Counter Measures*, that current countermeasures are ineffective. In reflecting on his reasoning, this paper will focus on events following 9/11, as the enactment of the US PATRIOT ACT of 2001, United Nations (UN) Resolution 1373, and the passage of New York State law outlawing money laundering, all of these being significant catalysts for a dramatic increase in AML/CTF efforts.[59] As Mr. Ridley states, "Terrorist financing was not left alone by international law enforcement, and efforts have been made to CTF. Ridley nevertheless sees such efforts as failures, "for three principle reasons:" legal complications, lag in adaptation and lack of strategic mindset.

1. ***The inherent and multiple legal difficulties involved in anti-terrorist financing measures***: Prior to the 9/11 AQ terrorist attacks, "international legal efforts against financing of terrorism were comparatively few and ill-supported."[60] The passage of the US PATRIOT Act and United Nations Resolution 1373, which specifically directed member states to "implement effective measures against terrorist financing, marked in Mr. Ridley's view "a high point in terms of the extent to which individual states were actively and effectively

[59] Nick Ridley, *Terrorist Financing: The Failure of Counter Measures*, 53
[60] Nick Ridley, *Terrorist Financing: The Failure of Counter Measures*, 53

pressurized."[61] For example FATF, "recognized as the global anti-money laundering and counter-terrorist financing"[62] international strategy body,[63] attempted to standardize guidelines and AML measures. The Egmont Group of financial intelligence units (FIUs)[64] tried to lay the groundwork for increased AML/CTF coordination and information sharing between nation-state FIUs. Lawmakers and government agencies directed regulatory instructions to the financial industry on how to operate in this dramatically increased compliance environment. Nevertheless, the multi-jurisdiction nature of the global financial system, along with "difficulty caused by a lack of an accepted and internationally codified definition of terrorism"[65] continued to result in significant international barriers. A simple Google search of UN websites confirms the lacking of a consistent definition of terrorism. While just a single issue, the fact that UN members cannot agree on even a uniform definition of terrorism indicates a lack of consistency and effective cross-border coordination. Resulting compliance regulations, by nation-states and non-governmental organizations (e.g. FATF), and the required implementation by the financial industry, are potentially at odds. The recent IS attacks in Brussels, for example, illustrate the failures associated with this principle reason.[66]

2. A failure to perceive the full significance of the modus operandi of terrorist financing:

Mr. Ridley contends that "the second cause of the failure of international efforts against

---

[61] Nick Ridley, *Terrorist Financing: The Failure of Counter Measures*, 55

[62] Financial Action Task Force (FATF), *FATF Report: Emerging Terrorist Financing Risks*, October 2015. ii

[63] Nick Ridley, *Terrorist Financing: The Failure of Counter Measures*, 54

[64] The Egmont Group of Financial Intelligence Units is an international network designed to improve interaction among FIUs in the areas of communication, information sharing and training cooperation. Its primary purpose is to combat money laundering and terrorist financing, and currently has 151 member states with centralized FIUs. For example, the Financial Crimes Enforcement Network (FinCEN) is the US government FIU. More information is available at http://www.egmontgroup.org/

[65] Nick Ridley, *Terrorist Financing: The Failure of Counter Measures*, 51

[66] Viktoria Dendrinou, "Brussels Attacks Expose Europe's Scant Progress on Security," *The Wall Street Journal,* 24 March 2016, accessed 10 April 2016, http://www.wsj.com/articles/brussels-attacks-expose-europes-scant-progress-on-security-1458829690

terrorist financing is that of a failure to perceive the full significance of the various *modus operandi* (method of operation) of terrorist financing."[67] In this area, he makes the assertion that government stakeholders are behind in discovering new forms of terrorist financing, or neglect methods such as trade-based money laundering, counterfeiting of goods and cash couriers. The consequences ultimately can cascade down to the financial services industry, whose constituents configure their internal AML/CTF compliance programs to comply with government laws, regulations and requirements.

As an example, he highlights two specific areas demonstrating the slow response of regulators and the industry: stored value/pre-paid cards,[68] and trade-based illicit transfers.[69] While those are just two examples, there is ample evidence to support Mr. Ridley's position. For stored value/pre-paid card products, Saudi Arabia's FIU reported in 2015 that the IS was actively using social network for fundraising with prepaid cards, including from European Union (EU) member states.[70] The European Union, however, has been slow to enact effective AML rules around prepaid cards, with some evidence mounting that the November 2015 IS Paris attacks utilized this method for storing of illicit funds. At of the writing of this paper, the European Commission is still drafting stricter rules, with proposed rules for the 27-nation union scheduled for release by June 2016.[71]

With respect to Mr. Ridley's trade based illicit transfer example, the situation is even more sobering, with some officials describing it as "a ready-made vehicle for dirty

---

[67] Nick Ridley, *Terrorist Financing: The Failure of Counter Measures,* 65
[68] Nick Ridley, *Terrorist Financing: The Failure of Counter Measures*, 105
[69] Nick Ridley, *Terrorist Financing: The Failure of Counter Measures*, 109
[70] FATF, *FATF Report: Emerging Terrorist Financing Risks*, 33
[71] Francesco Guarascio, "EU to step up checks on Bitcoin, prepaid cards to fight terrorism," *Reuters*, 2 February 2016, accessed 10 April 2016, http://www.reuters.com/article/us-eu-terrorism-financing-idUSKCN0VB1N7

money." [72] As an example, the Global Financial Integrity (GFI), a Washington D.C. based non-profit organization focused on studying illicit financial flows (IFF), estimated in a December 2015 report that a total of $1.1 trillion USD of illicit, trade-based outflows from developing countries (which generally have weaker AML/CTF controls, as compared to the US) took place in 2013 alone.[73] The organization identified two primary methods, deliberate trade mis-invoicing (gross excluding reversals or GER) and leakages in balance of payments (hot money narrow or HMN),[74] with four-fifths of this activity "linked to arms smuggling, drug trafficking, terrorism or public corruption."[75] Overall, the rise of trade based illicit transfers, particularly from developing countries, is attributed to the following reasons:

1. Increasing number of free-trade zones
2. Lack of government and industry cross-border information (e.g. establishment of trade transparency units[76]) sharing agreements
3. Increasing scale of global trade

[72] The Economist, "Uncontained," *The Economist*, 3 May 2014, accessed 10 April 2016, http://www.economist.com/news/international/21601537-trade-weakest-link-fight-against-dirty-money-uncontained

[73] Dev Kar and Joseph Spanjers, "Illicit Financial Flows from Developing Countries: 2004-2013," Global Financial Integrity, December 2015, viii

[74] Dev Kar and Josepoh Spaniers, "Illicit Financial Flows from Developing Countries: 2004-2013," viii

[75] The Economist, "Uncontained"

[76] The Economist, "Uncontained"

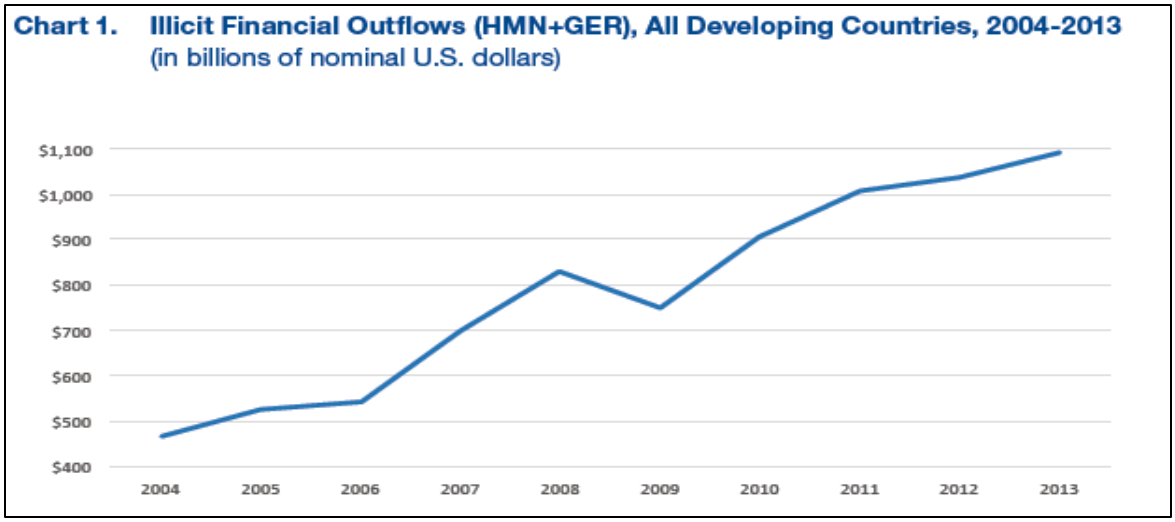


Table 2: Global Financial Integrity, IFF Outflows from Developing Countries[77]

3. ***The strategic mindset of government and law enforcement intelligence agencies."***[78] In his third reason, Mr. Ridley states that government officials have a "narrow strategic mind-set."[79] There is a lack of full appreciation of the funding acquisition and transmission potential of transnational terrorism organizations. In other words, because of this narrow mind-set, there is a "delayed recognition by government and law enforcement intelligence of terrorist financing *modus operandi*."[80] The key takeaway is that government stakeholders still engage in a game of *whack a mole*, failing to see larger trends around transnational terrorist financing, or fail to appreciate the adaption of traditional methods. Micro-level achievements and a near constant, underestimation of these nefarious groups create a false sense of effectiveness. Along with a lack of effective international legal and information sharing coordination, the terrorist financing *modus operandi* remains elusive.

