Freezing Assets:

How the United States Lost the War on Terrorist Financing

Macalah Danielsen

On September 24, 2001, just thirteen days after the worst terrorist attack in history on U.S. soil, President George W. Bush signed an Executive Order that froze terrorists' assets, effectively identifying the disruption of terrorist financing as one of the primary weapons to be utilized in the War on Terror. At the time, Americans around the country were in a state of shock and rage, and, for the first time in years, they pulled together, collectively, regardless of political affiliation. Even policymakers put aside differences in order to push legislation through as quickly as possible which resulted in several new policies. At the time, it was a general belief that disrupting terrorist financing was the equivalent of preventing terrorist attacks, as capital is essential to terrorist group's success. However, despite the U.S. Department of the Treasury freezing approximately sixty million in 2015, ISIS still maintained a yearly income of 1.7 billion. Terrorism has remained a relevant threat to the U.S. in spite of efforts to counteract it through disruptions in funding and shifts in policy and strategy. Terrorist groups continue to adapt to current U.S. counterterrorism strategy and discover new financing methods as a result. This is not to say that the United States has made no progress in its fight against funding and would be better off abandoning this approach, but that more short-term and long-term solutions should be put in place alongside the current policies and initiatives. Short-term solutions such as the development of financial typologies, continuous research regarding the evolution of finances, flexible strategies, and improved collaboration between both the international and domestic agencies are needed in order to continue the fight against terrorist financing until a more long-term solution is reached. Additionally, the rise of the internet has played a significant role in funding processes as well as instant communication worldwide. Here I outline the relevancy of terrorism, the role and methods of financing, the responsibilities of several U.S. departments, and the counterterrorism measures of each since 9/11.

For methodology, I referred to John Gerring's *Case Study Research: Principles and Practices* in order to explain aspects of this paper. According to Gerring, a case study is "highly focused, meaning that considerable time is spent by the researcher analyzing, and subsequently presenting, the chosen case, or cases, and the case is viewed as providing important evidence for the argument" (Gerring, pg. 28).That said, the goal of this "small-C study" is to explain the chosen cases as well as relay the argument that current methods of disrupting terrorist financing are inadequate. Several sample cases regarding Al Qaeda, methods of terrorist funding and numerous recent attacks are drawn from, representing a descriptive "small-C study." On top of being a descriptive study, it is also typical which is to say the selected cases do not represent the entire distribution, but rather the central tendencies of a population. Nevertheless, it is also important to note the research designs of the study which include with-in case and cross-case. The with-in case is analyzed before the cross-case in order to identify the commonalities between the studies. Furthermore, this piece is qualitative due to the fact that each piece of information is relevant to the central argument. The argument discussed is valid both internally and externally as it demonstrates impartiality as well as relevancy (Gerring).

Relevancy of Terrorism

When discussing terrorism, it is important to note a key problem that affects every aspect of the subject – the lack of a universal definition. Furthermore, that statement also applies to agencies within the United States government. Each U.S. agency has a different definition of terrorism that reflects their various fields. Because there is no principle definition, cooperation and collaboration between countries is challenging for multiple political and legal reasons. The United States defines terrorism under the Federal Criminal Code stating that is consists of "…activities that involve violent… or life-threatening acts… that are a violation of the criminal

laws of the United States or of any State and… appear to be intended (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and…(C) occur primarily within the territorial jurisdiction of the United States…" (Various Definitions). Although, according to the Department of Defense, terrorism is "The unlawful use of violence or threat of violence, often motivated by religious, political, or other ideological beliefs, to instill fear and coerce governments or societies in pursuit of goals that are usually political" (DOD Dictionary). On the other hand, the Department of Homeland Security defines terrorism as "as an insider threat is an unlawful use of force and violence by employees or others closely associated with organizations, against those organizations to promote a political or social objective" (Terrorism). The Federal Bureau of Investigation holds that terrorism is "The unlawful use of force or violence against persons or property to intimidate or coerce a Government, the civilian population, or any segment thereof, in furtherance of political or social objectives" (Various Definitions). Even with differing agency definitions, violence resulting from terrorism can sometimes be difficult to distinguish from other crimes, such as hate crimes, homicides, and other state and non-state conflicts. Nevertheless, there are a few clear indicators when analyzing attacks, for instance: the purpose, the long-term effects, the damages and the targets.

Generally, terrorist acts have a distinct political, economic, religious, or social purpose. A crucial component of long-term effects is whether the assault was designed to have "far-reaching psychological repercussions beyond the immediate victim or target" (Ritchie, Hannah). Terrorists aspire to exploit the media and gain as much publicity as possible in order to influence an audience and achieve their (usually political) goals. There are also acts that include public or

private property damage which are part of various legal definitions of terrorism. Another staple in terrorist attacks is when civilians are targeted without discrimination. Because terrorist activity varies from year to year, so does the death toll. In 2017, there were approximately 26,445 confirmed deaths that were the direct result of a terrorist attack worldwide, however, one of the highest numbers was in 2014 reaching 44,490 deaths (Ritchie, 2019). Compared to 2001, with deaths as high as 7,729 because of 9/11, the sharp increase in casualties can be attributed to the rise in internet usage. Many find solace online with other like-minded people and more individuals are encouraged to act on their beliefs or in the name of certain terrorist organizations.

Financing is believed to be an essential component of terrorism, because, like all groups, capital is needed to keep it functioning. Terrorist organizations require money as well as other assets for obtaining weapons, "training, travel and accommodation to plan and execute their attacks and develop as an organization" (Terrorist Financing). However, the rise in inexpensive individual attacks suggest that funding isn't always an issue, which reasons that the focus on countering terrorist financing is ineffective when looking through a lone-wolf lens. Nevertheless, the current policies in place are directed towards disrupting the funding of organizations and have thus far failed to eliminate the terrorist threat in the Middle East. Because methods of financing are constantly evolving, it can be difficult for the United States to succeed in preventing the financing of terrorism with such inflexible policies and, as a result, the U.S. is constantly a few steps behind. Therefore, a flexible strategy is necessary, especially concerning virtual funding tactics. In order to fully understand the issue, one must have a grasp on the basic principles which is why the organization, Al Qaeda, will be discussed as an example prior to the analysis of the differences between funding streams; the basis of financing; how terrorist

organizations operate; forms of financing; cryptocurrency; the role of the internet in funding; and the elements of a funding cycle.

