REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
01-05-2018	Master's Thesis	July 17-May 18

4. TITLE AND SUBTITLE
Cryptocurrencies: Emergent Threat to National Security

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
George, Derek R., Major, USMC

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
United States Marine Corps
Marine Corps University, School of Advanced Warfighting
3070 Moreel Avenue
Quantico, VA 22134

8. PERFORMING ORGANIZATION REPORT NUMBER
None

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Same as #7.

10. SPONSOR/MONITOR'S ACRONYM(S)
None

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
None

12. DISTRIBUTION/AVAILABILITY STATEMENT
No Restrictions

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The current strategic security environment is more complex than ever before. Adversaries such as North Korea, Iran, and Syria strive to destabilize regions while competitors—China and Russia—attempt to erode national security by challenging America's global power, influence, and interest. In addition, domestic and transnational threats such as terrorist groups, transnational criminal organizations, and non-state actors have increased destabilization activities, thereby threatening U.S. national security at home and abroad. Though not fully understood, cryptocurrencies and alternative remittance money laundering will continue to grow on a global scale and remain threat finance sources for the foreseeable future. The United States and Partner Nations must and will develop the capability to detect, disrupt, and dismantle cryptocurrencies and alternative remittance threat finance networks by increasing knowledge and information sharing, collaborating and cooperating internationally, and leveraging international and domestic financial enforcement authorities.

15. SUBJECT TERMS
Counter Threat Finance, Cryptocurrency, Alternative Remittance Systems, Bitcoins

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			MCU School of Advanced Warfighting
Unclassified	Unclassified	Unclassified	UU	24	19b. TELEPHONE NUMBER *(Include area code)* (703) 432-5318 (Admin Office)

United States Marine Corps
School of advanced Warfighting
Marine Corps University
3070 Moreell Avenue
Marine Corps Combat Development Command
Quantico, Virginia 22134

FUTURE WAR PAPER

Title
Cryptocurrency: Emergent Threat to National Security

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

Author
MAJOR DEREK R. GEORGE

AY 2017-18

Mentor: Dr. Bradley Meyer
Approved: Bradley J. Meyer
Date: 17 May 2018

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE SCHOOL OF ADVANCED WARFIGHTING OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

Table of Contents

Page

Figures

Page

Introduction

The current strategic security environment is more complex than ever before. Adversaries such as North Korea, Iran, and Syria strive to destabilize regions while competitors—China and Russia—attempt to erode national security by challenging America's global power, influence, and interest.[1] In addition, domestic and transnational threats such as terrorist groups, transnational criminal organizations, and non-state actors have increased destabilization activities, thereby threatening U.S. national security at home and abroad. Since September 11, 2001, the U.S. has conducted a series of financial pressure campaigns that go beyond classic sanctions and trade embargoes to isolate Al Qaeda, Islamic State of Iraq and Syria (ISIS), Iran, Syria, and North Korea.[2] The U.S. leveraged the international financial and commercial systems to constrict the flow of funds, making it more difficult for adversaries to move money and finance their activities.[3] The recently published 2017 *National Security Strategy of the United States of America* continues the strategic vision of a whole-of-government approach in collaboration with Partner Nations to target and dismantle financial support networks at the source to isolate adversaries and combat transnational threats.[4]

Understanding the Problem

Consequently, domestic and transnational threats continue to evolve their methods of obtaining funds and rapidly adapt to financial pressures. The convergence of transnational threats with each other and state actors is a growing phenomenon. Terrorists and insurgents frequently engage in criminal activities to raise funding. State actors also provide financial support to transnational threats, undermining the U.S. and Partner Nations' successes in countering threat finance. Failing and weak states are plagued by corruption, which enables transnational criminals to undermine the rule of law and spread fear deep within societies.