In addition to the above reasons for failure, it is just as pertinent to discuss the coordination between government and the financial services industry, specifically within the

[77] Dev Kar and Josepoh Spaniers, "Illicit Financial Flows from Developing Countries: 2004-2013," 2
[78] Nick Ridley, *Terrorist Financing: The Failure of Counter Measures,* 6
[79] Nick Ridley, *Terrorist Financing: The Failure of Counter Measures,* 207
[80] Nick Ridley, *Terrorist Financing: The Failure of Counter Measures,* 207

US. There is little doubt the subprime mortgage crisis and resulting Great Recession had a toxic impact on this relationship, and had cascading consequences with respect to AML/CTF compliance. Since the crisis, regulatory agencies came under increased scrutiny over enforcement, with elected officials placing increased pressure to enforce new or existing regulations. A high profile, emblematic, example of this dynamic took place in March 2013 before the US Senate Banking Committee. At a hearing examining the HSBC $1.9 billion USD deferred prosecution agreement with the Department of Justice,[81] Senate members (in particular Sen. Elizabeth Warren (D-MA)) grilled regulators from the Department of Treasury and Federal Reserve[82] on the lack of criminal action against HSBC and other financial institutions (See Appendix A for further discussion). Increased regulatory pressure does not excuse a lack of compliance, or willful neglect, on the part of financial institutions. What it does demonstrate, however, is the industry is now **reactive** to the government, and there is a lack of a shared strategic mindset between these significant stakeholders.

Mr. Ridley is not alone in this conclusion. In a 2014 report by the *Center on Law and Globalization*, and with the agreement of the International Monetary Fund (IMF),[83] the report's authors came to a sobering conclusion: "There is substantial skepticism about the efficacy of global systems and national regimes to control money laundering and the financing of terrorism."[84] Michael Levi of Cardiff University, Peter Reuter of the University of Maryland and Terence Halliday (Co-Director, *Center on Law and Globalization*), the report's authors,

[81] Office of Public Affairs, "HSBC Holdings Plc. and HSBC Bank USA N.A. Admit to Anti-Money Laundering and Sanctions Violations, Forfeit $1.256 Billion in Deferred Prosecution Agreement, " US Department of Justice, 11 December 2012

[82] Linette Lopez, "Elizabeth Warren Savaged A Treasury Official During A Hearing On HSBC's International Money Laundering Scandal," *Business Insider*, 7 March 2013, accessed 10 April 2016

[83] Terence Halliday, Michael Levi, and Peter Reuter, "Global Surveillance of Dirty Money: Assessing Assessments of Regimes to Control Money-Laundering and Combat the Financing of Terrorism," *Center on Law & Globalization,* University of Illinois, College of Law, 30 January 2014, 4

[84] Terence Halliday, Michael Levi, and Peter Reuter, "Global Surveillance of Dirty Money: Assessing Assessments of Regimes to Control Money-Laundering and Combat the Financing of Terrorism," 9

"studied the global anti-money laundering system, that it may facilitate some criminal investigations and prosecutions, but at best, it **snares just a fraction of 1 percent of criminal income inflows**."[85]

Despite the billions of dollars spent by government and the financial industry to detect and stop the flow of illicit funds, a criminal or terrorist organization enjoys a favorable playing field that is only going to improve do to distributed operations. Globalization, digitalization and the introduction of disruptive financial technologies open new methods for transnational terrorist organizations to ***distribute their financing*** that government, law enforcement and even the private sector are struggling to monitor. While it could tie into Ridley's second principle of understanding terrorist financing's *modus operandi*, this paper contends that the dramatic, transformational changes taking place in the financial services industry are significant enough to consider separately.

The following case study illustrates the macro-level problem facing stakeholders in the government and financial industry:

Case Study: Bank Robbery at the Point of a Keystroke

In February 2016, cyber thefts successfully stole approximately $81 million US dollars (USD) from a Bangladesh central bank account held at the Federal Reserve Bank of New York.[86] As reported in the *New York Times*, "hackers appeared to have been intent on transferring nearly $1 billion USD out of Bangladesh's account, with nearly three dozen messaging requests. They

[85] Charles Kenny, "Why the World Is So Bad at Tracking Dirty Money," *Bloomberg*, 23 February 2015, accessed 3 April 2016, http://www.bloomberg.com/news/articles/2015-02-23/why-the-world-is-so-bad-at-tracking-dirty-money

[86] Rick Gladstone, "Bangladesh Bank Chief Resigns After Cyber Theft of $81 Million," *The New York Times*, 15 March 2016, accessed 16 March 2016, http://www.nytimes.com/2016/03/16/world/asia/bangladesh-bank-chief-resigns-after-cyber-theft-of-81-million.html

succeeded in four requests, totaling $81 million, to move money to the Philippines."[87] The transfer's significance to the Philippines as the destination country is that Manila-based casinos ultimately received the funds as part of the perpetrators money-laundering scheme. Casinos and other gambling institutions are not subject to the country's already weak anti-money-laundering (AML) laws, thus making these entities not subject to any reporting or monitoring requirements to detect or stop suspicious financial activity.[88]

While the perpetrators of this electronic heist remain at large and unknown, the possibility that a transnational terrorist or criminal organization, or individual(s) for that matter, were able to execute this robbery is sobering. The nefarious beneficiary not only successfully stole funds across nation-state borders, but also manipulated payment order messages, which were, in the words of a short statement from the New York Fed, "fully authenticated by the SWIFT[89] (*Society for Worldwide Interbank Telecommunication*) messaging system in accordance with standard authentication protocols."[90] What this single example captures is the essence of the *wicked problem*: Despite efforts by stakeholders determined to detect and stop transnational, illicit financing, the dilemma persists. Cyber thefts successfully got the Federal Reserve Bank of New York, a financial institution operating under some of the strictest and most robust AML/CTF and fraud regulations globally, to electronically transfer a central bank's funds to a private entity in Manila. Let that sink in for a moment.

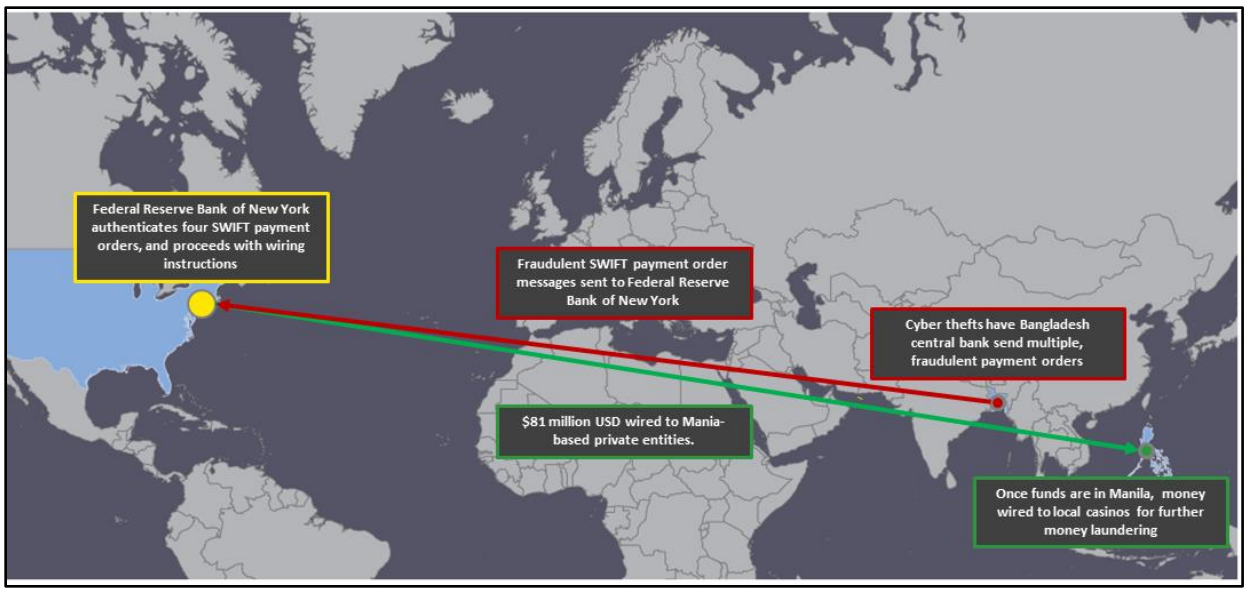
---

[87] Rick Gladstone, "Bangladesh Bank Chief Resigns After Cyber Theft of $81 Million"

[88] Cris Larano, "Casino-Junket Operator Turns Over $4.63 Million in Central-Bank Theft Case," *The Wall Street Journal*, 31 March 2016, accessed 1 April 2016, http://www.wsj.com/articles/casino-junket-operator-turns-over-4-63-million-in-central-bank-theft-case-1459435114. Casino-junket operator Kim Wong turned over part of the stolen funds to Philippine authorities, and has not been implicated in any wrongdoing.