The Financing of Al Qaeda

Following 9/11, Al Qaeda transformed in a decentralized organization with three distinct but interlinked factions. There is the original group that was formerly led by Osama Bin Laden, the group that trains new recruits and serves as an example, and the group that consists of newly radicalized militants who form local cells. While these cells share the fundamental objectives with Al Qaeda, they are generally independent. However, like their more official counterpart, most if not all have resorted to diverse methods of crime to fund activities (del Cid Gómez, 2010). Apart from materials purchased specifically for attacks, such as weapons, vehicles and explosives, the organization also incurs the costs of maintaining itself, for instance the living expenses for members as well as their families, reliable channels of communication, training new recruits which require specialist skills like piloting aircraft, travel costs, propaganda, and, at times, social legitimization through charitable activities. As previously stated, Al Qaeda's fundraising activities are as diverse as they are illegal, for instance they utilize many charities or NGOs, companies or other entities, kidnapping, drug trafficking, robberies, credit card theft, and more. When it comes to countering terrorist financing, the U.S. attempts to freeze assets didn't affect Al Qaeda in the way it was intended, partially because of the previously stated methods of raising capital, but also the fact that members used Hawalas and cash couriers to move funds. However, surprisingly, enforcing the 'know your customer' regulation from the Bank Secrecy Act on financial institutions served to prevent several transactions from taking place.

It was discovered in the early 2000's that approximately one-third of Islamic nongovernment organizations (NGO) support terrorism by either funding groups or employing individuals with

terrorist connections. There are also cases in which the charities are legitimate – until they're infiltrated by corrupt employees. Osama Bin Laden utilized NGOs, such as the Global Relief Foundation (GRF) and the Al-Haramain Islamic Foundation, to secretly launder and funnel up to fifty percent of all donations in cash which served to conceal the group's financial network (Jacobson, 2010). Additionally, more funds are accumulated during the holy month of Ramadan, partly because corrupt employees gain access to mosques as well as zakat which is obligatory almsgiving (del Cid Gómez, 2010). Charities are an ideal target for terrorist organizations to exploit because while they have access to a significant amount of funds, they also have the confidence of the public. In order to deceive donors, charities may "create false documentation for the benefit of unwary donors, purportedly showing that the money had actually been spent on orphans or starving refugees" (Kohlmann). Not only did the charities launder money on behalf of Al Qaeda, they also provided assistance by moving funds into areas where they had ongoing operations.

Moreover, Al Qaeda used multiple offshore businesses and entities, such as those similar to Barakaat, to both finance itself and transfer funds. Barakaat operated in forty different countries and, not only funneled millions of dollars to Al Qaeda annually, but managed and invested their funds before distributing the money on behalf of them. Nevertheless, there are a multitude of other business activities that Al Qaeda has partaken in, for instance "the export of coal to the Middle East, the provision of transport, security and protection services, telecommunications, commercial centres, running hawalas and other financial services, agricultural and hotel companies and was even involved in the distribution of fishing rights" (del Cid Gómez, 2010).

Kidnapping and robbery as financing methods are much less common than drug trafficking or credit card fraud. Kidnappings usually only occur in Al-Qaeda in the Islamic Maghreb

(AQIM), which operates within the desert region between Mali, Mauritania and Algeria. Robberies are more common in Morocco as well as Spain, but the latter to a lesser extent. However, drug trafficking is also very prominent in both countries. Moroccan thieves specialize in modern technology, such as GPS, cellphones, etcetera. Lastly, stolen credit cards can be used to either buy supplies or fund a cell through false charges. Apparently, there was an Al Qaeda cell located in the United Kingdom that planned to carry out attacks there as well as the U.S. and Middle East using stolen credit cards to "buy items such as GPS systems, night vision goggles, sleeping bags, telephones, knives and tents from hundreds of websites" (del Cid Gómez, 2010).

Terrorist Financing Elements

Funding is how terrorists conduct operations, run organizations, and influence others to follow in their image. Terrorist groups depend on capital to sustain three primary funding streams: organizations, operations, and either individual or group operatives. While individual attacks do not require a substantial amount of funding, terror organizations can be compared to large companies that need a constant flow of funds to remain active and support operations. Individuals, also known as lone wolves, are either directed by a terrorist group or inspired by one. However, it is much more difficult to catch a lone wolf, despite that this classification of people are over thirteen times more likely to have a mental illness than their counterparts that work as part of a group (Worth, Katie).

Directed individuals are generally group members and are typically funded by the organizations, however, there are cases where an individual is self-funded, such as the attacks in and near Barcelona, Spain. In 2017, thirteen people were killed and at least another hundred injured after a van drove through a crowded tourist destination. Police arrested two suspects, although the driver got away. ISIS claimed responsibility for the assault, but it's believed that

this attack was related to another that occurred two days later when an Audi A3 containing five passengers drove into pedestrians, killing one. The perpetrators engaged in a shootout with the police and all were killed (Terrorist Attacks).