Furthermore, these threat networks rely increasingly on encrypted communication and the dark web to evade detection and finance their operations.[5]

Though not fully understood, cryptocurrencies and alternative remittance money laundering will continue to grow on a global scale and remain threat finance sources for the foreseeable future. Criminals and terrorist are mobile and increasingly migratory, "shifting both their locations and their vocations in order to exploit geographic, political, enforcement, and regulatory vulnerabilities."[6] The absence of common international regulatory standards and inadequate global capabilities to counter these threat finance sources are root causes of this wicked problem. U.S. national security, interest abroad, and economic stability are at risk; therefore, it is imperative for the international community to understand the implications of a global market driven by both mainstream globalization and encrypted technical infrastructure. ***The United States and Partner Nations must and will develop the capability to detect, disrupt, and dismantle cryptocurrencies and alternative remittance threat finance networks by increasing knowledge and information sharing, collaborating and cooperating internationally, and leveraging international and domestic financial enforcement authorities.***

Elements of Threat Finance

The first step in defeating a threat finance network is understanding the elements of the threat finance and conceptualizing the network as a system. Joint Publication (JP) 3-25, *Countering Threat Networks*, defines threat finance as "the manner in which adversarial groups raise, move, store, and use funds to support their activities."[7] Threat finance activities can be categorized into operational and support activities. Operational activities include execution of illicit acts such as terror attacks and drug trafficking, while support activities include security, recruitment, transportation, and safe havens.[8] Illicit activities can have global reach and are

generally not geographically constrained. In 2012, Nils Gilman, Jesse Goldhammer, and Steven Weber introduced the concept of "deviant globalization, [which] describes crossborder economic networks that produce, move, and consume" a variety of illicit goods and services such as narcotics, human beings, counterfeit goods, and other criminal activities.[9] Money from these activities is often laundered with licit funds from legitimate businesses, charitable donations, or state governments. The funds are moved in two stages: placement and layering. During placement, the acquired funds are placed into a local, national, or international financial system.[10] During layering, the funds are moved through several accounts or repeatedly converted into different forms to create distance between the origination of the funds and their eventual destination.[11] Once successfully moved, laundered money can be stored as bulk-cash, deposited in banks, or invested in stocks or real estate until needed. Now ready for third and final stage of integration, the funds are made available to the threat network for their use or re-investment into other licit and illicit operations.[12] The more complex and encrypted the laundering scheme, the more difficult it is to counter.

Alternative Remittance Systems

Alternative remittance systems often referred to as "underground banking" represent a finance source that can directly and indirectly threaten national security. Checks and wire transfers are traditional means of remitting money that are transparent to banking institutions and

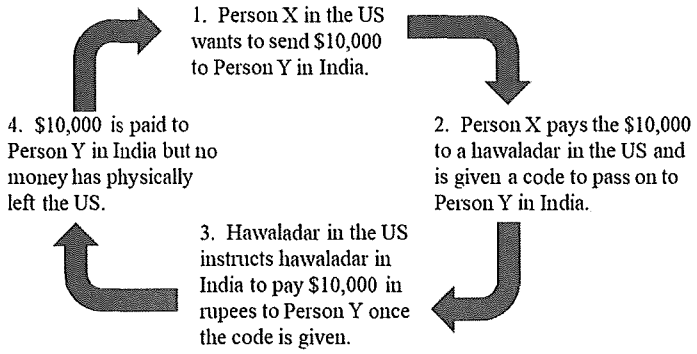

Figure 1: Hawala Process

financial enforcement agencies. *Hawala*, for example, is an alternative remittance system that "exist[s] and operate[s] outside of, or parallel to traditional banking or financial channels."[13] *Hawala* originated in India and remains a major remittance system used worldwide. China also has alternative remittance systems known as "chop," "chit," or "flying money."[14] Alternative remittance transactions are significantly dependent upon trustworthy connections such as family, common cultures and ethnicities, or regional ties because money or an equivalent value is exchanged through a third party. In the *hawala* system, *hawaladars* serve as the conduit for money transfers and often operate legitimate business which effectively advertise alternative remittance services. Figure 1 illustrates how transactions are completed.[15]

Implications of Alternative Remittance Systems as a Threat Finance Source

The informal mechanisms that allow money transfers to be completed without actually moving money make alternative remittance systems ideal sources for threat finance. Money laundering via alternative remittance systems is done effectively using the three phases previously discussed: placement, layering, and integrations. During placement, legitimate businesses that also offer remittance services periodically deposit small amounts of money into banks in order to avoid suspicion. During the layering stage, fraudulent records are kept on hand, and invoices are manipulated to mask the true amount and origin of the illegal money exchanged for legal goods. Once the money is successfully layered, integration is virtually seamless. The money now appears legitimate and is available for reinvestment in support of threat activities.