[89] The *Society for Worldwide Interbank Telecommunication* (SWIFT) is a cooperative directly owned by financial institutions utilizing its messaging services. It does not initiate a funds transfer, but rather provides a secure, financial messaging service for financial institutions to send payment order instructions. More information is available at https://www.swift.com/

[90] Federal Reserve Bank of New York, "Statement on Media Reports About Bangladesh," *Federal Reserve Bank of New York*, 9 March 2016, accessed 16 March 2016, https://www.newyorkfed.org/newsevents/statements/2016/0311-2016



	The Wicked Problem Statement	Case Study	Result
Terrorist Financing	Transnational, terrorist or criminal organizations have the motivation and will to finance their activities. Globalization and digitalization of the financial system exposes vulnerability of exploitation, cyber hacking and digital theft	Steal $1 billion USD from a Bangladesh central bank account held by the Federal Reserve Bank of New York	Successful illicit funds transmission of $81 million USD to Philippine casinos
Financial System[91]		A Bangladesh government account domiciled in the United States illicitly transmits $81 million USD to the Philippines	Weak, Philippine AML laws and regulations with respect to casinos creates a window of opportunity to exploit across nation-state borders
		Nefarious actors manipulate SWIFT messages to legitimize and mask illegal payment order requests	The New York Fed's fraud detection countermeasures fail, resulting in the transmission of funds to the Philippines
	Disruptive technologies		
Government	Law enforcement and national security agencies attempt to stop and capture illicit funds through the enforcement of laws and regulations. Mandated by lawmakers, the financial industry must implement policies, procedures and necessary infrastructure for detecting and reporting suspicious, illicit activity	In an attempt to grow the casino and gambling business in the Philippines, competing with other hubs such as Macao, the Philippine government exempts casinos from AML regulatory requirements	Philippine AML laws with respect to casinos are weak, as these non-banking financial institutions are not subject to the country's monitoring and reporting requirements
Financial Industry		The New York Fed has AML and fraud compliance programs in place to meet regulatory requirements, but fail as the illicit activity is legitimized by manipulated SWIFT messages	The nefarious actors digitally exploited a vulnerability in the New York Fed's monitoring systems, resulting in the funds transfer

Table 3: Summary table of Bangladesh central bank case study

This single episode is impressive by its scale, ability to use the global financial system, the manipulation of SWIFT messages, and exploitation of regulatory gaps. Nevertheless, it is but one event existing within an annual, trillion-dollar dilemma. Utilizing *distributed terrorist*

[91] Disruptive technologies are not relevant to this particular case study, but other examples will address this. The key takeaway from the Bangladesh central bank example is the scale and brazen nature of the illicit financing act.

financing[92] nefarious organizations have at their disposal the necessary resources to amass funds through multiple avenues. Additionally, while this example demonstrates a high quantity value of illicit activity, "modern terrorists need little money for their operations."[93] Despite the time and resources dedicated by government officials and stakeholders in the financial industry, transnational terrorist (and criminal) organizations continue to successfully generate, transmit and use illicit funds on a daily basis. Instead of attempting to solve this problem, it is important to acknowledge the following: Transnational terrorist financing is a *wicked problem* that will never have a permanent solution. What it requires, rather, ever-evolving responses to an ever-changing environment amid a constant monitoring of the larger systemic problem.

Defining the Wicked Problem

What exactly is a *wicked problem*? Academics in the field of design and urban planning first utilized the phrase, describing a problem that, "[has] innumerable causes, is tough to describe, and doesn't have a right answer."[94] In 1973 Horst W. J. Rittel and Melvin M. Webber, professors from the University of California, Berkeley, co-authored an article defining wicked problems, and their corresponding properties. Critical of *desired outcomes* planning and using scientific bases in addressing social problems, Rittel and Webber sought to highlight a key fact, "The kind of problems that planners deal with --- societal problems --- are inherently different from the problems scientists and perhaps some classes of engineers deal with. Planning

[92] Megan Eckstein, "A Year Into Distributed Lethality, Navy Nears Fielding Improved Weapons, Deploying Surface Action Group," *United States Navy Institute News,* 13 January 2016, accessed 23 March 2016. https://news.usni.org/2016/01/13/a-year-into-distributed-lethality-navy-nears-fielding-improved-weapons-deploying-surface-action-group.
[93] Michael Levi and Peter Reuter, "Money Laundering," Crime and Justice: A Review of Research, Vol. 34*;* 289
[94] John C. Camillus, "Strategy as a Wicked Problem"

problems are inherently wicked."[95] How transnational terrorist financing fits this description is that government and financial industry stakeholders face a societal problem:

> *"As distinguished from problems in the natural sciences, which are definable and separable and may have solutions that are findable, the problems of governmental planning (*in this case, detecting and stopping transnational terrorist financing*) --- and especially those of social and policy planning --- are ill-defined; and they rely upon elusive political judgment for resolution (Not "solution." **Social problems are never solved. At best they are only re-solved --- over and over again**)…The problems that scientists and engineers have usually focused upon are mostly "tame" or "benign" ones. As an example, consider a problem of mathematics…the mission is clear. It is clear, in turn, whether or not the problems have been solved."*[96]

Using this proposition, the questions facing those focused on detecting and stopping transnational terrorist financing are the following:

1. ***Is the planning problem of detecting and stopping transnational terrorist financing ill defined?*** By using Rittel and Webber's approach, the answer is yes. This is not because of an inability to identify what transnational terrorist financing is, nor does it arise from any lack of information on trends and methods. FATF and the US Department of Treasury National Terrorist Financing Risk Assessment (NTFRA) provide such data. The problem is that supposedly clear goals (e.g. detect and stop transnational terrorist financing) do not have clear solutions. Already in 2005, questions were arising as to whether the solutions mandated by government towards the financial industry were working, As stated, "Many experts, both in government and the private sector, admit that the chances of detecting terrorists' funds in a bank sufficiently far in advance of a planned attack that it can be prevented are incredibly small."[97] The comment may be ten years old, but it is certainly

---

[95] Horst W. J. Rittel and Melvin M. Webber, "Dilemmas in a General Theory of Planning," *Policy* Sciences, 4, 1973. 160

[96] Horst W. J. Rittel and Melvin M. Webber, "Dilemmas in a General Theory of Planning," 160

[97] "Financing Terrorism: Looking the Wrong Places," *The Economist*, 20 October 2005, accessed 25 March 2016, http://www.economist.com/node/5053373

worth answering again today. Are our efforts working, or would a cost-benefit analysis (however challenging) of AML/CTF regimes and compliance programs reveal negative results?

2. ***Is there a permanent solution, or rather a continuous cycle of temporary resolutions?*** Transnational terrorist financing is a problem that is resolved continuously. As an example, trade-based money laundering, the emergence of digital products and disruptive financial technologies, such as virtual currencies, show the need for further resolutions that are not cookie-cutter in nature from past ones. These methods, products and transformations enable the further distribution of illicit acquisition and transmission means. In addition, nefarious organizations do not simply abandon traditional methods because of the introduction of a new tool, but rather include it within a repertoire of distributed operations. As. Dr. Clarke identified:

> *"Combating terrorist financing, and in particular the financing of groups like AQ and IS, is challenging because these groups and their fund-raising schemes are ever moving targets in many cases. In response to government counter-measures, the methods of financiers and [terrorist] cells adjust in kind."*[98]

3. ***Does political judgment dictate an acceptable solution or resolution, if possible?*** Violent, non-state organizations inherently are political organizations, threatening the existence, vital interests or economic well-being of other nation-states, as IS threatens Iraq. To combat these groups and hinder their financing efforts, governments such as the United States enact laws and regulations, and use the instruments of national power (e.g. military and law enforcement, regulatory actions) to achieve a prescribed resolution. Questions surround feasibility of dictating a permanent solution, but political judgment can determine that a sufficient, albeit elusive and temporary, resolution (Ritter and Webber view resolutions as

[98] Colin P. Clarke, *Terrorism Inc.*, 172

requiring constant refinement and evaluation, and are not permanent) may satisfy the problem. With this situation, however, comes another problem: are the solutions imposed by government on the financial industry positive? This is a question that is beginning to gain traction for several reasons. Stakeholders lack any cost-benefit analysis on whether industry efforts, which aim to **comply with federal and state regulations,** are "actually effective in reducing money laundering and other financial crimes."[99] Additionally, AML/CTF compliance costs continue to increase, which can result in financial institutions engaging in de-risking (further discussion in next section).

A *wicked problem* does not contain the clarity and focused solutions often sought by individuals and groups engaged in solving the problem. Rittel and Webber outlined ten distinguishing properties to identify this situation, which Dr. John C. Camillus of the University of Pittsburgh summarizes in his *Harvard Business Review* piece:

[99] Ng, Michelle, Geoffrey Sant, and Lanier Saperstein. "The Failure of Anti-Money Laundering Regulation: Where is the Cost-Benefit Analysis." *Norte Dame Law Review Online* 91, no. 1 (December 2015): 3.

1. There is no definitive formulation of a wicked problem. It's not possible to write a well-defined statement of the problem, as can be done with an ordinary problem.
2. Wicked problems have no stopping rule. You can tell when you've reached a solution with an ordinary problem. With a wicked problem, the search for solutions never stops.
3. Solutions to wicked problems are not true or false, but good or bad. Ordinary problems have solutions that can be objectively evaluated as right or wrong. Choosing a solution to a wicked problem is largely a matter of judgment.
4. There is no immediate and no ultimate test of a solution to a wicked problem. It's possible to determine right away if a solution to an ordinary problem is working. But solutions to wicked problems generate unexpected consequences over time, making it difficult to measure their effectiveness.
5. Every solution to a wicked problem is a "one-shot" operation; because there is no opportunity to learn by trial and error, every attempt counts significantly. Solutions to ordinary problems can be easily tried and abandoned. With wicked problems, every implemented solution has consequences that cannot be undone.
6. Wicked problems do not have an exhaustively describable set of potential solutions, nor is there a well-described set of permissible operations that may be incorporated into the plan. Ordinary problems come with a limited set of potential solutions, by contrast.
7. Every wicked problem is essentially unique. An ordinary problem belongs to a class of similar problems that are all solved in the same way. A wicked problem is substantially without precedent; experience does not help you address it.
8. Every wicked problem can be considered to be a symptom of another problem. While an ordinary problem is self-contained, a wicked problem is entwined with other problems. However, those problems don't have one root cause.
9. The existence of a discrepancy representing a wicked problem can be explained in numerous ways. A wicked problem involves many stakeholders, who all will have different ideas about what the problem really is and what its causes are.
10. The planner has no right to be wrong. Problem solvers dealing with a wicked issue are held liable for the consequences of any actions they take, because those actions will have such a large impact and are hard to justify.