On the other hand, inspired individuals are mainly self-funded and act in the name of a group, which is to basically say the individual is not connected to a terrorist organization but are dedicating their actions to them. For example, in 2017, Sayfullo Habibullaevic Saipov, an inspired individual, rented a pickup truck and drove it down a busy bicycle path near the World Trade Center in New York. Eight people were killed and another twelve were wounded in the attack. A note claiming the assault was dedicated to ISIS was later found by authorities near the truck (Terrorist Attacks). In cases like these, it's almost impossible to predict an individual's actions by just looking at their finances and spending habits. Other details of the suspects life must be analyzed, such as internet content, political affiliation, and sometimes religion. Furthermore, the rise of the internet has enabled more individuals to act on their beliefs. It's a cheap tool that provides anonymity, fast communication, and information such as bomb building instructions (Zemen, Tomas).

The main differences between an operation and individuals lies in the amount of capital necessary to carry out the task. Operations are generally larger missions with more people involved which is more expensive. For instance, the 9/11 plot planned by Al Qaeda cost somewhere between $400,000 and $500,000 U.S. dollars, although most of the money had already been absorbed by the organization while they were still planning the operation. Before the hijackers arrived in the United States, funding went towards training camps at which the hijackers were chosen and trained, as well as their travel. After the hijackers arrived in the United States, they received roughly $300,000 through various methods which was spent on

"tuition for flight training, living expenses (room, board and meals, vehicles, insurance, etc.), and travel (for casing flights, meetings, and the September 11 flights themselves)" (Appendix). However, just before the flights, the hijackers returned around $26,000 to an Al Qaeda facilitator and later attempted to send back another $10,000 which the FBI seized after the operation.

The Role of the Internet

According to Louise Shelley and Nancy Hurst, there are five specific ideas that convey the most basic facts about terrorism throughout their statement. The first is that terrorists operate like organized crime groups and nearly all current terrorist organizations depend on illicit activities for funding. Typical forms of crime include counterfeiting, which is usually the least monitored type; meaning they have low risk with high profits. Oddly enough, this strategy provides terrorists with a double edge; gaining funds while destabilizing their enemies. However, with the rise of the Internet, there has been an understandable increase in cyber-related crimes and use of virtual currency such as Bitcoin, Litecoin, Ethereum, etcetera.

Originally, cryptocurrency was commonly used for purchasing illicit drugs and other goods. Currently, global money laundering organizations offer services that move as well as layer illicit profits into and through virtual currencies in order to make the trail more difficult to follow. Money laundering of physical capital and cryptocurrency is used as a reliable method of financing terrorist activities. It involves the three simple measures of placement, layering and integration.

The internet has played its own role in abetting the financing of terrorism. Terrorists and terrorist supporters utilize internet to fund organizations through legal and illegal online activity, such as credit card fraud, gambling sites, apps, charities, and other forms of payment. During the

early 2000s, Younis Tsouli, better known by his online code name "Irhabi 007," was one of the most prominent virtual terrorists of all time. He worked closely with Al Qaeda, posting their various videos and illegitimately raising money. Over the course of his two-year career, Tsouli and his partner, Tariq al-Daour, obtained over 37,000 stolen credit card numbers and had over 3.5 million dollars in charges. Tsouli was able to launder the money through multiple gambling sites before transferring it back into bank accounts established for that purpose. Terrorists have also begun using social media platforms to broadcast requests for financial support and raise capital. Furthermore, financiers can be identified when fundraising is accomplished through social media, but there are several factors that prevent authorities from apprehending the accused. As is the case with charities, some donors don't realize they are funding terrorists. As for the donors that are aware of who they are giving money to, they are encouraged to "use encrypted mobile applications that safeguard against external surveillance, posing a considerable challenge to counter-terror financing efforts" (Yuen, Stacey). Specifically, there is Telegram, a popular app used to transfer funds as well as coordinate recruitment. However, wire transfers are also widely used among supporters. As previously discussed, charities are used as fronts to collect funds and most utilize websites that either deceive potential donors or are honest about their activities. Nonetheless, charities and NGOs are a definite weak link in the fight against terrorist funding since "banned or exposed charities tied to terrorism can also shut down one day, and reopen the next under a new name—a tactic often used successfully by terrorist organizations" (Jacobson, 2010). Other forms of financing include transferring funds electronically through services like PayPal or by using cell phones to make M-payments. Incidentally, the newer policies inflicted by Paypal are meant to prohibit customers from laundering money, committing fraud or other financial crimes. That said, Paypal participates in

the Know Your Customer requirements by screening client names against government watchlists and requiring proof of identity (Paypal, 2019).

Elements of a Funding Cycle

Elements of a terrorist funding cycle consist of methods of raising, moving, storing, and spending money. Capital can be raised through both legitimate and illegitimate means. Lawful funding can come from private donations or commercial enterprises. On the contrary, illegitimate funding includes the illicit cigarette trade and natural resource trade, counterfeits, state sponsorship, and the trafficking of drugs, people, arms, and artifacts.

When it comes to moving money, there are several modes of physical transportation as well as virtual. Physical means include cash couriers, informal transfer systems, high value commodities, money service businesses, formal banking, and false trade invoicing. A cash courier is considered the simplest and most tried method of moving money, especially across uncontrolled borders. Money is often concealed in packages or luggage and requires prior arrangements and coordination.

A centuries old system originating from Asia, Hawalas are informal money transferring networks that are most common in places with limited to nonexistent formal banking institutions and, in an effort to regulate the business, some countries have legalized the practice (de Goede). However, because of high fees, many dealers choose to operate illegally. According to Marieke de Goede, “the defining aspect of informal money transfers is that they escape the formal accounting procedures of national governments and international institutions” (2003). Hawala networks were discovered by the U.S. government shortly after 9/11 as a method of moving money that leaves no paper trail, operating on cash and trust alone. Hawala is a quick way of

transferring money without physically moving it and can be accomplished within a day. For instance, if a man wants to send his wife cash then he can approach a Hawala and give them the money he wants to send. Because this is a business that requires multiple people, Hawalas are usually family operations. The first Hawala will contact a second Hawala in the area the husband wants to send the money and they will then give the first Hawala, as well as the husband, a code. It's the husband's job to give his wife the code so she can tell it to the second Hawala and they will give her the funds. Nevertheless, if funds need to be physically transferred then hawaladars have been known to use high value commodities, money service businesses, and false trade invoicing. High value commodities simply mean gold or diamonds, which are quick and easy to trade for cash but more difficult to move in high amounts. In addition, it cannot be devalued unlike fiat money (Freeman and Ruehsen).