Anti-money laundering laws make it harder for transnational threats to move money through the international banking system; therefore, alternative remittance systems are increasingly used to fund threat activities. According to Al-Jarani, "before 2007, 30% of

terrorist finance moved through banks…22% transported physically through cash smuggling…[and] 5% via money service businesses which include hawala."[16] Since 2007, the terrorist finance flowing through banks dropped to just 8%, while physical transport and use of money service businesses increased to 37% and 30%, respectively.[17] This shift can be attributed to the simplicity of completing transaction using alternate remittance systems. The infinite number of ways to complete these transactions significantly contributes to the difficulties recognizing money laundering in order to counter this threat finance source.

Afghanistan, for example, has a robust *hawala* system. Approximately 90 percent of the remittance brokers in Kandahar and Helmand provinces facilitated drug transactions.[18] Dubai serves as a cashpoint for Afghans as the markets are unregulated and provides anonymous transit lounges and black-market proliferation networks to purchase U.S. military equipment and clean illicit funds.[19] The attacks of September 11, 2001 was funded by both licit and illicit funds, illustrating the difficulties U.S. officials had in recognizing the threat finance activities of Osama bin Laden and the al Qaeda network. The terrorist group successfully circumvented government and private sector oversight of traditional banking in order to carry out the attacks. Furthermore, al Qaeda likely relied on the *hawala* transactions to fund the Mumbai attacks of November 2008.

Countering Alternative Remittance Systems

Joint Publication (JP) 3-25 outlines a framework for countering threat finance such as alternative remittance systems. According to JP 3-25, a whole of government approach where the U.S. Departments of Defense (DoD), Treasury, State, and Justice, and other U.S. governmental agencies in collaboration with Partner Nations is the most effective way to counter threat financial networks. The DoD is often not the lead agency; therefore, planners must understand the operating environment, core competencies of various agencies, and means and

circumstances related to national security and operational objectives.[20] As a part of the Joint Intelligence Preparation of the Operating Environment (JIPOE) process, the threat financial system analysis focuses on tracking the generation, storage, movement, and use of funds. Valuable insight may also be gained into the threat network's leadership, business practices, and the identification of critical requirements and critical vulnerabilities. As threat networks rapidly adapt, the challenge is identifying decisive points to target in order to deter, disrupt, and dismantle threat finance networks.

Money laundering through alternative remittance systems is relatively easy accomplish, although difficult to detect; therefore, a meticulous and collaborative approach is required to investigate indications and warnings of illicit activities. U.S. banks consistently monitor accounts and provide financial enforcement agencies with information about suspicious deposits that exceed the threshold $10,000. Significant deposits from one or more ethnic communities (e.g. Afghan, Bangladeshi, Indian, Pakistani, and Somali) normally indicates a *hawala*, especially if the transaction is associated with a known hawaladar.[21] Wire transfers to a major financial center known for *hawala* such as Great Britain, Switzerland, and Dubai are also clear indicators.[22]

Afghan Threat Finance Cell

In 2009, for example, U.S. interagency and international efforts successfully disrupted and exploited the threat finance network in Afghanistan. The multiagency Afghan Threat Finance Cell (ATFC) was formed, consisting of specialists from the Departments of Defense (DoD), Justice, and Treasury, Central Intelligence Agency (CIA), Federal Bureau of Investigations (FBI), and the Drug Enforcement Administration (DEA). The ATFC gathered and analyzed intelligence specific to Taliban operational and narcotic finances in order to determine

the best ways to disrupt the network.[23] The ATFC collected tens of thousands of financial documents, uncovered and raided *hawala* networks, and exposed the New Ansari Money Exchange as a narcotics-trafficking, money-laundering organization.[24] Furthermore, the ATFC traced money movements from Afghanistan to Dubai, leading to targeted sanctions by U.S. Treasury Department.[25]