Table 4: The Ten Properties of Wicked Problems[100]

It is important to note that a wicked problem does not have to connect with all ten distinguishing properties. The summary outlined by Dr. Camillus helps identify criteria are, "not a set of tests that mechanically determine wickedness;[101] in a certain degree, they provide insights that help one judge whether a problem is wicked."[102] The key takeaway from this section is defining a *wicked problem*, how to identify it and why "traditional processes" will not result in a solution. Dr. Camillus further notes that not only do conventional processes fail to tackle wicked problem, they may in fact exacerbate situations by generating undesirable consequences. Arguably, the attempt to regulate the problem out of existence by monitoring the large volume of global monetary transactions generated pressure for transnational terrorist organizations to distribute the "lethality" of terrorist financing, so as to evade detection.

[100] John C. Camillus, "Strategy as a Wicked Problem"
[101] Rittel and Webber do not mean to personify these properties of social systems by implying malicious intent (See page 161). The properties are not ethically deplorable, but use the term in a meaning akin to that of "malignant," in contrast to "benign."
[102] John C. Camillus, "Strategy as a Wicked Problem"

V. TRANSNATIONAL TERRORIST FINANCING WICKED PROBLEM PROPERTIES

So what…why does it matter to identify transnational terrorist financing as a *wicked problem*? The reason why is, as Mr. Ridley and the *Center of Law and Globalization* study spell out, the current solutions used by government and stakeholders in the financial industry are potentially ineffective despite massive financial, technical and personnel investments. Part of appreciating this involves viewing transnational terrorist financing as a *wicked problem* for the following reasons:

1. ***There is no definitive formulation of a wicked problem***. In order to have a well-defined problem, "an exhaustive formulation can be stated containing all the information the problem-solver needs for understanding and solving the problem."[103] Transnational terrorist financing cannot meet the criteria of a well-defined problem, because knowledge of all conceivable solutions is required. Take the example of a chess match. While there are numerous, even thousands of potential moves available to the two opponents, there are a finite number of them in order to win, and knowledge of all conceivable solutions is possible. The key point is that all necessary information is available to define the problem.

Start with the following, simple problem statement: Transnational terrorist financing is harmful. => Who is it harmful to? => The United States. => Why is it harmful? => Because it negatively affects US security. => Why does it negatively affect US security? Do we have to consider other states? If another state benefits from this nefarious activity, what course of action can the US use? The problem statement initiates a sequence of follow-on inquires, attempting to discover a solution to an ill-defined problem. The conclusion is that the transnational terrorist financing problem has no definitive formulation.

[103] Horst W. J. Rittel and Melvin M. Webber, "Dilemmas in a General Theory of Planning," 161

2. ***Wicked problems have no stopping rules***. A person reaches a solution to transnational terrorist financing when the activity completely halts, and has no negative effect on security. The reality, however, is that this situation is not possible. The evidence presented with respect to this problem show that it continues, and the individuals or groups developing solutions do not know if their job is complete, or even successful. Rittel and Webber establish the condition of having no stopping rules as a matter of resources rather than resolution. "The planner terminates work on a wicked problem, not for reasons inherent in the "logic" of the problem. He stops for considerations that are external…out of time, money, or patience."[104]

In similar fashion, the financial services industry continues to dedicate a greater amount of resources to their AML/CTF compliance programs, but continue to express concern with the challenges of complying with government regulations. Financial institutions do not have infinite resources, and see emerging risks with sustaining and improving their internal AML/CTF programs. *LexisNexis* and the *Association of Anti-Money Laundering Specialists* (ACAMS) conducted a 2015 survey of AML/CTF compliance personnel from the financial industry, and concluded that significant concerns exist for their [AML compliance programs] ability to address the *wicked problem*.[105] The following table illustrates the risk concerns within the financial industry, with greater and changing regulatory requirements the two most significant concerns:

[104] Horst W. J. Rittel and Melvin M. Webber, "Dilemmas in a General Theory of Planning," 162
[105] LexisNexis and Association of Anti-Money Laundering Specialists, Current Industry Perspectives into Anti-Money Laundering Risk Management and Due Diligence, LexisNexis, December 2015, 6

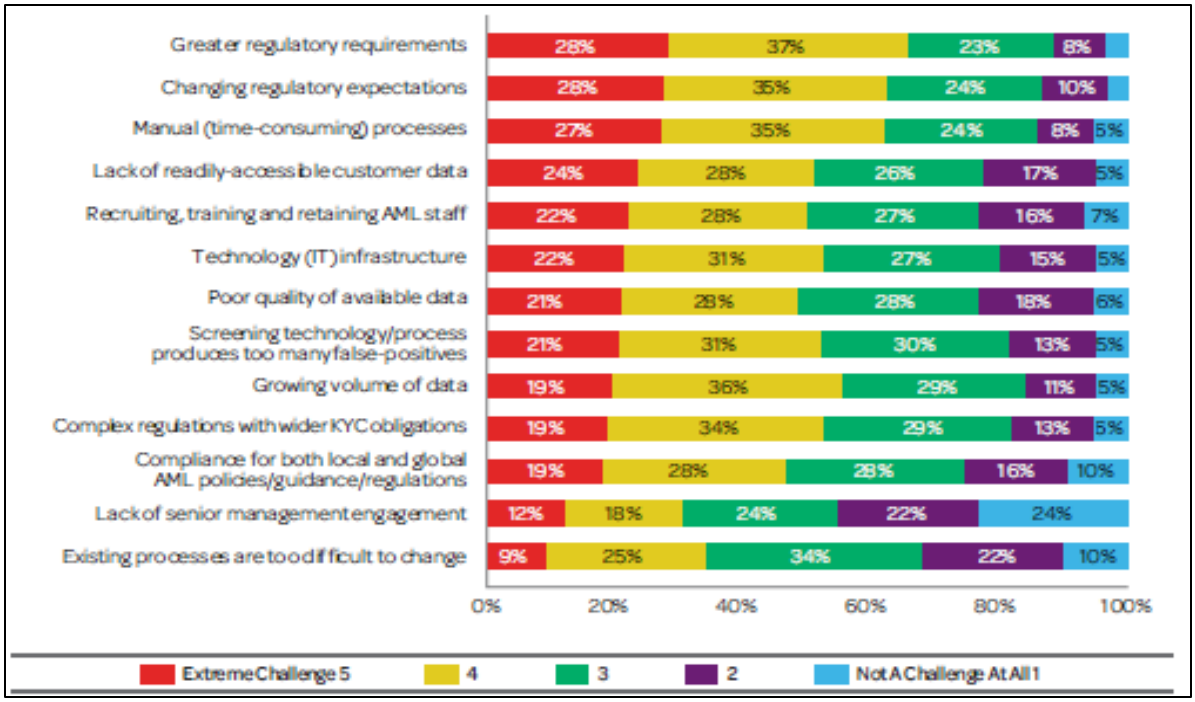


Table 5: LexisNexis AML Survey: Greatest Challenges Identified: AML Risk Assessment[106]

3. ***Solutions to wicked problems are not true or false, but good and bad.*** "Choosing a solution to a wicked problem is largely a matter of judgment."[107] This is certainly the case with the problem of transnational terrorist financing and legality. The UN and FATF attempted a level of global standardization but "difficulties of definition and creating specific terrorist offences have led to differing perceptions"[108] on identifying terrorist financing. This point connects to Nick Ridley's first reason why past countermeasure efforts failed: inherent and multiple legal difficulties create a subjective environment that is not globally consistent. In addition, there is criticism directed at organizations such as FATF and the IMF, where their "assessments focused almost entirely on formal compliance with FATF standards and whether countries appeared to implement programs. Very little emphasis, if any, was given to program or outcome

[106] LexisNexis and Association of Anti-Money Laundering Specialists, Current Industry Perspectives into Anti-Money Laundering Risk Management and Due Diligence, 27
[107] John C. Camillus, "Strategy as a Wicked Problem"
[108] Nick Ridley, *Terrorist Financing: The Failure of Counter* Measures, 52

effectiveness."[109] This may be the case for regulators themselves, as they may now care more about how much a financial institution spends on AML/CTF compliance programs, rather than focusing on their effectiveness.[110] The reason for this may be that regulators use this as a simple metric for reporting to lawmakers, demonstrating a particular regulation's effectiveness in their eyes.

4. ***There is no ultimate test of a solution to a wicked problem***. The key consideration of this property is that, "with wicked problems…any solution, after being implemented, will generate waves of consequences over an extended---virtually an unbounded---period of time…and may yield utterly undesirable repercussions which outweigh the intended advantages or advantages accomplished."[111] An example of this situation is a financial institution engaging in ***de-risking***, which FATF defines as a, "phenomenon of financial institutions terminating or restricting business relationships with clients or categories to avoid, rather than manage, risk in line with the FATF'S risk-based approach."[112] It can have unintended consequences, such as having a high-risk AML customer transact in less regulated environments, and hurt legitimate commerce as well. As a recent, high profile example:

> *"In July 2015, Citigroup agreed to pay $140 million in penalties to federal and California regulators for purported anti-money laundering weaknesses at its Banamex USA subsidiary. On the same day, Citigroup announced it would close Banamex USA. The two events are almost certainly linked, as the fine imposed on Banamex USA equaled roughly one-sixth of the bank's assets."*[113]

---

[109] Terence Halliday, Michael Levi, and Peter Reuter, "Global Surveillance of Dirty Money: Assessing Assessments of Regimes to Control Money-Laundering and Combat the Financing of Terrorism," *Center on Law & Globalization,* University of Illinois, College of Law, 30 January 2014

[110] Ng, Michelle, Geoffrey Sant, and Lanier Saperstein. "The Failure of Anti-Money Laundering Regulation: Where is the Cost-Benefit Analysis." 5.