Generally, money service businesses follow the same laws and regulations as banks, but they differ because they only require a valid form of identification instead of an existing account. Formal banking includes types of financial institutions, for example banks and credit unions, and are subject to the Bank Secrecy Act. Yet banks can still be used as a medium of illicit financing even if they are careful to follow procedures. False trade invoicing is one of the most popular laundering methods because of its difficulty to detect. Operatives either use under-invoicing or over-invoicing to transport money internationally.

In order to store and spend funds, it's important to recognize whether capital is for an organization, operation, or individual because, as stated above, organizations require significantly higher funds and each funding stream has different needs. Organizations can require millions of dollars whereas an operation only requires mid to high thousands. Individuals

generally only need a couple thousand dollars or less to complete their task, as seen with many recent vehicular attacks.

As previously stated, terrorist organizations incur numerous costs including maintaining itself, recruitment, living expenses of members as well as their families, and training. However, expenses relating to operations are different as they entail costs of target selection, planning, deployment, the attack itself, the escape, and media exploitation. Target selection is important because it determines whether operatives will need to travel to the location and if surveillance is necessary. There is also the question of how frequently and by whom? Planning itself is one of the most important aspects of the attack because one overlooked detail can cause the whole plan to fail. Planning involves purchasing weapons, determining target layouts or whether additional surveillance is necessary, acquiring vehicles (if needed), etcetera. During deployment, it's essential to estimate the costs of travel, lodging, food and communications, as well as determine for how many people and how long. When calculating the attack itself, it is crucial to ascertain if the expenses were required for command and control or if communication devices were necessary. As for the escape, again, deciding whether travel and lodging is needed and, additionally, whether it supports elements of the attack. Lastly, media exploitation is a large part of why attacks are carried out – extremists incite public fear in an attempt to cause either social or political change. It is critical to identify whether there are media or internet expenses and who exploitation was driven by. For instance, whether a group claimed the actions of a terrorist, the attackers published a manifesto, etcetera.

U.S. Countermeasures and Policies

In the aftermath of 9/11, President Bush maintained that "Money is the lifeblood of terrorist operations. Today, we're asking the world to stop payment." The President, along with Colin Powell, the Secretary of State, and Paul O'Neill, the Secretary of the Treasury, explained the purpose and actions the order authorized. The first piece of action immediately froze twenty-seven different entities that held U.S. assets and prohibited transactions between the U.S. and those bodies. It also established a Foreign Terrorist Asset Tracking Center that recognized and investigated financial infrastructure as well as international terrorist networks. In addition, there will be more interagency cooperation for two reasons; following the money as a trail to terrorists and freezing it to disrupt operations. On top of internal interagency cooperation, President Bush asserts that information sharing on an international level will prevent terrorists from taking advantage of international financial system.

The following sources were obtained from recent federal counterterrorism policies and shifts in administration and agency strategy and serve as the building blocks for a firm foundation towards a new future. While analyzing United States countermeasures regarding illicit terrorist financing, agencies are reviewed as well as the role they play in disrupting terrorist funds, promoting counterterrorism processes, and interagency coordination. In order to understand terrorist financing, sources that analyze terrorist assets and explore primary funding streams are a necessary requirement. Lastly, sources are needed to break down the elements of a funding cycle and introduce both licit and illicit methods of financing.

In a comparison of both former President Obama's 2011 counter-terrorism strategy and current President Trump's 2018 counter-terrorism strategy, key differences as well as solutions are discussed. The predominant differences between the President's approaches are seen in the threat actors, the primary entities responsible for addressing the threat, and the core principles

that are key to countering the threat of terrorism. However, both Presidents recognize global threats as well as domestic. Although the Obama administration focuses narrowly on Al Qaeda and its affiliates whereas the Trump administration acknowledges all terrorist threats to the United States (Rollins).

Several departments within the federal government play a role in counterterrorism policies and developments. However, "Combating illicit finance is integrated into each agency's strategic goals to enhance national security and counter the threat of terrorism" (National Strategy for Combatting Terrorism, pg. 5). Despite all agencies having a vested interest in eliminating potential threats, departments such as the Department of Homeland Security and the U.S. Department of the Treasury have more responsibilities regarding countering terrorist finances than the Department of Defense and Department of State.

Department of Homeland Security

According to the "Strategic Framework for Countering Terrorism and Targeted Violence," the Department of Homeland Security (DHS) identified a connection between terrorist groups, illicit internet transactions and the sale of counterfeit goods. Consequentially, counterterrorism strategy now encompasses efforts to lower e-commerce risk, strengthen supply chain transparency, and modify key targets to detect and disrupt illicit pecuniary matters. Indirect measures to combat terrorist financing include the National Bulk Cash Smuggling Center, Cornerstone, Project STAMP, and SEARCH Initiative.

Department of the Treasury

The US Department of the Treasury consists of numerous offices and agencies, all of which interact with each other to a certain degree. One of which is the Office of Terrorism and Financial Intelligence (TFI), an organization whose primary mission is "countering illicit finance by utilizing Treasury's unique expertise, access to financial intelligence, and authorities, including financial sanctions and regulatory enforcement actions, to disrupt and disable terrorists, criminals, WMD proliferators, and other national security threats to the United States and to protect the U.S. and international financial systems from misuse" (National Strategy for Combatting Terrorism, pg. 5). The TFI consists of four subdivisions: Terrorist Financing and Financial Crimes (TFFC); Office of Foreign Assets Control (OFAC); Office of Intelligence and Analysis (OIA); Treasury Executive Office for Asset Forfeiture (TEOAF).

