Trends in Terror Finance

Part 2: The Unregulated Sector

by John Solomon - World-Check Terrorism & Insurgency Unit

This is the second of three reports addressing the unregulated financial sector in regard to its use for the financing of terrorism. The first report discussed the anticipated shift from low-tech informal value transfer systems (IVTS) to increasingly high-tech IVTS. It specifically explored mobile banking (m-banking) as an emerging path for TF. The third report will examine the regulatory challenges and possible responses to high-tech IVTS.

This report examines two additional and interrelated high-tech modalities that are vulnerable to TF: virtual currencies (or 'e-currencies') and massive multiplayer online games (MMOGs). Virtual currencies are digitized forms of money issued by private sector companies that function without the backing of national governments. Overlapping with virtual currencies are virtual worlds which are also known as MMOGs. MMOGs are virtual online worlds where hundreds of thousands of people can meet and interact simultaneously via the Wide World Web. Second Life is perhaps the most prominent example. Virtual worlds often contain unregulated economies in which substantial sums of money can be exchanged anonymously without government oversight. E-currencies and MMOGs are generally unregulated and the industries involved have heretofore not undertaken baseline Know-Your-Customer procedures. Therein lies the danger.

HIGH-TECH IVTS: VIRTUAL CURRENCIES

Unregulated or under-regulated virtual currencies on the Internet, similar to m-banking and other modes of high-tech IVTS, are most probably attractive to tech-savvy terrorists and insurgents that are intent upon moving and storing money for their attacks and infrastructures.

The use of virtual currencies to launder illicitly obtained money has been associated closely with transnational crime groups that take part in cyber fraud schemes involving the theft of private identification and credit card information. Terrorist financial operatives have continuously demonstrated that they are never far behind their professional criminal counterparts.

The World Wide Web is the medium through which virtual currency issuers and exchange agents operate in order to facilitate global financial transactions for their customers. The issuers provide the virtual currency and usually back its value through precious metal holdings such as gold or platinum. These issuers also provide financial services similar to what a brick and mortar banking institution would provide to its checking account customers. The exchange agents buy and sell virtual currency in exchange for other virtual currencies or national currencies.

Customers can purchase virtual currencies from exchange agents online using an array of real or virtual currencies. In order for customers to use virtual currency for goods and services, they can use a debit card linked to a corresponding e-currency account. Issuers and exchange agents may issue debit cards that bear well-known credit card brands, which enables holders of virtual currency to easily obtain national currencies and goods and services at ATMs and retailers worldwide.

The use of virtual currencies as a money laundering tool has trended up over recent years as criminals of all stripes gravitate towards online money laundering strategies. The story of E-Gold, an Internet currency exchange, is such an example.

E-Gold is operated online and, until it faced US federal charges earlier this year, was physically registered in Nevis, a financial jurisdiction known for its lax regulatory oversight. E-Gold gave its customers an anonymous way to move and store value backed against a supposed gold reserve held privately in Europe and the United Arab Emirates. Identity thieves, credit card fraudsters and child pornographers in cyberspace all demonstrated an acute predilection for the anonymous financial services which E-Gold was reputed to provide.

For example, E-Gold functioned as the de facto bank and currency for some members of Shadowcrew, a global crime forum that operated in cyberspace as a virtual market for stolen identification and financial information. According to a 4 October 2007 US affidavit brought by the US Secret Service, Omar Dhanani used E-Gold to reportedly launder between $40,000 to $100,000 a week for Shadowcrew from his Fountain Valley, California, home.

The money laundering and terrorist financing risk in regard to virtual currencies such as E-Gold was made clear in an April 2007 US Department of Justice indictment. The indictment accused E-Gold of money laundering and illegal money transmitting from 1999 through December 2005. In the context of this indictment and the emerging trend of illicit use of high-tech IVTS, a senior official in the FBI's Cyber Division said: "The advent of new electronic currency systems increases the risk that criminals, and possibly terrorists, will exploit these systems to launder money and transfer funds globally to avoid law enforcement scrutiny and circumvent banking regulations and reporting."

Terrorists continuously demonstrate that they will use the latest, most sophisticated criminal means to raise and move money. Therefore, practitioners must monitor this typology closely. It must be underscored that terrorists and insurgents often appropriate the illicit activities of their organized crime counterparts in order to raise funds for their attacks and infrastructures.

Like decentralized criminal networks, the al-Qaeda-led Jihadist movement is known to use the Wide World Web extensively for financing activities in addition to other recruiting, radicalization and training purposes.