[111] Horst W. J. Rittel and Melvin M. Webber, "Dilemmas in a General Theory of Planning," 163

[112] FATF, "FATF clarifies risk-based approach: case-by-case, not wholesale de-risking, 23 October 2014, accessed 21 March 2016, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-and-de-risking.html

[113] Ng, Michelle, Geoffrey Sant, and Lanier Saperstein. "The Failure of Anti-Money Laundering Regulation: Where is the Cost-Benefit Analysis." 2.

Whether Citigroup was deserving of this regulatory action is beside the point. The fact is that the financial institution is closing Banamex USA, and all remittance activity, primarily to Mexico, potentially might take place in a less regulated or surveilled construct. Even worse, illegal methods may gain attractiveness, like the *Black Peso Money Exchange* utilized by Columbian drug cartels for money laundering. Regulators used a solution of fines and deferred prosecution against financial institutions. Justified or not, the action had the unintended consequence of de-risking.

5. ***Every solution to a wicked problem is a "one-shot" operation; because there is no opportunity to learn by trial and error, every attempt counts significantly***. In order to meet the criteria of this property, "every implemented solution is consequential…and every attempt to reverse a decision or to correct for the undesired consequences poses another set of wicked problems, which in turn are subject to the same dilemmas."[114] While halting the implementation of a solution at the micro-level may be possible, at the macro-level this is extremely difficult due to the time, effort and resources law enforcement, regulators and the industry itself invest in detecting and stopping transnational terrorist financing. The previous example of de-risking fits this property again as the consequence is that regulators aggressively penalize financial institutions for what they perceive to be lax or non-compliant AML/CTF monitoring programs. As a result, institutions may decide to de-risk and avoid the problem altogether, creating unintended results. An example of this phenomenon is Merchants Bank of California. Complying with FATF rules, the bank "cut money transfers to Somalia…between $160 million and $180 million."[115] Faced with potential regulatory liabilities, the bank decided on a de-risking course of action, despite no evidence of any wrongdoing. There is the potential that

[114] Horst W. J. Rittel and Melvin M. Webber, "Dilemmas in a General Theory of Planning," 163
[115] Charles Kenny, "Why the World Is So Bad at Tracking Dirty Money"

remittance payments by Somali expatriates may use "less savory financial institutions as intermediaries,"[116] or the *hawala* exchange system.

6. ***Wicked problems do not have an exhaustively describable set of potential solutions, nor is there a well-described set of permissible operations that may be incorporated into the plan.*** "There are no criteria which enable one to prove that all solutions to a wicked problem have been identified and considered."[117] The introduction of disruptive financial technologies, such as virtual currencies and mobile payment systems, and the opportunities they present to violent, non-states organizations show that further solutions remain. The nature of the problem continues to change, unlike a game of chess that "has a finite set of rules, accounting for all situations that can occur."[118]

7. ***Every wicked problem is essentially unique***. To explain this property statement, Rittel and Webber add, "Despite seeming similarities among wicked problems, one can never be *certain* that the particulars of a problem do not override its commonalities with other problems already dealt with."[119] In other words, the risk of transnational terrorist financing may have similarities to other cross-border security issues, but the particular characteristics of finance create a uniqueness where a one-size fits all solution to all cross-border issues is not possible. What is also unique to transnational terrorist financing is that the vast majority of information and monitoring, much like with information technology companies such as Facebook, takes place within private enterprises. This situation creates legal and infrastructure barriers between the government and financial industry, and across the industry itself. For example, the financial

[116] Charles Kenny, "Why the World Is So Bad at Tracking Dirty Money"
[117] Horst W. J. Rittel and Melvin M. Webber, "Dilemmas in a General Theory of Planning," 164
[118] Horst W. J. Rittel and Melvin M. Webber, "Dilemmas in a General Theory of Planning," 164
[119] Horst W. J. Rittel and Melvin M. Webber, "Dilemmas in a General Theory of Planning," 165

industry reports their findings to the government through suspicious activity reports (SARs). This is a unique characteristic, and places a dependency of law enforcement on a private entity.

8. ***Every wicked problem can be considered a symptom of another problem*****:** The basic notion of this property is that a wicked problem "is entwined with other problems, and those problems [do not] have one root cause." A simple demonstration of how transnational terrorist financing meets these criteria is the on-going criminal and terrorist activities of AQ and IS.

9. ***The existence of a discrepancy representing a wicked problem can be explained in numerous ways*****:** The way to understand this property is that, "[a] wicked problem involves many stakeholders, who all have different ideas about what the problem really is and what its causes are."[120] As outlined in the introduction, this particular problem has numerous stakeholders in law enforcement, national security and regulatory agencies, non-governmental organizations such as FATF and the industry itself. Segmenting these groups further by nation-state authority or country of domicile make it's evident that this problem has many stakeholders." The case study involving the New York Fed, Bangladesh central bank and Philippine casinos demonstrate this point.

Similar to property #2, this aspect has further significance. As stated earlier, transnational terrorist financing is a societal problem, and thus subject to a wide range of views on the part of individual stakeholders from the government and financial industry. In connection with Ridley's third reason for the failure of,[121] government and financial industry stakeholders focused on detecting and stopping of transnational terrorist financing often have a mindset that does not appreciate other views. From a government perspective, an unregulated financial system is not possible because of risk and political considerations, but one cannot turn off the global financial

[120] John C. Camillus, "Strategy as a Wicked Problem"

[121] Countermeasures Ridley focuses on intelligence and law enforcement, but for the discussion it will expand to all stakeholders

system, as this is not possible. As a result, regulation is necessary. From the private sector perspective, compliance is an overhead cost of meeting these regulatory requirements that is not offset by revenue. Unless regulations are in place, the financial industry may not take any action to address terrorist financing, viewing it as the responsibility of government to enact laws and regulations. This attitude can inhibit a strategic mindset among all stakeholders.

10. ***The planner has no right to be wrong*****:** In this property, "planners are liable for the consequences of the actions they generate."[122] While it is simple to associate this with the actions of law enforcement or military personnel, AML compliance personnel working at financial institutions face a similar situation. As recently as January 2016, "A U.S. District Court in Minnesota ruled that compliance officers and other individuals can be held responsible for anti-money laundering control failures under the Banking Secrecy Act, dealing a setback to a former chief compliance officer who was hit with a $1 million fine by the Financial Crimes Enforcement Network (FinCEN)."[123] This example stems from regulatory action against former Moneygram Chief Compliance Officer Thomas Haider, and his case of a compliance team member held responsible, by the government, for AML control failures. The individual, and not just the institution, is potentially liable, even if acting in good faith. This judgment may ultimately rest with the regulators or courts.

Key Take Away Point

Since this paper established how transnational terrorist financing links to the *wicked problem* properties, the final part is to identify key take away points. To begin with, government regulators and financial industry stakeholders risk examining this problem in a linear fashion.

---

[122] Horst W. J. Rittel and Melvin M. Webber, "Dilemmas in a General Theory of Planning," 167

[123] Stephen Dockery, "Court Rules Anti-Money Laundering Law Applies to Compliance Officers," *The Wall Street Journal,* 13 January 2016, accessed 21 March 2016, http://blogs.wsj.com/riskandcompliance/2016/01/13/court-rules-anti-money-laundering-law-applies-to-compliance-officers/

What the connection to the wicked problem properties demonstrates is the need to avoid this pitfall. Along with the need of a unifying, strategic mindset amongst all AML/CTF stakeholders, it is necessary to acknowledge that solutions implemented in the hopes of cementing a permanent fix are not possible.

Additionally, it is just as important for all stakeholders, whether regulators, law enforcement of the industry itself to recognize each other's goals and limitations. It is simple to state that everyone has a goal to detect and stop transnational terrorist financing. It is another to acknowledge the constraints and restraints that each must contend with on a daily basis. The following section will build off this point, and outline initial recommendations for the consideration of AML/CTF stakeholders.

VI. CONCLUSION AND INITIAL RECOMMENDATIONS

This thesis' intention is to encourage a rethinking of the transnational terrorist financing problem, through the lens of a *wicked problem*. Following the properties developed by Rittel and Webber, it established that the planning problem of detecting and stopping illicit financing is ill-defined, there are only continuous cycles of temporary resolutions vice a permanent solution, and finally, political judgement plays a significant role in determining a resolution's acceptance. To provide evidence and justification for the previous stated findings, evidence was presented with respect to each question, and the ten properties of a *wicked problem* developed. Despite this and the monumental task facing those individuals and organizations trying to stop violent, transnational terrorist organizations, it remains possible to discover new, more effective resolutions.

Nick Ridley has strong evidence in stating that AML/CTF efforts have been generally ineffective, due to the three principle reasons around a lack of legal uniformity, understanding a terrorist organization's *modus operandi* and need for a strategic mindset. As this thesis proposes, there is a fourth principle reason involving globalization, digitalization and the introduction of disruptive financial technologies requiring separate consideration. The government and financial industry invests billions of USD, employs thousands of individuals and deploys infrastructure to combat terrorist financing, yet the problem persists and evolves to the tune of *at least* $800 billion USD annually. Nefarious organizations now have at their disposal distributed means to achieve violent ends. Whether through traditional methods such as private donations via *hawalas*, or criminal cyber ransom payments via a virtual currency, the challenge is daunting…***but not impossible***. A *wicked problem* is not impossible to solve, but does require alternative thinking. It is not a game of chess! A game of chess has finite solutions, and unless

the world is going to turn off the global financial system tomorrow, it will require a continuous cycle of resolutions. This is a systemic, nonlinear view of the world, involving a feedback loop of iterative reassessment leading to continual updating and refinement of mitigation measures, along with a constant recalculation of risk and cost-benefit analysis.