The Office of Terrorist Financing and Financial Crimes (TFFC) develops strategies designed to combat terrorist financing, money laundering, WMD proliferation, and other illicit crimes whether they be domestic or international. The Office of Foreign Assets Control (OFAC) works under the national emergency powers of the President and is responsible for enforcing economic and trade sanctions that align with the United States national security and foreign policy goals. The mission of the Office of Intelligence and Analysis (OIA) is to identify threats of financial networks and provide timely and accurate intelligence to ensure Treasury decisions are well informed. The Treasury Executive Office for Asset Forfeiture (TEOAF), also known as the administrator of the Treasury Forfeiture Fund, promotes programs that target the disruption of criminal enterprise activity by utilizing proceeds from asset forfeitures. Additionally, the TEOAF encourages the vitality and economic stability of the fund while identifying risks to the program (Terrorism and Financial Intelligence).

Department of State

The primary mission of the U.S. Department of State is to lead foreign policy, promote democracy abroad, and further American interests via diplomacy, advocacy, and assistance. Appointed by the President with the consent of the Senate, the Secretary of State is the President's chief foreign affairs advisor. The Secretary's principal responsibility is to implement the President's foreign policy objectives throughout the State Department and overseas. Each year, the State Department is responsible for submitting an annual report to Congress per Title 22 of the United States Code, Section 2656f. The report, also known as the Country Reports on Terrorism, is comprised of a complete account of terrorism worldwide, involving both countries and groups.

Within the department, but below the Under Secretary for Civilian Security, Democracy, and Human Rights is the Bureau of Counterterrorism and Countering Extremist Violence. Its mission is "to promote U.S. national security by taking a leading role in developing coordinated strategies and approaches to defeat terrorism abroad and securing the counterterrorism cooperation of international partners" (Bureau of Counterterrorism, 2019). The Bureau consists of nine separate programs and initiatives including the Antiterrorism Assistance Program; Countering the Financing of Terrorism Finance; Counterterrorism Partnerships Fund; Foreign Emergency Support Team; Global Counterterrorism Forum; Technical Support Working Group; Terrorist Screening and Interdiction Programs; Trans-Sahara Counterterrorism Partnership; Partnership for Regional East African Counterterrorism.

Federal Agencies, Policies and Executive Orders

Prior to 9/11, interagency coordination and cooperation were subpar. However, federal organizations have recognized and addressed limited information-sharing as a problem and implemented policies and processes throughout public and private sectors to ensure secure lines of communication. For instance, in 2017, under section 314 of the USA Patriot Act, the Financial Crimes Enforcement Network (FinCEN) established the FinCEN Exchange—a new approach that involves information-sharing between financial institutes and federal agencies. Specifically, the FinCEN Exchange "brings together law enforcement, FinCEN, and different types of financial institutions from across the country to sha1re information that can help identify vulnerabilities and disrupt money laundering, terrorist financing, proliferation financing, and other financial crimes" (National Security for Combatting, pg. 8).

While there are numerous programs regarding anti-terrorism, six specific policies, powers, and Executive Orders impact U.S. strategy, outlook, and sanctions. Firstly, the Antiterrorism Act of 1996 prohibits U.S. citizens from intentionally providing terrorist groups with material support or resources. The Bank Secrecy Act (BSA) of 1970 made it a requirement to "know the customers," as in clients had to have existing accounts, maintain records, and report suspicious transactions or transactions over ten-thousand U.S. dollars. However, Jim Harper, an associate from the Competitive Enterprise Institute, argues that the BSA undermines the privacy of law-abiding citizens and when it was ratified, "the U.S. Supreme Court laid the groundwork for what is now known as the "third party doctrine."" This allows a third party to share your information without a warrant even in spite of a contract declaring confidentiality.

The aforementioned Executive Orders include E.O. 13224, E.O 12947, and E.O. 13099. Executive Order 13224 was designed with the purpose of "Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten To Commit, or Support Terrorism." It

drastically widened the scope of existing U.S. sanctions against terrorist organizations. President Clinton signed E.O. 12947 into effect in 1995 which "Prohibit[ed] Transactions With Terrorists Who Threaten To Disrupt the Middle East Peace Process". Clinton later amended E.O. 12947 and added three individuals and an organization to the Annex which turned it into E.O. 13099. The last power is OFAC's blacklist labelled the "Specially Designated Nationals and Blocked Persons List" (2018 Terrorist Asset Report).

Terrorist Assets and State Sponsors

Since 1993, the US Department of Treasury has compiled a list of terrorist assets annually. The report consists of two subgroups labelled "Assets Relating to International Terrorist Organizations" and "Assets Relating to State Sponsors of Terrorism." As previously stated, the OFAC enforces economic and trade sanctions, but it also is the primary "U.S. Government agency responsible for implementing sanctions against the assets of international terrorist organizations and terrorism-supporting countries" (2018 Terrorist Asset Report). According to the 2018 report targeting international terrorist organizations, roughly forty-six million dollars were blocked by OFAC by the implementation of sanctions programs. Furthermore, the report targeting state sponsorship identified three states (Iran, Sudan, and Syria) with terrorist funding links and blocked approximately 216.83 million dollars in assets using economic sanctions.

According to the Bureau of Counterterrorism and Countering Violent Extremism, there are currently only four countries sponsoring terrorist organizations: Iran; Sudan; Syria; and Democratic People's Republic of Korea. The definition of state sponsorship requires that "the Secretary of State must determine that the government of such country has repeatedly provided support for acts of international terrorism" (Country Reports, 2017). A country labelled as a state sponsor obtains several negative consequences including: A ban on arms-related exports and

sales; Controls over exports of dual-use items, requiring thirty-day Congressional notification for goods or services that could significantly enhance the terrorist-list country's military capability or ability to support terrorism; Prohibitions on economic assistance; and Imposition of miscellaneous financial and other restrictions. Only when a designated country is in accordance with the statutory criteria, will the designation be rescinded.