Financial Action Task Force

Another important counter threat finance ally that the U.S. should collaborate with is the Financial Action Task Force (FATF). FATF is "an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering and terrorist financing."[26] The FATF was formed following the 1989 G7 Summit in Paris to coordinate global efforts against drug trafficking related money laundering. While not a formal authority under international law, the FATF's *40 Recommendations* for international anti-money laundering standards are accepted internationally. By 2004, the FATF's *Nine Special Recommendations on Terrorist Financing* (known as the *FATF 40+9 Recommendations*) added emphasis on alternative remittance, government corruption, and enhanced coordination with the private sector. FATF continues efforts to "harmonize standards on transparency, beneficial ownership, reporting of suspicious transactions and international cooperation."[27] Due to the emergence of virtual currencies as means to trade value for goods and service, the FATF published *Guidance for a Risk-Based Approach to Virtual Currencies* in 2015.[28] According to the 2015 report, transnational criminals and terrorist organizations increasingly use encrypted virtual currencies and the dark web to fund their illicit activities.

Cryptocurrency

In 1998, a programmer under the alias Satoshi Nakamoto used cryptography and a digital encoding method called "mining" to solve complex mathematical problems to create the first and probably most well-known cryptocurrency—Bitcoin.[29] According to Raiborn and Sivitanides, "a bitcoin is a digital medium of exchange that is created, acquired, held, and traded electronically."[30] Cryptography masks and encrypts digital currencies making them as secure as possible as, hence the term cryptocurrency. Bitcoin has already changed the global financial landscape. Currently, more than 900 different cryptocurrencies exist (e.g., Ethereum, NEO, Ripple, and Dash) for mining. Miners are key members of cryptocurrency communities or exchange and use "specialized computers and custom-designed chips called Application-Specific Integrated Circuits (ASICs) which are optimized to conduct the mathematical calculations needed for mining."[31] Miners also serve as cryptocurrency exchangers and accept conventional currencies in exchange for cryptocurrencies. Once acquired, the cryptocurrencies are stored in a digital wallet associated with the user's virtual address, "designated by a complex string of letters and numbers [similar] to a bank account number."[32]

Digital wallets are used to complete anonymous peer-to-peer transactions using cryptographic algorithms and a set of public and private keys. There are two types of wallets: "hot" wallet and "cold" wallet. A "hot" wallet is heavily encrypted digital wallet directly connected to the Internet, while a "cold" wallet is a nonconnected item (such as a flash drive or a piece of paper) that contains the cryptocurrency information.[33] The public key is the computer address needed by both parties to engage in transactions; the private key is each individual's digital wallet password needed to send cryptocurrency to another public key.[34] Once complete,

cryptocurrency transaction between wallets are recorded in a distributed ledger technology called the blockchain.

The blockchain is the underlying technology and core to how cryptocurrencies work. Multiple computers are used by Miners within the decentralized cryptocurrency network to validate blocks of transactions. The faster Miners solve specific cryptographic problems, the more coins they earn. Completed transactions are then added to the exchange "registry in a linear, chronological order and cannot be modified or replaced."[35] In addition, each computer used to validate transactions automatically receives a copy of all cryptocurrency transactions, thus making the transactions traded transparent to those within the networks.[36] Of the two threat finance sources discussed for the purpose of this paper, cryptocurrency has emerged as one of the most profitable yet problematic forms of threat finance to counter.

Implications of Cryptocurrency as a Threat Finance Source

Anonymity, global reach, speed of transactions, and non-repudiation make cryptocurrency networks attractive to transnational threat financing, money laundering, and other illicit activities. The anonymity of cryptocurrencies makes them ideal finance sources for inexpensive lone wolf attacks. According to the May 2017 Center for a New American Security report, "In the past several years, terrorist groups in Gaza have solicited support in Bitcoin; there are isolated reports that ISIS has used the cryptocurrency; and cybercriminals use it and other virtual currencies in a range of circumstances."[37] The global reach and speed of transactions allow virtual currency to be converted to cash quickly and easily from any location around the world. Transnational criminal organizations effectively build cryptocurrency networks to buy and sell illicit goods and services ranging from weapons to hitmen for hire. Because cryptocurrency transfers are currently irreversible, cybercriminals are successfully hacking

cryptocurrency exchanges and e-wallets to steal virtual currencies and identities. Furthermore, cryptocurrencies allow countries like Iran, North Korea and Russia to evade international sanctions, thereby weakening U.S. diplomatic efforts and escalating global conflict.

