ACAMS

SANCTIONS SPACE

WHERE CRYPTOASSETS MEET CONFLICT: THE ROLE BEING PLAYED BY CRYPTO IN THE UKRAINE.

Tragic events in Ukraine have established a new rank of armchair generals operating in the social media ecosphere. This is unsurprising given our capacity to jump on technological developments to justify our own point of view or denigrate someone else. During previous international wars the threat of terrorist or proliferation financing has been front and centre of a global response. Yet, this might be the first war where a particular form of technology has been a critical element of international debate for its perceived role in events.

Cryptoassets have been picked out as integral to Russian sanctions evasion, money laundering and aggressive cyber-attacks and, on the flip side, Ukrainian fundraising efforts for its military and NGOs. This quandary was visibly demonstrated this week when the Ukrainian Vice Prime Minister called for all Russian cryptoasset exchange accounts to be frozen whilst, at the same time, the government-verified Twitter account called for donations in Bitcoin, Ethereum or USDT to the Ukrainian military. This article attempts to breakdown what we do and don't know about cryptoassets' influence on the current conflict and where events might take us.

That there are a variety of myths around cryptoassets and their links to criminality might be stating the obvious, but to some it is less well accepted. Perhaps predictably the first practical use of cryptoassets was to purchase drugs, weapons or fraudulently obtained data to target others. Criminals getting in front of technology is hardly news but the supposed complexity of cryptoassets – its pseudonymous, decentralised and peer-to-peer facets contributed to a widespread view that cryptoassets principal function was to facilitate criminality.

Certainly, cryptos' link to darknet marketplaces, criminally complicit exchanges and malign North Korean activity have not helped its public reputation. Cryptoassets, whether you trust in its underlying technology/ benefits, have an image problem. Even investors in cryptoassets sometimes believe it is simply a tool for money laundering or fraud. How far this reputation is fair and whether it is currently being reassessed bears consideration.

[i] Chainalysis.

A few points to note:

- Illicit activity involving cryptoassets is believed to correspond to 0.15% of its legitimate use[i].
- For all their notoriety, cryptoassets are now widely acknowledged by law enforcement and blockchain forensic firms as being inherently trackable and traceable.
- There are multiple proven ways and means of money laundering or sanctions evasion that threat actors are likely to consider effective tactics.
- Liquidity trading and off-ramping illicit cryptoassets is arguably harder than fiat currency.
- Oligarchs and Government officials attempting to use cryptoassets are stymied by the same barriers as bog standard criminals: regulation, investigation, and limited opportunity.

All this paints a balanced picture of the extent of cryptoasset abuse and its possible utility in the Ukraine war. This perspective is reinforced when money laundering and sanctions evasion tactics by jurisdictions such as Russia and Iran have so many other potential methodologies. If you know you can circumvent sanctions and AML controls via trade-based money laundering, money laundering through the capital markets or trade finance mechanisms, why complicate matters? Still, the perception of threat remains. Cryptoassets are tarred by their own past. So, what can we differentiate about the nature of the threat and the risk cryptoassets pose to this and other conflicts?

Cryptoassets are utilised by criminals and nation states alike to undertake illicit activity. North Korea alone is suspected to have built up reserves of $400m of cryptoassets through hacks on crypto exchanges in 2020 and, presumably, financial speculation of these funds. Russia is a known hub for cyber-criminality and ransomware with ¾ of the proceeds of ransomware attacks in 2020 going through Russian hackers[ii]. At the other end of the scale, drug dealers put their illicit proceeds through cryptoasset ATMs and peer-to-peer services and cryptoassets are the known currency of choice for online paedophilia. So, are cryptoassets as risky as some commentators and financial institutions claim?

That risks exist is obvious enough. However, is this not true of fiat currency (Dollars, Sterling, Euros etc), to a far greater extent? Russia could employ its intelligence forces to undertake massive ransomware attacks on Ukrainian and/or Western entities for which the currency of exchange would be cryptoassets, probably incorporating privacy enhancing tokens such as Monero or Zcash. Frequent hacking attacks on crypto exchanges are highly profitable and low risk for cybercriminals. Even the process of mining cryptoassets is judged to be profitable for jurisdictions such as Iran.