As of 2017, Iran has remained thus far the world's principal state sponsor of terrorism and is responsible for undermining foreign government interests and supporting attacks against Israel among other activities. The Iranian Government has been branded as a state sponsor of terrorism since 1984 and remained so to the present. Their primary group ally is Hezbollah, located in Lebanon. Iran also supports the Assad regime in Syria, Al-Qaida and several other organizations throughout the Middle East including militias, Hamas, and Palestinian groups. The recruited militias, comprised of Shia combatants, are sent by Iran to aid the Assad regime in Syria, however many groups have committed human rights abuses against Sunni citizens. The Iranian Government also refuses to identify or prosecute senior Al-Qaida members that find refuge in Iran and, since, 2009, allows Al-Qaida to move funds as well as fighters to both Syria and South Asia via core facilitation pipeline. Support consists of providing funds, weapons, training, and even sponsoring cyberattacks against foreign governments as well as private entities. Iran utilizes the Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF) as a way to provide financial support to terrorist organizations, cover for covert operations, and create instability in the Middle East. However, in order to avoid more aggressive policies, Iran uses regional proxy forces as a method to deny and conceal sponsorship (Country Reports, 2017).

The Sudan government, despite being a designated state sponsor of terrorism since 1993, is taking steps to follow U.S. direction. Previously, they supported multiple foreign terrorist

organizations, such as the Palestine Islamic Jihad, Hamas, the Abu Nidal Organization, and Lebanese Hezbollah. As of 2017, Sudan completed the Five Track Engagement Plan which advised them to improve its interagency as well as international cooperation. As a result of this success, the United States lifted certain economic sanctions. Although there are challenges regarding border security, such as its expansive size, outdated technology, and limited visa restrictions. Sudanese forces must patrol the Sudanese-Libyan border to prevent entry to terrorists, weapons, and other illicit activities. Additionally, while Sudan does coordinate with the U.S. on counterterrorism strategies, they also possess a "de-radicalization" program that focuses "on reintegration and rehabilitation of returned foreign terrorist fighters and those espousing terrorist ideologies" (Country Reports, 2017).

Since Syria was first labelled as a state sponsor in 1979, it has maintained a strong relationship with Iran who, in turn, considers them to be a crucial ally. The mutual support between the Iranian Government and the Assad regime has remained firm, especially in defense of each other's policies. Like Iran, Syria backs Lebanon Hezbollah as well as other groups via political, military, and financial means. For instance, Syria has purchased oil from ISIS, released statements supporting Hezbollah as well as arming them. Additionally, as previously stated, militias in line with Iran travel to Syria to fight on behalf of the Assad regime. In 2017, the Syrian government was claiming to be the victims of the internal opposition as part of their strategy. Although, despite being part of the Chemical Weapons Convention, Syria, according to U.S. knowledge, has repeatedly employed chemical weapons against Syrian citizens nearly every year since in spite of former President Obama's threats (Country Reports, 2017).

The Democratic People's Republic of Korea (DPRK) was first designated as a state sponsor of terrorism in 1988 after its involvement in a Korean Airlines passenger flight bombing

in 1987. The designation was retracted in 2008 when the DPRK was evaluated and found to meet all statutory criteria for rescission. However, in 2017 it was determined that the DPRK had never stopped their support for international terrorism. They continued to back terrorist organizations, violate UN Security Council resolutions, resume nuclear and ballistic missile testing, been incriminated for foreign assassinations, and shelter four Japanese Red Army members involved in the Japan Airlines hijacking in 1970. In addition, Japan believes the DPRK abducted twelve nationals in the 1970s and 1980s, which only five have been repatriated (Country Reports).

Solutions

While the U.S. has not lost the war against terrorist financing, it has certainly lost a few battles. According to Michael Jacobson, author of "Terrorist Financing and the Internet," "Today, the terrorist threat is far more decentralized, and Al Qaeda's central command is not funding operations as it once did." As a result, growing terrorist cells raise funds via criminal activity which is not a new issue. The problem now is that the continuous evolution of the financing via the internet. Terrorists are constantly finding new online methods to both raise and launder money, along with the fact that it is nearly impossible to combat lone wolf attacks if one just examines financial spending. Most of the time, lone wolves can be found by analyzing their internet usage and many find their niche with other like-minded people so it wouldn't necessarily be a far jump from acting on their beliefs. Plus, there is the added consequence that inflicting damage doesn't have to be expensive.

Terrorism – by definition – cannot be defeated, however, it can be prevented. In order to further disrupt terrorist financing, the U.S. must implement both short-term and long-term solutions. Short-term solutions include those previously mentioned: the development of financial typologies; continuous research regarding the evolution of finances; flexible strategies; and

improved collaboration between both the international and domestic agencies. The first solution compares the financing of a specific attack with other similar attacks to identify the commonalities between both (Lormel, Dennis M.). Eventually, after gathering enough data, this form of investigation could lead to the development of financial typologies. According to Dennis M. Lormel, "terrorist financing monitoring and identification are inherently reactive processes." However, with the implementation of financial typologies, there is the potential for federal agencies to shift from a relatively reactive response to terrorist attacks to a more proactive approach. In order to identify commonalities, it is important to distinguish between the types of attack, which is to ascertain whether the attack was inspired, enabled, or directed. After that is determined, "financial institutions should be able to identify funding flows and fragments of financial intelligence in the use of financial mechanisms and spending patterns needed to facilitate such activity" (Lormel, Dennis M.). From there, the typologies can be further broken down to discern whether plans had similar venues, weapons, etcetera.

