Prioritizing SOF Counter-Threat Financing Efforts in the Digital Domain

Hugh Harsono

ABSTRACT

Threat financing describes how threat actors move, manage, and raise funds to support their specific goals. One emerging challenge for Special Operations Forces (SOF) support to counterterrorism missions is digital threat financing. This has risen to prominence in recent years with the evolution of digital currencies, cashless payments, and other forms of financial technology that allow for the near-instantaneous transfer of funds from one party to another. As such, SOF must undertake and prioritize counter-threat finance (CTF) efforts for its Theater Special Operations Commands (TSOCs) and its intelligence analysts to deter violent extremist organizations (VEO).

Keywords: *digital threat financing, counter-threat financing, cryptocurrency Campaigns*

INTRODUCTION

Special Operations Forces (SOF) routinely combat threats to the United States, with a specific focus on counterterrorism and counter-violent extremist organizations (CT/CVEO) missions. These efforts include the disruption and surveillance of enemy networks, direct-action missions, and partner-nation capacity building in advise-and-assist roles, among many others. While demonstrating great success at the tactical level, there is a clear need for "more sophisticated counterterrorism training and exchanges that specifically seek out and address the financial aspects of terrorist and VEO operations," argues SOF Colonel Clarence Bowman.[1] *Additionally, the Integrated Financial Operations Commander's Handbook*, which was developed with counter threat-finance

First Lieutenant Hugh Harsono is an Army officer most recently assigned as an Assistant Operations Officer in an Asian-based Special Operations Task Force. His previous military assignments have taken him throughout the Middle East and Asia, and he has served at various levels within the special operations enterprise. He holds a B.A. from the University of California, Berkeley, with a major in economics. Prior to commissioning through the United States Army Officer Candidate School at Ft. Benning, Georgia, Hugh worked in finance for an agrotechnology firm.

activities in mind, specifically mentions that it does not "adequately address counter-threat finance (CTF) activities designed to deny, disrupt, destroy, or defeat financial systems and networks that negatively affect US interests."[2] Keeping this in mind, SOF must begin to address the root causes supporting terrorist/VEO actions, understanding that a critical factor of these root causes revolves around threat financing. As a result, the SOF community must continue to refocus its priorities of effort and dedicate increasing resources to counter-threat finances to provide a long-term solution for CT/CVEO concerns.

Counter-threat financing is a particularly critical factor for SOF to address, given U.S. Special Operations Command (SOCOM) is the "DoD CTF lead component for synchronizing DoD CTF activities and operations."[3] CTF efforts apply to various threat actors, including hostile governments, violent extremist organizations, and paramilitary groups. This is critical because threat actors require financial resources to carry out their specific activities. Today, threat groups often fund these activities utilizing tactics ranging from criminal activities to the taxation of a local populace and online fundraising.[4] In fact, the U.S. Department of the Treasury estimates place similarly-raised Islamic State funds at over $1 billion in total revenue for 2015 alone.[5] Countering threat financing is becoming an increasingly important role within the SOF community. Understanding why it must receive such an intense focus will allow SOF elements to play an effective role in CT/CVEO.

HAWALAS: A TIME-HONORED CODE WITH DIGITAL POTENTIAL

The *hawala* system is a popular informal banking network and money transfer mechanism utilized primarily in the Middle East, North Africa, the Horn of Africa, and the Indian subcontinent.[6] Hawala forgoes modern banking technology in favor of a time-tested

network of honor-bound money brokers, also known as *hawaladars*,[7] who move funds without concern for specific nation-state borders or banking system rules. The hawala system is especially appealing to threat actors due to its relatively untraceable nature and ability to mobilize funds quickly from around the globe.[8] Despite the longstanding popularity of hawala, cryptocurrency has gained traction among an ever-increasing pool of users worldwide in recent years. More popularly known through brands such as Bitcoin, Ripple, and Ethereum, cryptocurrencies are peer-to-peer, public, and open-source digital platforms that also possess the ability to facilitate the movement of money with relative anonymity. This ability also makes cryptocurrency popular among threat actors, from fundraising in the Gaza Strip by the Ibn Taymiyya Media Center[9] to the allegation of digital currency used to help organize the ISIS-backed 2019 Sri Lanka Easter bombings.[10]