Countering Cryptocurrency as a Threat Finance Source

While "following the money" that flowed through banking institutions proved successful in the past, the rapidly evolving and adaptive nature of cryptocurrency networks requires more collaborative, innovative, and deliberate approaches to disrupt threat finance networks in the virtual domain. The U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) and the U.S. Federal Bureau of Investigation (FBI) have effectively used their tools and authorities to disrupt robust cryptocurrency threat finance networks. Let's look first at the FinCEN case.

FinCEN is responsible for enforcing compliance with the Bank Secrecy Act, which governs anti-money laundering (AML) and counterterrorism financing in the United States. FinCEN issued regulatory guidance and registration requirements for money services businesses who facilitate cryptocurrency transactions.[38] FinCEN defines virtual currency as "a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency."[39] In May 2013, Liberty Reserve, a Costa Rica-based currency transfer and payment processing company, was charged with laundering billions of dollars through 55 million customer transactions around the world using digital currency.[40] According to the indictment: "The defendants deliberately attracted and maintained a customer base of criminals by making financial activity on Liberty Reserve anonymous and untraceable."[41]

Initially, Liberty Reserve required network users to provide personal identifiable information, which later morphed into only the requirement of a working email. Liberty Reserve

employed Miners to serve as third party exchangers to "further obscure the money trail, thus enabling Liberty Reserve to avoid collecting any information about its users through banking transactions or other activity that would leave a centralized financial paper trail."[42] Liberty Reserve became an attractive source for threat finance activities. FinCEN was able to shut down Liberty Reserve by classifying them as an unlicensed money transmitting business which violates international AML laws. FinCEN's success highlights the importance of establishing international standards for classifying and regulating cryptocurrencies. Furthermore, FinCEN used traditional investigative techniques and applied existing laws to shut down Liberty Reserve.

In 2013, the FBI also shut down a cryptocurrency threat network called Silk Road, by methodically infiltrating the network and dismantling it from the inside. Ross Ulbricht, founder of Silk Road, was a savvy Bitcoin entrepreneur with libertarian views. He worked diligently to make Bitcoin a competitive alternative to the U.S. dollar and operated Silk Road for approximately two and a half years. Silk Road "was used by several thousand drug dealers and other unlawful vendors to distribute hundreds of kilograms of illegal drugs and other unlawful goods and services to well over a hundred thousand buyers, [laundering hundreds] of millions of dollars derived from these unlawful transactions."[43] According to the indictment: "Silk Road is alleged to have generated the Bitcoin equivalent of approximately $1.2 billion in sales and approximately $80 million in commissions."[44]

The website operated on a Tor network, which is a special network of computers designed to mask Internet Protocol addresses.[45] The problem that Ulbricht did not recognize was that the Office of Naval Intelligence created the Tor technology. By late 2011, a law enforcement agent from Homeland Security had opened an account on Silk Road and began making purchases and partnering with other governmental agency to collect and analyze

information obtained from the site. The most vulnerable node in the network were the exchangers, Robert Faiella in particular. In late January 2014, Faiella was charged with "running an exchange service directly on Silk Road that enabled Silk Road users to convert cash into Bitcoins anonymously [and] use those Bitcoins to make illegal purchases on Silk Road."[46] Because Faiella never registered as a money transmitting business, he was in violation of anti-money laundering laws. Once the FBI obtained access to the computer assets and exchange information, the site was shut down and subsequent arrests were made.

Potential Policy Recommendations and Further Research

The case studies described in this paper are only two examples of successful counter threat finance (CTF) operations. The following recommendations offer ways to better understand the implications of cryptocurrencies and alternative remittance systems as threat finance sources and available opportunities to standardize regulatory requirements internationally, refine CTF strategies, and increase collaboration and information sharing between governmental and private industries to keep pace with these rapidly evolving networks.

Promote Stronger International Standards

The international community must adopt global anti-money laundering (AML) standards to regulate cryptocurrencies and alternative remittance systems as a top priority to wage the long-term battle against these threat finance sources and protect the integrity of the global financial system. The FATF is the right organizations to facilitate stronger AML and CTF standards. U.S. policy makers must expedite domestic regulatory legislation that provides oversight to cryptocurrencies. Furthermore, the U.S. should enter into bilaterally and multilaterally agreements with Partner Nations to promote stronger international standards.