It is the recommendation of this paper that stakeholders in government and the financial industry consider the following recommendations and topics for initial consideration:

1. **Cost-benefit analysis of the AML regime**: As sourced in this paper, several individuals in academia and the industry are highlighting the need for a cost-benefit analysis of the AML regime. This paper does not minimize the difficulty of this proposal, or its ultimate feasibility. Nevertheless, it is vital that actions taken by government regulators and the financial industry are not only effective, but does not do more harm than good. The issue around de-risking highlighted a *wicked problem* property around unintended consequences, and is an appropriate starting point. In addition, Terence Halliday, Professor Michael Levi and Professor Peter Reuter lay out in their analysis immediate steps both FATF and the IMF can take to with respect to program and outcome effectiveness. These can initially, and at the very least, provide top-down guidance, and bottom-up feedback.
2. **Standardized legal definitions**: Getting the UN to agree on a definition of terrorism may be a bridge too far, given the inherit gridlock of the organization and conflicting interests. That being said, non-governmental organizations such as FATF and the IMF can not only codify standard legal definitions, but also push member nation-states to meet this. Beyond standardizing legal definitions, this can have the effect of aiding the development of effective, cost-benefit analyses around the many issues involving transnational terrorist financing.

3. **A strategic mindset**: This recommendation presents the greatest challenge. Nick Ridley is correct on the necessity of having a strategic mindset for AML/CTF, but that requires buy-in and leadership. Buy-in to AML/CTF efforts in 2001 took the death of thousands and billions of USD in damage. The next catalyst has the potential to make 9/11 look minor in comparison, and even this event did not result in a strategic mindset. It is, however, not impossible. It can start, but not end, with a renewed dialogue between US regulators, law enforcement and the financial industry beyond conferences, where boilerplate question and answer sessions take place but little progress takes place. In order to develop a strategic mindset, it will require more frequent interaction, beyond bank examinations or SAR reporting, so that each stakeholder has a better understanding of the goals and concerns of the other. The government has legitimate security concerns. At the same time, so does the financial industry with respect to cost and necessities of running a business. Building the framework of a strategic mindset requires trust and confidence between stakeholders, and each entity has a vested interest in developing this environment.

Developing resolutions to the transnational terrorist financing *wicked problem* will require time, effort and the will on the part of government and industry. Trust and confidence are critical components, along with a baseline of global, legal standardization. Finance and information sharing are issues filled with emotion and privacy concerns. This should, however, not create insurmountable roadblocks towards tackling the *wicked problem*, and combat violent organizations that inflict pain and suffering on millions of people annually.

APPENDIX A: U.S. AML/CTF REGULATIONS OVERVIEW

The US government, other nation-states and international organizations as early at 1970 recognized the dangers money laundering posed. Starting in 1970 with passage of the Currency and Foreign Transactions Reporting Act, also known as the Bank Secrecy Act (BSA), the USG took initial steps to combat criminal and terrorist financing. This act passed by Congress, "established requirements for record keeping and reporting by private individuals, banks and other financial institutions."[124] The BSA's purpose was to monitor the movement of currency in and out of the United States and financial institutions. The recordkeeping requirement was codified into law, enabling law enforcement and regulatory entities to more effectively investigation potential illegal activities. Between 1970 and 2001, additional acts, such as the Money Laundering Control Act of 1986[125] expanded the reach and requirements of the BSA. (See *Figure XX* for detailed timeline) It was not until the events of September 11, 2001 that significant changes came into law with respect to combating terrorist financing and money laundering.

Following the 9/11 attacks committed by *al-Qaeda*, the US Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, better known as the USA PATRIOT Act. The USA PATRIOT Act, "is arguably the single most significant AML law that Congress has enacted since the BSA itself,"

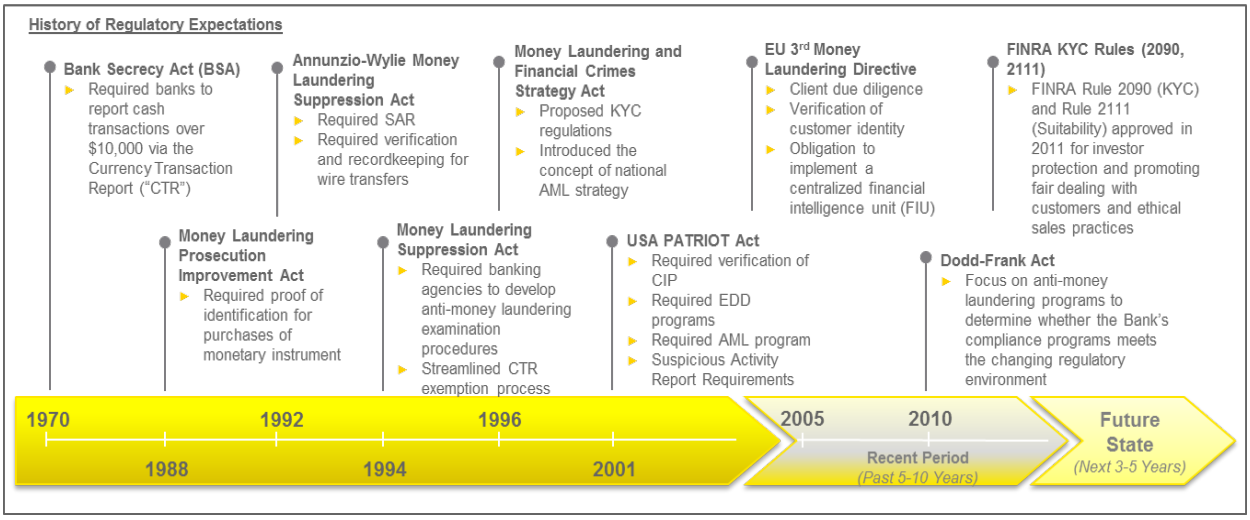
[124] FFIEC, 8

[125] The Money Laundering Control Act of 1986 augmented the BSA's effectiveness, applying the law's sections equally to banks of all charters by the FFIEC. In addition, the act precluded circumvention of the BSA requirements by imposing criminal liability on a person or financial institution that knowingly assists in the laundering of money, or that structures transactions to avoid them.

criminalizing "the financing of terrorism and augmented the existing BSA framework."[126] Title III[127] of the Act codified AML measures including,

1. Strengthening customer identification procedures (CIP) required by financial institutions
2. Prohibit financial institutions from engaging in business with foreign shell banks
3. Require financial institutions institute due diligence procedures, known as customer due diligence (CDD), and enhanced due diligence (EDD) for foreign "correspondent accounts"[128] and "private banking"[129] accounts
4. Improve information sharing between USG agencies and financial institutions
5. Expanded AML program requirements to all financial institutions
6. Increased civil and criminal penalties for money laundering

The chart depicts a high level evolution of the regulatory landscape over the past 40 years. Over this time, regulatory agencies have steadily increased the requirements for financial institutions



[126] FFIEC, 9

[127] Title III is referred to as the International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001

[128] FFIEC, 116. A correspondent account is an account established by a bank for a foreign bank to receive deposits from, or to make payments or other disbursements on behalf of the foreign bank, or to handle other financial transactions related to the foreign bank.

[129] FFIEC, 130. Private banking is broadly defined as providing personalized financial services to wealthy clients

As the above chart illustrates, the level of USG legislation passed into law steady increased over the last 40 years. Additionally, since the enactment of the PATRIOT Act, the USG through various regulatory agencies such the Office of the Comptroller of the Currency (OCC) and the Federal Reserve Board (FRB) placed increasing pressures on financial institutions to improve their anti-money laundering (AML) compliance programs. Since the financial crisis, elected officials demanded greater action on the part of regulators to enforce federal law. While the financial crisis dealt primarily with issues outside of criminal and terrorist financing (i.e. sub-prime mortgage crisis), the effect was nevertheless the same for all compliance issues. Since 2010 numerous globally, multi-billion dollar financial institutions were the subject of large regulatory fines and action. Some of the more notable fines and regulatory actions include:

1. **November 2012**: Wilmington-based First Bank of Delaware had its Federal Deposit Insurance Corporation (FDIC) insurance and state banking charter revoked, along with a $15 million USD civil penalty, for "failing to implement an effective anti-money laundering compliance program,"[130] and knowingly knew about fraudulent transactions taking place within the institution. The revoking of the bank's charter effectively put it out of business.
2. **December 2012**: London-based HSBC paid an approximately $1.9 billion USD fine for, as described by then U.S. Attorney Loretta Lynch, "blatant failure to implement proper anti-money laundering controls facilitated the laundering of at least $881 million in [Mexican cartel] drug proceeds through the U.S. financial system."[131]

[130] "First Bank of Delaware Loses Charter over AML Problems," *The Wall Street Journal*, November 19. 2012, accessed January 25 2016, http://blogs.wsj.com/corruption-currents/2012/11/19/first-bank-of-delaware-loses-charter-over-aml-problems/

[131] "HSBC Admit to AML and Sanctions Violations," U.S. Department of Justice, accessed 25 January 2016, http://www.justice.gov/opa/pr/hsbc-holdings-plc-and-hsbc-bank-usa-na-admit-anti-money-laundering-and-sanctions-violations

3. **June 2014**: Paris-based BNP Paribas, "agreed to plead guilty to criminal charges and pay an $8.9 billion penalty…BNP hid the names of Sudanese and Iranian clients when sending transactions through its New York operations and the broader American financial system."[132]

[132] "BNP Paribas Admits Guilt and Agrees to Pay $8.9 Billion Fine to U.S." *New York Times*, June 30, 2014, accessed on 25 January 2016, http://dealbook.nytimes.com/2014/06/30/bnp-paribas-pleads-guilty-in-sanctions-case/

APPENDIX B: ILLICIT FUND MOVEMENT TECHNIQUES

The Department of Treasury's *National Terrorist Financing Risk Assessment* identifies the following methods for the movement of illicit funds: "the physical movement of cash and the movement of funds through the banking system."[133] Criminal and terrorist organizations use the following mechanisms to move their illicit assets:

1. *Funds Transfers through Banks*: "The banking sector continues to be the most reliable and efficient way to move funds internationally, and remains vulnerable to terrorist financing."[134] This is primarily due to the global reach, speed and convenience that financial institutions provide as part of their services. Major US financial institutions such as JPMorgan Chase, Citibank or Wells Fargo can quickly and efficiency transfer funds globally, either to a branch within the institution, or through a correspondent banking relationship with a foreign financial institution.

