

COMMENT 217 - Terrorism financing: Crypto-Taliban?

By **Siegfried O. Wolf**

26 August 2021– DOI: [10.48251/SADF.ISSN.2406-5617.C217](https://doi.org/10.48251/SADF.ISSN.2406-5617.C217)



Dr. Siegfried O. Wolf, Director of Research at SADF (Coordinator: Democracy Research Programme); he was educated at the Institute of Political Science (IPW) and South Asia Institute (SAI), both Heidelberg University. Additionally he is member (affiliated researcher) of the SAI as well as a former research fellow at IPW and Centre de Sciences Humaines (New Delhi, India). Dr Wolf works as a consultant to NATO-sponsored periodic strategic independent research and assessment of Afghanistan-Pakistan issues.

The [United Nations Counter-Terrorism Week](#) in June 2021 focused on the financing of Islamist terror groups. The meeting zeroed in on the ‘[misuse of digital space for terrorist financing purposes](#)’. As noted in a [statement following](#) the meeting, ‘it was recognized that the pandemic enhanced opportunities for terrorist groups particularly to raise funds through online sources. The pandemic also impacted on the implementation of CFT [Countering the Financing of Terrorism] legislation and responses, particularly regarding the adoption of a regulatory framework to address the vulnerabilities of the virtual assets for terrorist financing purposes.’ Numerous speakers [pointed out](#) that the ‘digital space was a quickly evolving area and that terrorist groups acquired highly-specialized expertise in using all opportunities offered to raise and transfer funds through virtual assets platforms and well as to obfuscate the traceability of these transactions through complex blockchain mechanisms’.¹ The event, organised by the Counter Terrorism Committee of the United Nations Security Council, reflects heightened concerns. Due to the increased scrutiny on the traditional, formal financial sector², some are [concerned](#) that terrorists might ‘seek more secretive mechanisms for financing their activities’. Numerous actors involved in the set-up of the Anti-Money Laundering and

¹ Assistant Secretary-General Michèle Coninx, Executive Director, Counter Terrorism Executive Directorate: ‘We have focused on risks relating to increased use of the so-called digital space to raise and move funds, make payments, and conduct all kinds of financial transactions. Although these trends emerged well before the pandemic, the virtual nature of such transactions has certainly proven critical to reducing the risk of spreading the Covid-19 virus and to ensuring the continuation of essential financial services. However, it has also affected the ability of financial institutions and State authorities to identify anomalies and may have attracted criminal abuse, including by terrorists and their financiers attempting to benefit from the seemingly anonymous payment methods.’

² For example, through international watchdogs like the Paris-based Financial Action Task Force ([FATF](#)).

Countering the Financing of Terrorism provisions identify a serious threat scenario created by speedy and technologically complex payment methods provided by the digital space in the form of virtual (crypto) currencies (or VCs). Generally described as anonymous and able to operate across jurisdictions - meaning outside any meaningful oversight - VCs can be seen as the ‘[ideal way](#)’ for terrorists to hide their financing methods from both government agencies and law enforcement. By creating ‘[a “parallel” financial system that eludes traditional controls](#)’, it is predicted that VCs can speedily make ‘[the global regulatory system to block terrorist financing obsolete](#)’. Terrorist groups and their underlying (supporting) networks [are exploring](#) the new financial technologies (FinTech) to further their efforts. [According to](#) Yaya Fanusie from the Foundation for Defence of Democracies, ‘jihadist facilitation networks are innovating their financing methods by soliciting cryptocurrencies [foremost Bitcoin, the currently “lead currency” of the crypto market] to raise funds. Indeed, in recent history, [multiple examples of terrorist cryptocurrency funding campaigns](#) were detected,³ providing evidence for growing Jihadist activities in the digital space. Experts are therefore [identifying](#) ‘crypto-enabled terrorist financing as a real risk that demands serious attention’ and ‘[government authorities and organisations that track terrorist financing have begun to raise alarms about an uptick in the number of Islamist terrorist organizations experimenting with Bitcoin and other digital coins](#)’.

Notwithstanding, some observers stress the many obstacles and challenges faced by VCs. Some of the major limitations of VC usability as far as terrorists are concerned include high [price volatility](#) – the volatile nature of the crypto market makes VCs an unreliable [method of transferring or moving funds in meaningful volumes](#) in order to finance operations in a timely fashion. Furthermore, unlike traditional cash payments, VC transactions in the digital space are traceable, undermining the anonymity of those involved. [According to Benoît Gomis](#), ‘terrorist organisations appear to have largely steered clear of cryptocurrencies because of the lack of reliable technical and telecommunications infrastructure in many countries where they operate’. Furthermore, ‘managing large amounts of

³ For instance, in August 2020, the U.S. Department of Justice [announced](#) the disruption of two terrorism financing campaigns that utilized VC donations. These were carried out by al-Qaeda (and affiliated terror groups) as well as by al-Qassam Brigades, the military arm of Hamas.

cryptocurrencies requires specific skills, such as being “extremely savvy in cyber security”,’ which most of Jihadists – [according to experts](#) – do not appear to be.

In the centre of discussion lies the issue of how to monitor, control, and regulate financial cryptocurrency transactions in the digital space. Here, cryptocurrency exchanges ([digital marketplaces](#) that facilitate trade in cryptocurrency) are gaining significance. These platforms function both as marketplaces for selling and buying of VCs online and as ‘connection points’ between the digital space and the ‘[real world](#)’ (with its traditional financial mechanisms). In technical terms, at these connection points fiat money (government-issued currency) is transferred into VCs and other way around. The central role of these exchanges for VC transactions - and thus their potential use for the financing of terrorism – made them the focus of regulators, including the Countering the Financing of Terrorism/Anti-Money Laundering watchdogs.