Intelligence and Information Sharing

Traditional intelligence techniques should be employed in conjunction with forensic accounting techniques to locate and target operators at decisive points to disrupt threat finance networks. Traditional intelligence activities can identify threat groups that use virtual currency wallets which in turn reveals the locations where cryptocurrency records are stored. Geographic locations with prolonged conflict, corruption, and known transnational criminal and terrorist organizations generally serve as crytocurrency laundering hubs. The Silk Road case proves that undercover Miners can infiltrate the network and exploit the anonymity of cryptocurrency exchanges. Identifying Miners presents opportunities for authorities to seize computer assets and retrieve pertinent data to disrupt the network. In domestic cases, U.S. Government enforcement agencies have the authority to use subpoenas and other legal process to monitor activities, collect data, access exchange records, and seize computer hardware and documents. Regular interagency collaboration, reviews, and security updates are effective forums for intelligence and information sharing.

Financial intelligence and information sharing between U.S. Government, Partner Nations and private industry promotes timely and accurate decision-making pertaining to economic, political, and security matters. By strengthening the connection between governmental and private industries, cryptocurrencies and alternative remittance systems could become opportunities rather than a complex threat. The FATF can serve as a conduit to increase information sharing amongst international CTF agencies and develop common tools and practices for data collection and cryptocurrency threat networks analysis.

Targeted Financial Sanctions

Targeted financial sanctions are another means to effectively disrupt cryptocurrencies and alternative remittance threat networks. The complexity of these threat systems requires extensive research and investigation to identify individuals or State actors who support threat activities. Information sharing also facilitates the enforcement of U.S. and international sanctions. Furthermore, adopting global AML standards to regulate cryptocurrencies and alternative remittance systems makes it more difficult for individuals and States to evade sanctions through increased monitoring activities and timely reporting.

Technological Infrastructure Development

Additionally, U.S. Government and its partners must invest in training and infrastructure to build a coalition of experts with the appropriate assets to analyze and track cryptocurrency transactions in a manner similar to forensic accountants. Security and anonymity are critical requirements for cryptocurrency networks; however, these networks are not completely anonymous. As previously indicated, cryptocurrency transactions require Miners to verify and validate exchanges. The distributed ledger technology (blockchains) automatically store transaction dates and virtually the entire transaction history of the system, making Miners a key node to attack. Innovative technological infrastructure and software need to be developed not only to protect against cybersecurity threats, but also to track and target threat finance networks. Furthermore, just as hackers use cyberattack techniques to steal cryptocurrencies, authorities could use advanced technology to seize balances from virtual wallets, thereby disrupting the network. Partnering with private industry and international cybersecurity organizations facilitates advanced hardware and software development. Silicon Valley and cyber-warfare communities have some of the most qualified individuals to help solve this complex problem.

Conclusion

The U.S. and Partner Nations must remain vigilant and increase operational and technical capabilities to investigate and interdict threat financing at the source. As cryptocurrencies and alternative remittance continue to evolve, financial enforcement agencies must evolve their techniques, tactics, and procedure to identify and target key and vulnerable threat finance nodes. As seen in the Liberty Reserve and Silk Road cases, effectively enforcing AML laws facilitated the indictment and subsequent dismantling of unlicensed money transmitter and the threat networks respectively. Both FinCEN and the FBI used existing laws and traditional intelligence techniques to achieve success. Prosecuting the offenders not only served justice, it also served as a deterrent for illicit networks yet identified. The U.S. must continue to work with the international community to achieve consistency with respect to prosecution worldwide.

Finally, U.S. and international financial authorities should pay close attention to Russia's recent shift from its 2016 policy aim to ban cryptocurrencies. On April 20, 2018, VICE News aired an investigative report by correspondent Michael Moynihan, revealing Russia's efforts to integrate cryptocurrency into its financial system.[47] The president of VNESHECONOMBANK, Moscow's largest investment bank, recently signed a deal with Ethereum cryptocurrency blockchain founder Vitalik Buterin.[48] The 23-year-old will establish a new Blockchain Research Institute to develop Information Technology Specialist to support Russia's quest to be global leader in blockchain technology.[49] While many U.S. lawmakers remain skeptical of long-term stability of cryptocurrencies, leaders in countries such as Russia, Iran, and Venezuela are embracing the technology in an effort to evade U.S. and international sanctions, undermine global trade, and weaken the U.S. dollar. U.S. national security is at risk, and cryptocurrency will remain a threat finance for the foreseeable future.