   Additionally, "because of the importance of the United States to global financial market activity, many foreign banks have established subsidiary branches or agencies in the United States to gain access to U.S. based customers and to serve their own customers' needs."[135] Individuals and entities use the banking sector to transfer cash, electronic funds (EFT) such as a wire transfer, or monetary instructions (MI) (i.e. personal checks, traveler's checks). Think of this setup as the *meat and potatoes* of the global financial system: the movement of funds. Due to the tremendous value and volume this entails, criminal and terrorist organizations exploit this by setting up accounts for the express purpose of originating (sender) funds, and transferring them to a beneficiary (receiver of funds).

---

[133] U.S. Department of Treasury. *National Terrorist Financing Risk Assessment: 2015*, 46
[134] Financial Action Task Force (FATF), *FATF Report: Emerging Terrorist Financing Risks*, 20
[135] U.S. Department of Treasury. *National Terrorist Financing Risk Assessment: 2015*

Along with funds transfer through financial institutions, the arrangement of *correspondent banking* relationships presents a significant terrorist financing risk. U.S. financial institutions do not maintain either a legal or physical presence in all countries globally, and vice versa. Access to U.S. markets is also vital to foreign financial institutions, as part of their product offering to their customers. As a result, "the international financial system in interconnected and foreign institutions maintain correspondent accounts at and receive services from U.S. financial institutions in order to access the U.S. financial system."[136] This arrangement allows for the efficient execution of cross border transactions.

The risk from correspondent banking relationships is that they are inherently risky, "in large part to the challenges of 'intermediation,' where multiple intermediary financial institutions may be involved in a single funds transfer transaction."[137] AML compliance measures implemented by US-based financial institution may not exist with foreign banks, and the complexities of cross-border transactions create increased vulnerability to exploitation. While the USG has legal requirements to mitigate this for US entities and those operating directly in the United States, significant risk remains. This is due in large part to foreign financial institutions having a riskier profile due to their geographic location, products and services offered customer type and insufficient AML programs.

2. *Money Value Transfer Systems (MVTS)*: MVTS exist for a variety of purposes that potential customers utilize for remittance. In locations where traditional banking services do not have a strong presence, "remittance providers may be the primary financial institution through which consumers can engage in cross-border funds transfer activities."[138] The World Bank estimates that the total value of remittance payments globally is, "USD 440 billion dollars in

[136] U.S. Department of Treasury. *National Terrorist Financing Risk Assessment: 2015*, 50
[137] U.S. Department of Treasury. *National Terrorist Financing Risk Assessment: 2015*, 50
[138] Financial Action Task Force (FATF), *FATF Report: Emerging Terrorist Financing Risks*, 22

2010, of which USD 325 million went to developing countries, involving some 192 million migrants."[139] Remittance payments are often a vital source of income for migrant families back in the country of origin, and frequently involve expensive transaction fees on the part of the transferring agent. As a result, migrant workers typically explore alternative methods for wiring money back home, instead of utilizing traditional money service businesses.

Money service businesses (MSB) are often the primary mechanism for remittance transfers, and consist of large multi-national corporations like Western Union, to small independent operators in local communities. As previously stated, MSB services typically charge expensive fees to wire funds, and customers explore alternative options. The Department of Treasury identified this as unlicensed money transmitters, which are "individuals and entities operating illegally as unlicensed money transmitters."[140] On prominent example of this type of unlicensed activity was the case of Saifullah Anjum Ranjha, whom operated in the District of Columbia. Over the course of four years, Ranjha and his associated transferred at least $2.8 million USD aboard to members of AQ and their affiliates. While Treasury and other regulatory agencies issued regulations to crack down on unlicensed operators similar to the example mention, these *gray economy* services remain available due to the large populations served, and desire of migrants and diaspora workers to avoid high service fees.

3. *Cash Smuggling*: Cash remains a popular product for terrorist financing because of it availability, anonymity and portability. As Treasury notes as the primary risk of cash

[139]http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTFINANCIALSECTOR/0,,contentMDK:22121552~menuPK:6127416~pagePK:210058~piPK:210062~theSitePK:282885~isCURL:Y,00.html
[140] U.S. Department of Treasury. *National Terrorist Financing Risk Assessment: 2015*, 53

smuggling, "It is difficult – if not impossible – to completely stop the use of cash smuggling, and thus it remains a residual terrorist financing risk."[141]

[141] U.S. Department of Treasury. *National Terrorist Financing Risk Assessment: 2015*, 56

APPENDIX C: VIRTUAL CURRENCY OVERVIEW

To understand the concept behind Bitcoin, or any virtual currency, "to work as cash, bitcoin had to be able to change hands without being diverted into the wrong account and be incapable of being spent twice by the same person."[142] Normally, a financial institution would act as the intermediary and trusted broker, ensuring the integrity of the transaction. Satoshi Nakamoto, however, focused on creating a decentralized system, and this required the development of a substitute. As a result, he created the *blockchain*, "a global public ledger containing all Bitcoin transactions ever made."[143] This global ledger contains two key parts:

1. ***Block***: is a sequence that contains transactions users are requesting to execute via their "wallets – software which accesses the *blockchain* rather as a browser accesses the web, **but does not identify the user of the system**
2. ***Hash***: is the "digital signature."[144] If one user proposing a change from one wallet to another user's wallet, confirmation of the change takes place. "As the proposal propagates over the network the various nodes check, by inspecting the ledger, whether the user actually has the bitcoin they want to spend." If confirmed, "specialized nodes called miners will bundle" the proposed transaction with other, similar "reputable transactions to create a new block for the blockchain."[145] **The hash does not contain data**, but rather signifying a change to the global ledger and is unique. In other words, "It is easy to go from the data to their hash; impossible to go from the hash back to the data." The diagram below outlines the entire process:

[142] The Economist, "The Great Chain of Being Sure About Things," *The Economist*, October 31, 2015, 21
[143] Joshua Baron et al, 11
[144] Joshua Baron et al, 12
[145] The Economist, "The Great Chain of Being Sure About Things,", 22

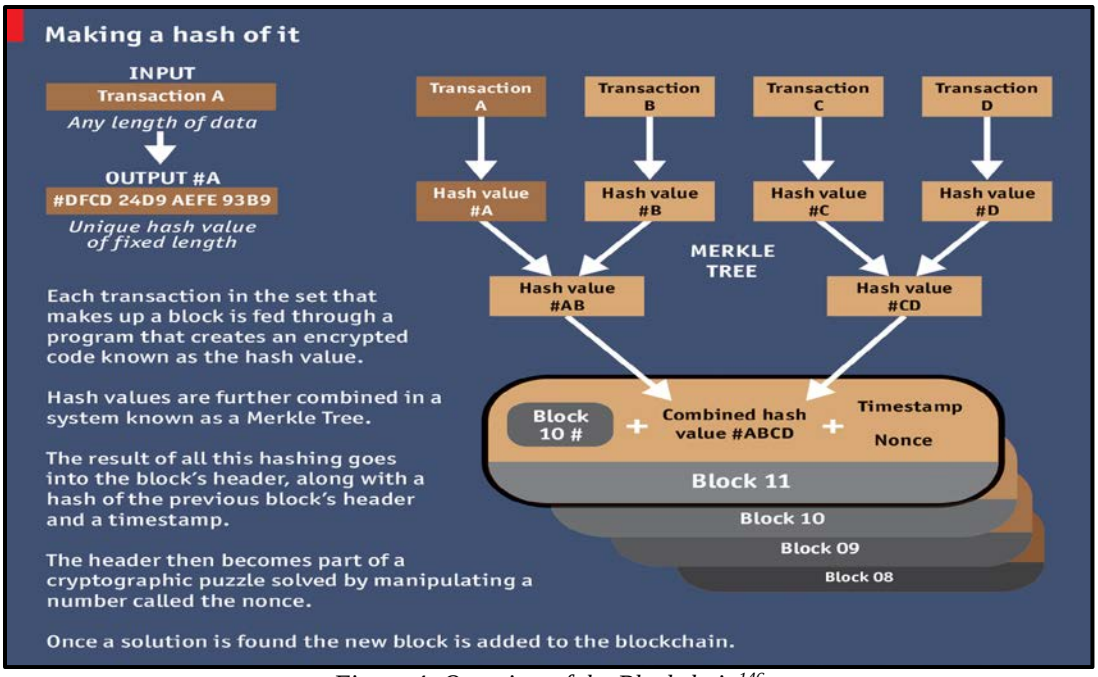


Figure 4: Overview of the Blockchain[146]

"Perhaps the most important distinction between Bitcoin and previous VCs is that while VCs do not technically require a central authority, one of Bitcoin's key features is its completely *decentralized* authority—and many VCs have followed Bitcoin precisely in this direction."[147] Once the new block is added to the global ledger, "the blockchain is distributed to all computers running the Bitcoin protocol; therefore all nodes in the Bitcoin network have a copy of all transactions ever made.[148] The VC provides decentralized control, with the global ledger as security through the following means outlined by *The Economist*:

- *Chance*: Individuals "cannot predict which miner will solve the puzzle, and so you cannot predict who will get to update the *blockchain* at any given time…this makes cheating hard."
- *History*: "Each new header contains a hash of the previous block's header, which in turn contains a hash of the header before that," and so on until the beginning of the *blockchain*. "It is this concatenation that makes the blocks into a chain." For example, if one attempted

[146] The Economist, "The Great Chain of Being Sure About Things,", 22
[147] Joshua Baron et al, 9.
[148] Joshua Baron et al, 12

to change a header from an earlier block, it will not match the latest block's unique identification, and would be rejected.