The next solution involves continuous research to identify new methods of financing as they are being developed, although it may also assist in the growth of financial typologies. This is necessary as funding practices are constantly evolving, especially those involving online activities. The internet has played a large role in expanding illicit crimes from the physical world to cyber as well as globalization's impact on worldwide communications. Federal agencies continue to revise strategies, combat threats, and open lines of communication between the public and private sectors to counteract terrorism. However, this isn't enough. To successfully combat terrorist financing, it is crucial to understand previous methods as well as current ones in order to keep pace with evolving techniques. Through continuous research, it is possible to

conduct effective investigations that are, at the same time, urgently reactive (Lormel, Dennis M.).

In order for the previous solution to make a legitimate difference, it must be applied to current policies, which is where flexible strategies come into play. In Congress, the Senate is meant to slow the policymaking process down whereas the House of Representatives is steered by public opinion which is continuously changing. This means, by the time a new method of financing is recognized and a law to counter it is passed and implemented, terrorists have already discovered a new funding technique. Therefore, instead of constantly passing new laws to keep up with terrorists, more flexible policies must be developed so agencies can keep pace with new research finds. That being said, the President may contribute by signing executive orders into place that counteract new methods.

The fight against terrorist financing is extremely complex and requires not only international collaboration on a long-term scale, but also cooperation between agencies and the private sector. Plus, bodies must have the capacity to act quickly without fear of backlash from allies. From there, the money can either be frozen or followed back to the terrorist organizations. Now considering the fact that each state and agency has its own interests and priorities, it is very unlikely that complete cooperation is attainable. Different countries cannot agree on a single definition of terrorism, let alone different U.S. agencies. On an international level, such a commitment would only be possible if "top- and mid-level decision makers have re-conceptualized national security threats to include transnational financing of terrorists and if they have redefined the paradigm of security threats from one centered on nation-states to one incorporating transnational nonstate actors" (Clunan, pg. 571). Just looking at the United States, this initiative would mean change in every department to accommodate this goal which wouldn't

necessarily be for the best. Conflict is necessary and offers substantial benefits. Conflict arises because every agency has its own purpose, priorities, and culture. However, it can contribute to a better conclusion since each agency has a differing expertise, information bases, values, and constituencies (Kamensky, 2019). Although admittedly, information-sharing has improved over time with better technology and procedures in place, but the rivalry remains.

According to Anne Clunan, a professor in National Security Affairs, in order to disrupt the flow of terrorist finances successfully, an anti-money laundering institutional capacity must be built. The first and most difficult step in building institutional capacity is regulating the formal and informal financial services industry and trade services via an anti-money laundering legal framework. The problem is that the framework must be enforceable as well as collect current intelligence and data on financial flows. It must also have a diverse workforce, fulfilling various occupations with personnel trained in criminal investigations and intelligence collection (Clunan, pg. 571). And yet, even if all this is achieved, another dilemma remains; the costs of completing this project while still taking into account unforeseen expenses from either add-on initiatives or adjusting the original design.

Conclusion

While the United States has accomplished much through political, military, and anti-counterterrorism financing means, there is still the question of whether continuing with this strategy is the correct course of action. Different methods of discovering terrorist financing must be pursued because at this rate, simply freezing assets is not making a significant enough change. It is more expensive to identify and seize assets, police the domestic and international community, and implement policies throughout federal agencies as well as abroad, than it is for terrorists to develop new methods of financing in response, which starts the process all over

again. The key is to be proactive or, at least, ‘urgently reactive’ in order to contain a situation. Following the suggested short-term solutions, more long-term solutions need to be explored, for instance; deradicalization. The end goal of combatting terrorist financing was always to prevent terrorism by Islamic extremists. Deradicalization programs would serve to put an end to financial support from sympathizers as well as reduce recruitment numbers, at least within the United States.

Work Cited

"Appendix A: The Financing of the 9/11 Plot." *U.S. Government Publishing Office*, Govinfo, govinfo.library.unt.edu/911/staff_statements/911_TerrFin_App.pdf.

2018 National Terrorist Financing Risk Assessment. U.S. Department of the Treasury, 2018, home.treasury.gov/system/files/136/2018ntfra_12182018.pdf.

"Anti-Money Laundering/Combating the Financing of Terrorism." *International Monetary Fund*, www.imf.org/external/np/leg/amlcft/eng/aml1.htm#financingterrorism.

Clunan, Anne. "The Fight against Terrorist Financing." Calhoun: The NPS Institutional Archive, 2006, core.ac.uk/download/pdf/36731187.pdf.

"Combatting Terrorist Financing." *ACAMS*, www.acams.org/aml-resources/combatting-terrorist-financing/.

"Country Reports on Terrorism 2017 - United States Department of State." U.S. Department of State, U.S. Department of State, 2017, www.state.gov/reports/country-reports-on-terrorism-2017/.

del Cid Gómez, Juan Miquel. "A Financial Profile of the Terrorism of Al-Qaeda and Its Affiliates." Perspectives on Terrorism, Oct. 2010, file:///C:/Users/macda/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/113-753-1-PB%20(1).pdf.

de Goede, Marieke. "Hawala Discourses and the War on Terrorist Finance." Citeseerx, 2003, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.138.333&rep=rep1&type=pdf

"Disrupt Terrorist Financing." *Department of Homeland Security*, 6 Aug. 2018, www.dhs.gov/topic/disrupt-terrorist-financing.

DOD Dictionary of Military and Associated Terms. Department of Defense, Oct. 2019, www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.

"Executive Order 12947." *Prohibiting Transactions With Terrorists Who Threaten To Disrupt the Middle East Peace Process*, U.S. Department of the Treasury, 23 Jan. 1995, www.treasury.gov/resource-center/sanctions/Documents/12947.pdf.

"Executive Order Freezing Terrorists' Assets." The Washington Post, WP Company, 24 Sept. 2001, www.washingtonpost.com/wp-srv/nation/specials/attacked/transcripts/bush092401.html.