[1]The White House, *The National Security Strategy of the United States of America* (Washington, DC, 2017), http://www.whitehouse.gov/nsc/nss/2017/.
[2]Juan C. Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare* (New York: Public Affairs, 2013), 2.
[3]*Ibid,* 3.
[4]*NSS*, 10.
[5]US Department of Defense, Countering Threat Networks. JP 3-25 (Washington, DC: US Department of Defense, December 21, 2016), B-1.
[6]Michael Miklancic and Jaqueline Brewer, *Convergence: Illicit Networks and National Security in the Age of Globalization* (Washington DC: National Defense University Press, 2013), xvii.
[7]DoD, JP 3-25, A-2.
[8]Miklancic, *Convergence,* 114.
[9]*Ibid*, 3.
[10]DoD, JP 3-25, A-2.
[11]*Ibid.*
[12]*Ibid*, A-3.
[13]Patrick M. Jost and Harjit Singh Sandhu, *The Hawala Alternative Remittance System and its Role in Money Laundering.* FinCEN (Vienna, VA: Financial Crimes Enforcement Network in cooperation with Interpol General Secretariat, Lyon, January 2000), 5, http://search.ebscohost.com/.
[14]*Ibid.*
[15]Rob McCusker, *Underground Banking: Legitimate Remittance Network or Money Laundering System?* (Canberra ACT: Australian Institute of Criminology, 2005).
[16]Yusef Al-Jarani, "A War Developing Countries Cannot (Afford To) Win." *Yale Law & Policy Review,* 35 (2017): 593. http://search.ebscohost.com/.
[17]*Ibid.*
[18]Miklancic, *Convergence,* 106.
[19]*Ibid.*
[20]*Ibid*, A-4.
[21]Jost and Sandhu, *The Hawala Alternative*, 13.
[22]*Ibid*, 14.
[23]Miklancic, *Convergence,* 122.
[24]*Ibid.*
[25]*Ibid.*
[26]FATF, *Money Laundering Using New Payment Methods* (France: Financial Action Task Force, 2010), 1.
[27]Brill and Keene, *Cryptocurrencies: The Next*, 26.
[28]FATF, *Guidance for a Risk-Based Approach to Virtual Currencies* (France: Financial Action Task Force, 2015), 3.
[29]Cecily Raiborn and Marcos Sivitanides, "Accounting Issues Related to Bitcoins," *The Journal of Corporate Accounting & Finance* (January-February 2015): 26, http://search.ebscohost.com/.
[30]*Ibid.*
[31]Alan Brill and Lonnie Keene, "Cryptocurrencies: The Next Generation of Terrorist Financing," *Defence Against Terrorism Review*, 6, no. 1 (Spring-Fall 2014): 12, http://search.ebscohost.com/.
[32]*Ibid.*
[33]Raiborn and Sivitanides, *Accounting Issues Related*, 26.
[34] *Ibid.*

[35]Otilia Manta and Napoleon Pop, "The Virtual Currency and Financial Blockchain Technology: Current Trends in Digital Finance," *Financial Studies* (March 2017): 51, http://search.ebscohost.com/.
[36]*Ibid.*
[37]Zachary K. Goldman, Ellie Maruyama, Elizabeth Rosenberg, Edoardo Saravalle, and Julia Solomon-Strauss, *Terrorist Use of Virtual Currencies: Containing the Potential Threat* (Washington DC: Center for a New American Security, 2017).
[38]Brill and Keene, *Cryptocurrencies: The Next*, 8.
[39]*Ibid, 9.*
[40]*Ibid,* 18.
[41]*Ibid.*
[42]*Ibid,* 19.
[43]*Ibid,* 20.
[44]*Ibid.*
[45]*Ibid.*
[46]*Ibid,* 21.
[47]*New Kid on the Blockchain,* Television Broadcast, Home Box Office, Inc (2018; USA: VICE Original Series, 2018).
[48]*Ibid.*
[49]*Ibid.*

Bibliography

Alcazar, Vincent. "Data You Can Trust: Blockchain Technology." *Air & Space Power Journal* 31, no. 2 (Summer 2017): 91-101. Ebscohost (123448757).