However, in the light of the technological advancements and the apparent build-up of digital skills and capacities by terrorists and their supporting networks one must wonder what happens when these ‘connection points’ concern states with little or no Countering the Financing of Terrorism/Anti-Money Laundering regimes in place. Such is the case of Pakistan, much more even of Afghanistan. Taliban-controlled Afghanistan could expand from being a mere physical hub for international terrorist groups towards becoming an online nodal point for crypto/fiat currencies transactions outside appropriate oversight.

It is interesting [to stress](#) that ‘Bitcoin adoption in Afghanistan has shot up over the last year amid economic turmoil brought about by the Taliban’s takeover of the country’. The Taliban overthrow of the Afghan government left the citizenry not only in life-threatening situations but also facing financial difficulties.⁴ It seems that many Afghans turned towards the crypto market to safe their financial assets. It seems unlikely that the signs of a growing crypto adaption in Afghanistan will go unnoticed by the Taliban. Considering the poor, deteriorating status of the country’s banking sector, one should expect not only an emerging [crypto economy](#) but also a

⁴ [According to observers](#), some of the most severe challenges regarding financial aspects the Afghan people are currently facing include ‘a mix of bank closures, cash shortages and the suspension of international money transfers from leading remittance providers like Western Union and MoneyGram’.

rapidly growing misuse of it, perhaps foremost by the Taliban and other affiliated terrorist organisations. Afghanistan might well become a launchpad for illegal (terror) activities in the digital space beyond terror financing purposes like cyber-attacks or online radicalisation campaigns. Finally, the emerging “liaison” between Beijing and the Taliban - as well as the triangular comradery that includes Pakistan - should be matter of additional concern considering possible technology transfers from China to Afghanistan.

References:

Alexandre, A. (2018, September 11). Report: Crypto Not Effective for Financing Terrorist Groups. Cointelegraph.

<https://cointelegraph.com/news/report-crypto-not-effective-for-financing-terrorist-groups>

Carlisle, D. (2019, February 13). Countering the Use of Cryptocurrencies for Terrorist Financing. Elliptic. Blog.

<https://www.elliptic.co/blog/countering-terrorist-financing-cryptocurrency>

Cuthbertson, A. (2021, August 23). Bitcoin adoption in Afghanistan spikes amid Taliban takeover.

<https://www.independent.co.uk/life-style/gadgets-and-tech/bitcoin-afghanistan-crypto-taliban-economy-b1907180.html>

Gomis, B. (2019, November). Crypto connections: Terrorists' use of cryptocurrency remains limited. Jane's Intelligence Review.

https://www.researchgate.net/publication/349722204_Crypto_connections_Terrorists'_use_of_cryptocurrency_remains_limited

Keatinge, T., Carlisle, D., & Keen, F. (2018, May). Virtual currencies and terrorist financing: assessing the risks and evaluating responses. Brussels: European Parliament, Directorate General for International Policies. Policy Department for Citizens' Rights and Constitutional Affairs. Counter Terrorism.

[https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU\(2018\)604970_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf)

Little, K. (2021, July 20). Want to Buy Crypto? Here's What to Look for In a Crypto Exchange. NextAdvisor (in partnership with Time).

<https://time.com/nextadvisor/investing/cryptocurrency/what-are-cryptocurrency-exchanges/>

Popper, N. (2019, August 18). Jihadists See a Funding Boon in Bitcoin. The Wall Street Journal.

<https://www.wsj.com/articles/jihadists-see-a-funding-boon-in-bitcoin-1519131601>

Salami, I. (2017). Terrorism Financing with Virtual Currencies – Can Regulatory Technology Solutions Combat this? Studies in Conflict & Terrorism.

<http://dx.doi.org/10.1080/1057610X.2017.1365464>

https://www.researchgate.net/publication/319136877_Terrorism_Financing_wi_th_Virtual_Currencies_Can_Regulatory_Technology_Solutions_Combat_This

Saravalle, E., & Rosenberg, E. (2018, January 9). Bitcoin can help terrorists secretly fund their deadly attacks. Fox News.

<https://www.foxnews.com/opinion/bitcoin-can-help-terrorists-secretly-fund-their-deadly-attacks>

Sigalos, M. (2021, August 21). Inside Afghanistan's cryptocurrency underground as the country plunges into turmoil. CBNC.

<https://www.cnn.com/2021/08/21/bitcoin-afghanistan-cryptocurrency-taliban-capital-flight.html>

Tarrant-Cornish, T. (2018, January 10). Terrorist dream come true' ISIS using Bitcoin to fund deadly attacks and buy weapons. Express.

<https://www.express.co.uk/finance/city/902517/ISIS-Bitcoin-terrorist-attack-deadly-weapons-funding-cryptocurrency-money-laundering>

U.S. Department of Justice. (2020, August 13). Global Disruption of Three Terror Finance Cyber-Enabled Campaigns. Washington: U.S. Department of Justice, Office of Public Affairs.

<https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns>

United Nations. (2021, June 25). The Permanent Missions of France and India, UNODC, UNOCT, CTED and the 1267 Monitoring Team hold side event about countering the financing of terrorism in the post COVID-19 landscape. United Nations, Security Council, Counter Terrorism Committee (CTC).

<https://www.un.org/securitycouncil/ctc/news/permanent-missions-france-and-india-unodc-unoct-cted-and-1267-monitoring-team-hold-side-event>