Does this suggest that the risk is real? Absolutely. ‘Parasite’ exchanges such as SUEX and Chatex have been eliminated by U.S. law enforcement action. But this malign activity is a drop in the ocean compared to ‘traditional’ means of money laundering, including corporate structures, correspondent banking or alternative investments. Loopholes and vulnerabilities in the cryptoasset ecosphere certainly need to be mitigated and cracked down on. Early signs are positive. Cryptoasset forensic firms are adept, as the Watergate scandal

[ii] Ibid.

put it, at 'following the money'. Law enforcement have recently seized billions in funds from known criminal wallets.

Ransomware will almost certainly increase as a means of hostile state activity as well as a criminal cash cow. Nevertheless, for all the (high)-risk activity linked to cryptoassets, we should consider that many of its flaws and vulnerabilities are down to other factors, principally cybersecurity. Nobody singles out cash as the main enabler for criminality during a bank robbery. Someone will always try to exploit new technology. This is not a surprise. As with other forms of currency exchange and transmission, the issue could more efficiently be dealt with through effective regulation, governance, and education.

Cryptoassets and blockchain technology are at a crossroads. With the right education, advocacy, and training, cryptoasset exchanges in regulated jurisdictions can become a vital cog of anti-financial crime efforts. Sanctions exploitation might be considered persona non grata amongst cryptos growing take-up of users, not least in the Ukraine, which ranks 4th in the world in terms of cryptoasset adoption. Historically, Russia has demonstrated an aversion to cryptoassets and has even gone so far as to ban their use, although recent disputes between the Russian Central Bank and the Government appear to row back from that position, and a digital ruble is now being developed.

Cryptoasset supervision is a core component to reducing the risk of widespread abuse of cryptoassets and their infrastructure. Many countries have begun to apply the basic precepts of the Financial Action Task Force guidance on how to control cryptoasset money-laundering risks. This guidance focuses on treating cryptoasset services as 'virtual asset service providers' (exchanges in common parlance) and extends to applications such as DeFi, NFTs and DAOs. The United States classes exchanges as money services businesses and effectively treats them the same as other firms registered under the Bank Secrecy Act.

Sadly, we are yet to see uniformity in this endeavour. Some jurisdictions lag behind the supervision and requirements demanded by other countries. As the Financial Stability Board recently made clear, a collective and holistic framework for regulation is vital to manage wider cryptoasset related risks. The eagerly awaited White House Executive Order on cryptoasset regulation has been delayed but is expected to recommend a 'whole of government' approach to managing cryptoasset national-security risks. The Chairman of the FATF has made statements expressing his concerns about jurisdictions not implementing the 'travel rule' requiring an exchange of information tied to digital-asset transfers.

What can the industry do to prove its credentials? First and foremost, act to apply current regulations and put in place a framework of systems and controls in accordance with local and multilateral guidance. Many of the best cryptoasset exchanges have adopted these controls, be they transaction monitoring, KYC, or sanctions screening. Crypto forensic capabilities back up many large exchanges' investigative capacity. Although, sadly, regulatory arbitrage and porous compliance still persist in parts of the world yet to sign up to the FATF doctrine of cryptoasset services as VASPS, providing threat actors with a chance to sidestep restrictions on their ill-gained assets.

'TradFi' institutions such as retail, wholesale, insurance, and asset management firms have had over 30 years to respond to AML/CTF rules, not always successfully to say the least. What should cryptoasset providers learn from this paradigm? Doing the right thing should be a cultural shift rather than a tick-box exercise. Cryptoasset services and other fintechs are uniquely well placed to implement world-class compliance systems. Investment in personnel, training, and cyber-security will stand the industry in good stead. All of this is an established part and parcel of banking cooperation with law enforcement, such as the FinCEN Exchange or the National Cyber Forensics and Training Alliance. Now is the moment to test how far the industry has come.

ACAMS is the largest global membership organization dedicated to enhancing the knowledge and skills of anti-money laundering (AML) and financial crime prevention professionals from a wide range of industries, *with over 85,000 members in over 175 countries/regions*. Its CAMS certification is the most widely recognized AML certification among compliance professionals worldwide. *ACAMS offers two exclusive programs for sanctions professionals – the internationally recognized Certified Global Sanctions Specialist (CGSS) accreditation, and the Sanctions Compliance Foundations online certificate (new in 2021).*

Visit **acams.org** for more information.

Joby Carpenter
Global SME – Cryptoassets and Illicit Finance

March 2022