Al-Jarani, Yusef. "A War Developing Countries Cannot (Afford To) Win." *Yale Law & Policy Review,* 35 (2017): 585-602. http://search.ebscohost.com/.

Brill, Alan and Lonnie Keene, "Cryptocurrencies: The Next Generation of Terrorist Financing," *Defence Against Terrorism Review*, 6, no. 1 (Spring-Fall 2014): 12. Ebscohost.

Crawford, Mark. "The Insurance Implications of Blockchain." *Risk Management* 64, no. 2 (March 2017): 24-28. Ebscohost (121421902).

FATF. *Money Laundering Using New Payment Methods*. France: Financial Action Task Force, 2010.

Goldman, Zachary K., Ellie Maruyama, Elizabeth Rosenberg, Edoardo Saravalle, and Julia Solomon-Strauss. *Terrorist Use of Virtual Currencies: Containing the Potential Threat.* Washington DC: Center for a New American Security, 2017.

New Kid on the Blockchain. Home Box Office, Inc. USA: VICE Original Series, 2018. Television Broadcast.

Jost, Patrick M. and Harjit Singh Sandhu. *The Hawala Alternative Remittance System and its Role in Money Laundering.* FinCEN. Vienna, VA: Financial Crimes Enforcement Network in coorperation with Interpol General Secretariat, Lyon. January 2000. http://search.ebscohost.com/.

Keene, Shima D. "Operationalizing Counter Treat Finance Strategies." *The Letort Papers.* Carlisle: Strategic Studies Institute and U.S. Army War College Press, December 2014. www.StrategicStudiesInstitute.army.mil.

Kirkland, Rik and Don Tapscott. "How Blockchains Could Change the World." *McKinsey Quarterly* no. 3 (2016): 110-113. Ebscohost (118459144).

Manta, Otilia and Napoleon Pop. "The Virtual Currency and Financial Blockchain Technology. Current Trends in Digital Finance." *Financial Studies* 21, no. 3 (March 2017): 45-59. Ebscohost (126014924).

McCusker, Rob. *Underground Banking: Legitimate Remittance Network or Money Laundering System?* Canberra ACT: Australian Institute of Criminology, 2005.

McGreevy, Gerry. "Blockchain: Considerations for Infosec." *ISSA Journal* 15, no. 8. (August 2017): 25-31. Ebscohost (124471361).

Miklaucic, Michael and Jacqueline Brewer. *Convergence: Illicit Networks and National Security in the Age of Globalization.* Washington D.C.: National Defense University Press, 2013.

Moldof, Al. "Bitcoin, An Introduction: Part 1." Accountability

Piazza, Fiammetta. "Bitcoins in the Dark Web: A Shadow Over Banking Secrecy and a Call for Global Response." *Southern California Interdisciplinary Law Journal* 26, no. 3 (Summer 2017): 521-546. Ebscohost (123824519).

Raiborn, Cecily and Marcos Sivitanides. "Accounting Issues Related to Bitcoins." *The Journal of Corporate Accounting & Finance,* (January-February 2015): 26. Ebscohost.

The White House. *The National Security Strategy of the United States of America* (Washington, DC, 2017), http://www.whitehouse.gov/nsc/nss/2017/.

Underwood, Sarah. "**Blockchain** Beyond Bitcoin." *Communications of the ACM* 59, no. 11 (November 2016): 15-17. Ebscohost (119379430).

US Department of Defense. Countering Threat Networks. JP 3-25. Washington, DC: US Department of Defense, December 21, 2016.

Walch, Angela. "Blockchain's Treacherous Vocabulary: One More Challenge for Regulators." *Journal of Internet Law* 21, no. 2 (August 2017): 1-16. Ebscohost (124462667).

Workie, Haimera and Kavita Jain. "Distributed Ledger Technology: Implications for Blockchain for the Security Industry." *Journal of Securities Operations & Custody* 9, no. 4 (Autumn/Fall 2017): 347-355. Ebscohost (125354942).

Zarate, Juan C. *Treasury's War: The Unleashing of a New Era of Financial Warfare.* New York: Public Affairs, 2013.