Freeman, Michael, and Moyara Ruehsen. "Terrorism Financing Methods: An Overview." *Perspectives on Terrorism*, 2013, www.terrorismanalysts.com/pt/index.php/pot/article/view/279/html.

Gerring, John. Case Study Research: Principles and Practices. 2nd ed., Cambridge University Press, 2018.

Harper, Jim. "Don't Follow the Money." Competitive Enterprise Institute, Ceidotorg, 6 July 2017, cei.org/blog/dont-follow-money.

Jacobson, Michael. "Terrorist Financing and the Internet." Taylor & Francis, Mar. 2010, www.tandfonline.com/doi/full/10.1080/10576101003587184.

Johnston, Patrick B, and David Manheim. “Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats.” *Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats*, by Cynthia Dion-Schwarz, RAND Corporation, 2019, pp. 7–35.

Kamensky, John. “When Interagency Conflict Is a Good Thing.” Government Executive, Government Executive, 12 June 2019, www.govexec.com/management/2018/08/when-interagency-conflict-good-thing/150713/.

Kohlmann, Evan F. The Role of Islamic Charities in International Terrorist Recruitment and Financing. Danish Institute for International studies, 2007, www.econstor.eu/bitstream/10419/84554/1/DIIS2006-07.pdf.

Lormel, Dennis M., and Syed Ali Raza. “Terrorist Financing: Visualizing Funding Flows.” *ACAMS Today*, 18 Sept. 2018, www.acamstoday.org/terrorist-financing-visualizing-funding-flows/.

Lormel, Dennis M. “Assessing Terrorist Financing Through the Lens of the Terrorist Attack Cycle.” ACAMS Today, 20 Mar. 2018, www.acamstoday.org/assessing-terrorist-financing-through-lens-of-terrorist-attack-cycle/?_ga=2.63379823.1192261340.1574110001-768332609.1574110001.

Maruyama , Ellie, and Kelsey Hallahan. “Following the Money.” *Center for a New American Security*, 9 June 2017, www.cnas.org/publications/reports/following-the-money-1.

National Proliferation Financing Risk Assessment. U.S. Department of the Treasury, 2018, home.treasury.gov/system/files/136/2018npfra_12_18.pdf.

National Strategy for Combating Terrorism and Other Illicit Financing. U.S. Department of the Treasury, 2018, home.treasury.gov/system/files/136/nationalstrategyforcombatingterroristandotherillicitfinancing.pdf.

Neumann, Peter R. "Don't Follow the Money." Foreign Affairs, Foreign Affairs Magazine, 8 Dec. 2018, www.foreignaffairs.com/articles/2017-06-13/dont-follow-money.

"PayPal." PayPal, 2019, www.paypal.com/us/webapps/mpp/ua/aml-full.

"President Bush Addresses the Nation." The Washington Post, WP Company, 20 Sept. 2001, www.washingtonpost.com/wp-srv/nation/specials/attacked/transcripts/bushaddress_092001.html.

"Programs and Initiatives - United States Department of State." *U.S. Department of State*, U.S. Department of State, 2019, www.state.gov/bureau-of-counterterrorism-and-countering-violent-extremism-programs-and-initiatives/.

Ritchie, Hannah, et al. "Terrorism." Our World in Data, 2019, ourworldindata.org/terrorism#how-many-people-are-killed-by-terrorists-worldwide.

Rollins, John W. "The Trump Administration's National Strategy for Counterterrorism: Overview and Comparison to the Prior Administration." *Congressional Research Service Reports*, CSR, 29 Jan. 2019, fas.org/sgp/crs/terror/IN11027.pdf.

Shelley, Louise, and Nancy Hirst. "Exploring the Financial Nexus of Terrorism, Drug Trafficking, and Organized Crime." *Financial Services,* The Terrorism and Illicit Finance Subcommittee, House Financial Services Committee, 20 Mar. 2018, financialservices.house.gov/uploadedfiles/03.20.2018_louise_shelley_testimony.pdf.

Skinner, Chris. "The US Dollar Is No Longer American." *BankNXT*, 4 Aug. 2017, banknxt.com/61372/us-dollar/.

"State Sponsors of Terrorism - United States Department of State." U.S. Department of State, U.S. Department of State, www.state.gov/state-sponsors-of-terrorism/.

Strategic Framework for Countering Terrorism and Targeted Violence. Department of the Homeland Security, 2019, www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf.

"Terrorism." *Department of Homeland Security,* 24 Oct. 2019, www.dhs.gov/cisa/terrorism.

"Terrorist Attacks by Vehicle Fast Facts." *CNN*, Cable News Network, 4 Sept. 2019, www.cnn.com/2017/05/03/world/terrorist-attacks-by-vehicle-fast-facts/index.html.

"Terrorism and Financial Intelligence." *U.S. Department of the Treasury*, 17 July 2019, www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Terrorism-and-Financial-Intelligence.aspx.

"Terrorist Financing." Documents - Financial Action Task Force (FATF), www.fatf-gafi.org/publications/fatfgeneral/documents/terroristfinancing.html.

Various Definitions of Terrorism. dema.az.gov/sites/default/files/Publications/AR-Terrorism%20Definitions-BORUNDA.pdf.

Worth, Katie. “Lone Wolf Attacks Are Becoming More Common -- And More Deadly.” PBS, Public Broadcasting Service, 2016, www.pbs.org/wgbh/frontline/article/lone-wolf-attacks-are-becoming-more-common-and-more-deadly/.

Yuen, Stacey. “It's Not Just Russia - Terror Financiers Are Also Using Social Media Propaganda.” CNBC, CNBC, 1 Jan. 2018, www.cnbc.com/2017/12/18/social-media-propaganda-terror-financiers-operate-on-internet.html.

Zemen, Tomas, et al. “Role of Internet in Lone Wolf Terrorism.” Research Gate, Dec. 2017, www.researchgate.net/publication/322130271_Role_of_internet_in_Lone_Wolf_Terrorism.