- *51% Attack*: The *51% attack* is a phrase meaning that an individual, in theory, controls more than half of the computers in a particular system. Why this is relevant to virtual currencies is that rule exists if someone wanted to manipulate the *blockchain*, he or she would not have sufficient time, as "the rest of the network would have lengthened the original *blockchain*. And the node always works on the longest version of the *blockchain* there is. This rule stops the occasions when two miners find the solution almost simultaneously from causing anything more than a temporary folk in the chain. It also stops cheating."

BIBLIOGRAPHY

Associated Press. *Mexico Got More Money from Remittances Than From Oil Revenues in 2015.* February 3, 2016. http://www.nbcnews.com/news/latino (accessed April 10, 2016).

Baron, Joshua, Angela O'Mahony, David Manheim, and Cynthia Dion-Schwarz. *National Security Implications of Virtual Currency: Examining the Potential for Non-State Actor Deployment.* Santa Monica: RAND Corporation, 2015.

Camillus, John C. *Strategy as a Wicked Problem.* May 2006. https://hbr.org/2008/05/strategy-as-a-wicked-problem (accessed March 19, 2016).

Clarke, Colin P. *Terrorism, Inc. The Financing of Terrorism, Insurgency and Irregular Warfare.* Santa Barbara: Praeger, 2015.

Commission, 9/11. *The 9/11 Commission Report.* Commission Report, Washington, DC: National Commission on Terrorist Attacks Upon the United States, 2004.

Dendrinou, Viktoria. "Brussels Attacks Expose Europe's Scant Progress on Security." *The Wall Street Journal*, March 24, 2016.

Dockery, Stephen. "Court Rules Anti-Money Laudering Law Applies to Compliance Officers." *The Wall Street Journal.* January 13, 2016. http://blogs.wsj.com/riskandcompliance/2016/01/13/court-rules-anti-money-laundering-law-applies-to-compliance-officers/ (accessed March 21, 2016).

Dominiczak, Peter, Christopher Hope, and Tom Whitehead. "Jihadists Funded by Welfare Benefits, Senior Police Warns." *The Telegraph.* London, November 26, 2014.

Eckstein, Megan. "A Year Into Distributed Lethality, Navy Nears Fielding Improved Weapons, Deploying Surface Action Group." *United States Navy Institute News.* January 16, 2016. https://news.usni.org/2016/01/13/a-year-into-distributed-lethality-navy-nears-fielding-improved-weapons-deploying-surface-action-group. (accessed March 23, 2016).

Economist, The. "Financing Terrorism: Looking the Wrong Places." *The Economist*, October 20, 2005.

—. "The Great Chain of Being Sure About Things." *The Economist*, October 31, 2015: 21-24.

—. "Uncontained." *The Economist*, May 3, 2014.

Ellyatt, Holly. "Global Drugs Trade As Strong As Ever As Fight Fails." *CNBC.* August 13, 2013.

Federal Financial Institutions Examination Council (FFIEC). *Bank Secrecy Act/Anti-Money Laundering Examination Manual.* Washington, DC: Federal Financial Institutions Examination Council (FFIEC), 2014.

Federal Reserve Bank of, New York. "Statement on Media Reports About Bangladesh." *Federal Reserve Bank of New York.* March 9, 2016. https://www.newyorkfed.org/newsevents/statements/2016/0311-2016 (accessed March 16, 2016).

Financial Action Task Force. *Emerging Terrorist Financing Risks: October 2015.* FATF Report, Paris: Financial Action Task Force, 2015.

Financial Action Task Force. *Financing of the Terrorist Organisation Islamic State in Iraq and Levant (ISIL).* Paris: Financial Action Task Force, 2015.

Forbes. "The World's Most Valuable Brands." *Forbes.* October 2015. http://www.forbes.com/companies/apple/ (accessed January 23, 2016).

Gladstone, Rick. "Bandladesh Bank Chief Resigns After Cyber Theft of $81 Million." *The New York Times.* March 15, 2016. http://www.nytimes.com/2016/03/16/world/asia/bangladesh-bank-chief-resigns-after-cyber-theft-of-81-million.html (accessed March 16, 2016).

Guarascio, Francesco. "EU To Step Up Checks on Bitcoin, Prepaid Cards to Fight Terrorism." *Reuters.* February 10, 2016.

Halliday, Terence, Michael Levi, and Peter Reuter. *Global Surveillance of Dirty Money: Assessing Assessments of Regimes to Control Money-Laundering and Combat the Financing of Terrorism.* Assessment Report, Center on Law and Globalization, University of Illinois, 2014, 4, 9.

International Monetary Fund. *Globalization: A Brief Overview.* 2008. www.imf.org/external/np/exr/lib/2008/053008.htm.

—. "World Economic Outlook Database, October 2015." *International Monetary Fund.* October 2015. http://www.imf.org/external/pubs/ft/weo/2015/02/weodata/weorept.aspx (accessed January 27, 2016).

Jost, Patrick M., Sandhu, Harjit Singh. *The Hawala Alternative Remittance System and its Role in Money Laundering.* Research Report, Financial Crimes Enforcement Network and INTERPOL, n.d.

Kar, Dev, and Joseph Spanjers. *Illicit Financial Flows from Developing Countries: 2004-2013.* Washington, DC: Global Financial Integrity, 2015.

Kenny, Charles. "Why the World Is So Bad at Tracking Dirty Money." *Bloomberg.* February 23, 2016. http://www.bloomberg.com/news/articles/2015-02-23/why-the-world-is-so-bad-at-tracking-dirty-money (accessed April 3, 2016).

Larano, Cris. "Casion-Junket Operator Turns Over $4.63 Million in Central-Bank Theft Case." *Wall Street Journal.* March 31, 2016. http://www.wsj.com/articles/casino-junket-operator-turns-over-4-63-million-in-central-bank-theft-case-1459435114. (accessed April 1, 2016).

Levi, Michael, and Peter Reuter. "Money Laundering." *Crime and Justice: A Review of Research*, n.d.: 289.

Levitt, Matthew. "Countering ISIL Financing: A Realistic Assessment." Washington, DC, February 2, 2015.

LexisNexis; Association of Anti-Money Laundering Specialists. *Current Industry Perspectives into Anti-Money Laundering Risk Management and Due Diligence.* Survey Report, LexisNexis, 2015.

Lopez, Linette. "Elizabeth Warren Savaged A Treasury Official During A Hearing On HSBC's International Money Laundering Scandal." *Business Insider*, March 7, 2013.

Moyer, Justin Wm. "After Computer Hack, L.A. Hospital Pays $17,000 in Bitcoin Ransom To Get Back Medical Records." *Washington Post*, February 18, 2016.

New York Times. "BNP Paribas Admits Guilt and Agrees to Pay $8.9 Billion Fine to U.S." *New York Times*, June 14, 2014.

Ng, Michelle, Geoffrey Sant, and Lanier Saperstein. "The Failure of Anti-Money Laundering Regulation: Where is the Cost-Benefit Analysis." *Norte Dame Law Review Online* 91, no. 1 (December 2015): 3.

Press, Cambridge University. *Where There's A Will There's A Way.* n.d. http://dictionary.cambridge.org/us/dictionary/english/where-there-s-a-will-there-s-a-way (accessed January 25, 2016).

Ridley, Nick. *Terrorist Financing: The Failure of Counter Measures.* Northamption: Edward Elgar, 2012.

Rittel, Horst W. J., and Melvin M Webber. "Dilemmas in a General Theory of Planning." *Policy Science*, 1973: 155-169.

Rollins, John, and Liana Sun Wyler. *Terrorism and Transnational Crime: Foreign Policy Issues for Congree.* Washington, DC: Congressional Research Service, 2013.

Rowden, VADM Thomas, RADM Peter Gumataotao, and Peter RADM Fanta. "Distributed Lethality." *Proceedings Magazine*, January 2015.

Sirkeci, Ibrahim, Jeffery H. Cohen, and Dilip Ratha. *Migration and Remittances During the Global Financial Crisis and Beyond.* Washington, DC: The World Bank, 2012.

The World Bank. *Personal Remittances, received (current US$).* March 21, 2016. http://data.worldbank.org (accessed March 21, 2016).

U.S Department of Treasury. *National Money Laundering Risk Assessment.* Washington, DC: U.S. Department of Treasury, 2015.

U.S. Department of Justice, Office of Public Affairs. *HSBC Holdings Plc. an HSBC Bank USA N.A. Admit to Anti-Money Laundering and Sanctions Violations, Forfeit $1.256 Billion in Deferred Prosecution Agreement.* Washington, DC: U.S. Department of Justice, 2012.

U.S. Department of Treasury. *National Terrorist Financing Risk Assessment: 2015.* Washington, DC: U.S. Department of Treasury, 2015.

—. *Resource Center: Money Laundering.* n.d. https://www.treasury.gov/resource-center/terrorist-illicit-finance/Pages/Money-Laundering.aspx (accessed January 11, 2016).

United Nations Office of Drug Control. *Money Laundering and Globalization.* n.d. https://www.unodc.org/unodc/en/money-laundering/globalization.html (accessed December 28, 2015).

Wall Street Journal. "First Bank of Delaware Loses Charter over AML Problems." *Wall Street Journal*, November 19, 2012.

World Bank. *World Economic Outlook Database, October 2015.* October 2015. www.imf.org/external/pubs/ft/weo/2015/02/weodata/weorept.aspx (accessed January 27, 2016).