However, as efficient as the hawala system may be, younger generations are more often in tune with the utilization of the Internet in conducting everyday transactions,[11] to include money movement among different nation-states and groups. As such, digital currencies have, in some ways, replaced the hawala network, allowing individuals to bypass the socialized and relationship-based nature of the hawala in favor of near-instant transactions.[12] Therefore, the US government must continue to monitor digital currencies for involvement in terrorist activity, enabling the disruption of specific funding, activities, and organizing of threat actors.

HOW DIGITAL CURRENCIES WORK

Digital currencies, also known as cryptocurrencies, have the potential to replace traditional banking systems, with their source of innovation coming from the blockchain construct. Utilizing conventional banking as an analogy, the blockchain is essentially a full historical log of banking transactions shared by all users.[13] However, unlike traditional banking, the blockchain is public and decentralized, providing a higher degree of transparency within the cryptocurrency construct. Therefore, the transfer of cryptocurrencies is 100 percent digital in nature and conducted between two individuals or organizations through online exchange platforms. This type of peer-to-peer transaction allows for a certain level of anonymity when using digital currencies.[14] This relatively anonymous framework emerges primarily in two forms: the tying of individuals to specific cryptocurrency accounts as well as the utilization of digital exchanges. The relatively anonymous nature of cryptocurrency has created significant differences in the enforcement of Know Your Customer/Anti-Money Laundering (KYC/AML) regulations across various nation-state borders.[15] This presents challenges in tying individuals to specific cryptocurrency accounts.[16] Similarly, the use of digital exchanges to transfer cryptocurrency into spendable money is also difficult to trace due to the relative fluidity of such exchange organizations.[17] Therefore, cryptocurrencies have become a kind of virtual hawala,[18] utilizing a network of connected digital actors to move specific amounts of money throughout the world.

Threat actors are continuing to expand their ability to maintain, store, and share funds among themselves, while taking advantage of a lack of oversight and regulations.[19] Consequently, with digital currencies allowing for the virtual movement of money that is protected under an umbrella of anonymity, it is vital for the SOF community to properly assess the threat for what it is: a difficult-to-trace way of funding threat actors, which has received insufficient emphasis in today's military. It is therefore incumbent on SOF to understand and counter the potential risk that digital threat financing poses to national security.

CAN SOF COUNTER DIGITAL THREAT FINANCING?

The SOF community has the unique ability to carry out a variety of missions throughout the world. However, its focus must shift from strictly kinetic engagements to cooperating with US partners. There are a variety of ways that SOF can utilize both current and emerging assets to provide further emphasis on the root funding sources of terrorist/VEO groups. It is critical for SOF to increase CTF personnel presence at Theater Special Operations Command (TSOC) unit level, as well as providing more emphasis on digital financial intelligence (FININT) collection.

Some readers may pose the question, "Why SOF?" Other organizations are already tackling the problem of threat financing, including the National Security Agency, the State Department,[20] and the Federal Bureau of Investigation-led National Cyber Investigative Joint Task Force.[21] Additionally, many defense practitioners believe it is difficult to operationalize threat finance intelligence efforts. However, the increasingly digital-exclusive nature of finance requires increased coordinated efforts between all government and law enforcement entities, necessitating SOF-led Department of Defense (DoD) involvement in such requirements. Additionally, SOF is the one entity most flexible and adaptable organization within the DoD, providing the military with the potential ability to action and operationalize any intelligence that emerges from CTF efforts.

SOF must begin to provide additional resources to staff CTF global requirements. Currently, USSOCOM has minimal personnel working on countering threat financing. This group is located within the Counter-Threat Finance Branch of USSOCOM's J-36 Transnational Threats Division.[22],[23] Despite an established ability to examine threat financing, the J-36 is extremely limited in size, with the Counter-Threat Finance Branch having less than a handful of individuals to tackle issues globally.[24] This framework helps consolidate information at the USSOCOM level. It demonstrates that USSOCOM is shifting its focus to emphasize and examine threat finance. Unfortunately, to create actionable objectives arising from CTF efforts, USSOCOM must increase CTF personnel presence at TSOCs to establish global reach and presence, specifically with an emphasis on digital fund payments and transfers. Establishing such a priority will drive the regionally aligned TSOCs to focus on CTF efforts specifically in their regions of responsibility and the digital domain, allowing a deeper understanding

of both area-based and online nuances regarding digital threat financing. Additionally, the joint nature of TSOCs provides for a distribution of information within SOF, branching out to all the different service components within DoD and providing further engagement to each subordinate component cyber group. Ultimately, distributed CTF personnel will allow for tailored region-specific capabilities approach to be implemented much more effectively at the local level.

Additional emphasis must also be placed upon collecting digital FININT while ensuring that CTF efforts remain an emerging critical priority. This precise targeting method as a military strategy is particularly important, given the almost limitless area covered by the Internet. Therefore, if applied with extreme precision, CTF can be a useful tool for network disruption by tracking and potentially halting the monetary flow between terrorists and VEOs. FININT will continue to evolve in the digital realm regarding financial records, specific VEO-favored exchanges (such as those lacking in KYC/AML regulations), and much more. However, intelligence collectors must be aware and capable of exploiting and operationalizing FININT.[25] While traditional methods of tracking money flow between international organizations are notions that have been accepted and utilized for some time, the use of digital networks to transfer funds remains relatively new.[26] This creates a scenario where the value of such intelligence is through its recognition and interpretation, with careful analysis enabling the identification of specific items such as critical targets, monetary flow, and terrorist/VEO affiliates.[27] These digital trails can be followed by a careful collection of FININT, allowing SOF intelligence analysts to enhance their understanding of digital terrorist/VEO funding methods. Additionally, financial disruption strategies will enhance CT/CVEO operations with immense effect, ensuring a more sustainable way of effecting actions against threat actors. These efforts are possible only if FININT is prioritized and taught to intelligence collectors, with many of these individuals already having a presence within the SOF community.

SOF possesses a ready-made framework to help curb digital threat finance opportunities. With key stakeholder relationships created between strategic interagency and international partners, the SOF community already has a presence and intelligence collector ability to provide this shift in emphasis to CTF efforts. However, additional personnel must be placed at the TSOC level to increasingly effect CTF presence, while SOF intelligence collectors must be trained to identify and analyze FININT. These two critical opportunities offer other means to address threat actors in their tracks through countering digital threat financing.

CONCLUSION

Digital threat financing is an emerging issue with which SOF must swiftly contend. The emerging nature and use of digital currencies afford SOF the ability to shape the digital battlefield and develop the proper implementation actions to address this critical national security threat. SOF possesses the necessary tools to commit to such actions, and with its unique flexibility and skill in adapting to dynamic situations it is postured to be the premier US instrument to counter digital threat financing. In conjunction with the abilities of and cooperation with, other organizations, SOF can genuinely help make a difference on the frontline in curbing digital threat financing efforts.

NOTES

1. Clarence W. Bowman, *Countering Threat Finance as a Critical Subset of Irregular Warfare: An Interpretive Case Study of Northern Nigeria*; Report, Fort Leavenworth, KS: United States Army Command and General Staff College, 2009, 1-63.
2. Joint Warfighting Center, *Integrated Financial Operations Commander's Handbook*. Manual. Joint Concept Development and Experimentation, United States Joint Force Command, 2010, 1-126.
3. Jennifer E. Carter, *Emerging DoD Role in the Interagency Counter Threat Finance Mission*, Report, Fort Leavenworth, KS: United States Army Command and General Staff College, 2012, 1-34.
4. Howard Altman, "SOCOM Tracking Money that Funds Violent Extremists," March 29, 2015, accessed August 1, 2019, http://tbo.com/list/military-news/altman/socom-tracking-money-that-funds-violent-extremists-20150329/
5. Zachary Goldman, Ellie Maruyama, and Elizabeth Rosenberg, *Terrorist Use of Virtual Currencies*, Report, Washington DC: Center for a New American Security, 2017, 1-56.
6. Genesis Martis, *A guide to understanding hawala and to establish the nexus with terrorist Financing*, Report, Miami: Association of Certified Anti-Money Laundering Specialists, 2018, 1-25.
7. Martis, 9.
8. Financial Action Task Force, *The Role of Hawala and Other Similar Service Providers in Money Laundering and Terrorist Financing*, Report, "Paris: Organisation for Economic Co-operation and Development," 2013, 1-70.
9. Yaya J. Fanusie, "The New Frontier in Terror Fundraising: Bitcoin," August 24, 2016, accessed July 15, 2019, https://www.thecipherbrief.com/column/private-sector/the-new-frontier-in-terror-fundraising-bitcoin.
10. Yashu Gola, "ISIS Used Bitcoin to Fund Horrific Sri Lanka Easter Bombings, Research Claims". February 05, 2019, accessed August 10, 2019, https://www.ccn.com/isis-bitcoin-fund-sri-lanka-easter-bombings/.
11. Jaime Toplin, "Gen Z Banking & Payments Trends for 2020." May 1, 2019, accessed December 29, 2019, https://www.businessinsider.com/banking-and-payments-for-gen-z.
12. Atanu Biswas and Roy, Bimal, "Bitcoin, the new hawala," June 14, 2017, accessed August 10, 2019, https://economictimes.indiatimes.com/blogs/et-commentary/bitcoin-the-new-hawala/.
13. Australia Securities & Investments Commission, "Cryptocurrencies," October 24, 2018, accessed July 30, 2019, https://www.moneysmart.gov.au/investing/investment-warnings/virtual-currencies.
14. Australia Securities & Investments Commission, 2.
15. Allen & Overy Consulting, Cryptocurrency AML risk considerations, Report, "Legal and Regulatory Risks for the Finance Sector," 2018, 1-10.
16. Allen & Overy, 3.
17. Allen & Overy, 4.
18. Biswas & Roy, 2.
19. Cynthia Dion-Schwarz, David Manheim, and Patrick Johnston, 16.
20. Dana Priest and William Arkin, "A hidden world, growing beyond control," July 18, 2010, accessed August 5, 2019, https://www.pulitzer.org/cms/sites/default/files/content/washpost_tsa_item1.pdf
21. Brandon Gaskew, "Reader's Guide to Understanding the US Cyber Enforcement Architecture and Budget," February 21, 2019, accessed July 30, 2019, https://www.thirdway.org/memo/readers-guide-to-understanding-the-us-cyber-enforcement-architecture-and-budget.
22. Altman, 3.
23. House Committee on Armed Services Subcommittee on Terrorism and Unconventional Threats and Capabilities, 111th Congress, 7 (2009) (testimony of Matthew Levitt).
24. Kurt Gredzinski. "LinkedIn Profile," accessed August 10, 2019, https://www.linkedin.com/in/kurt-gredzinski-0a9b7315.
25. Joint Warfighting Center, 15.
26. Resty Woro Yuniar, "Bitcoin, PayPal Used to Finance Terrorism, Indonesian Agency Says,"World - Asia News. January 10, 2017, accessed October 18, 2017, https://www.wsj.com/articles/bitcoin-paypal-used-to-finance-terrorism-indonesian-agency-says-1483964198.
27. Shima D. Keene, "Operationalizing Counter Threat Finance Strategies," Paper, Carlisle. PA: U.S. Army War College, 2014, 1-51.