Cyber fraud is a well-documented typology that al-Qaeda, especially in Europe, has used to raise money.

Second generation British citizen and computer hacker, Younis Tsouli, known online by his handle "Irhabi007" (Irhabi literally means "terrorist" in Arabic), was from 2004-2006 a key conduit connecting Jihadist networks in locations spanning from the US and UK to Abu Musa'ab al-Zarqawi's al-Qaeda network in Iraq.

Tsouli mastered and spread knowledge of online hacking techniques including encrypting sensitive data and communications, constructing Jihadist websites anonymously and, more germane to this topic, cyber fraud. US investigators revealed that Tsouli used stolen credit card numbers and identities to buy web hosting services and some 250 airline tickets with 110 different stolen credit cards. The illegal funds were used to expand the Jihadist presence online and probably to facilitate international travel for terrorist training and mobilization.

A significant portion of Tsouli's energies were devoted to disseminating Jihadist ideology; however, his deputy Tariq al-Dour was more singularly committed to the group's cyber fraud activities. At the time of al-Dour's arrest, in his possession were some 37,000 stolen credit card numbers in addition to the corresponding identity theft information which included addresses, dates of birth and other private credit data.

Using phishing scams and computer programs such as Trojan horses, the group fraudulently charged more than $3.5 million to purchase operational equipment like night-vision goggles, knives and prepaid mobile phones for possible Jihadist recruits.

Tsouli and al-Dour mainly laundered the stolen money through online gambling websites. But as many terrorism experts specializing in the monitoring of Jihadist websites have attested to an increased incidence of cyber fraud schemes within the Jihadist community, it is reasonable to conclude that virtual currencies could be and probably are being exploited by terrorists.

VIRTUAL WORLDS, VIRTUAL CURRENCIES

An overlapping concern regarding virtual currencies is their use in Virtual Online Communities (VOCs) or Massive Multiplayer Online Games (MMOGs) such as Second Life, World of Warcraft and many others. Second Life is an MMOG that has been widely-discussed in the media due both to its popularity (it's said to have five million users) and its potential vulnerability to terrorist exploitation; specifically terrorist financing. Second Life has its own e-currency named the Linden Dollar (LD). As of April 2007, 270 LD equaled $1 in real US currency. With substantial commerce taking place in virtual real estate and commodities, Second Life is a veritable economic zone within which about 1.9 billion LD or $7 million is in circulation daily. For a terrorist to anonymously enter and transact in this economy is not inconceivable.

The problem with Second Life is the very thing that makes it so attractive and popular: anonymity. Creating an avatar or 3-D online identity in Second Life does not require validated identification information. As security officials and terrorism experts indicate, the anonymity factor could enable terrorists to use Second Life and other MMOGs to covertly disseminate ideology, recruit and train. However, the most obvious risk stems from the ability for terrorists to anonymously transfer virtual currencies, since this is a possible TF typology that terrorists should be expected to exploit.

Concern over the specter of money laundering and other illicit activities using virtual currencies in MMOGs has perhaps been most remarkably experienced in China. Chinese lawmakers have been vocal in claiming that the exponential growth of online communities and MMOGs in China has resulted in more money laundering. The lawmakers' protests were followed by an order that China's central bank issued earlier this year. It stated that China's central bank "is strengthening the standards and management of virtual currency used in online games" and "strictly limiting" their use. World of Warcraft and other MMOGs in which virtual currencies are exchanged are exceedingly popular among China's estimated 30m gamers. Internet companies there are reported to have launched at least ten virtual currencies as China's Internet population surged to 137 million by the end of 2006.

While China's experience may not be a representative case of the relationship between MMOGs and money laundering or terrorist financing risk in general, it is reasonable to anticipate based on its example that an increased incidence of money laundering and terrorist financing will likely be symptomatic of the continued growth and popularity of unregulated virtual worlds, economies and currencies.

Although there is insufficient information available at present from which to draw any solid conclusions, more research is needed to determine whether there is a possible correlation between the type of criminal enterprise undertaken by a terrorist operative to raise money and the predicate typology used to launder the ill-gotten gains. For example, the more high-tech the fraudulent activity, the more likely it would seem for the financial operative to use a correspondingly high-tech method to clean the money. Perhaps this would be due to an increasingly tech-savvy and younger generation of Jihadist sympathizers and operatives. Just as al-Dour and Tsouli used the Internet to steal money, so too did they use the Internet to clean it. If this pattern emerges, then as cyber fraud becomes more prevalent as a preferred terrorist financing typology, we should expect to see increased use of virtual currencies by financial operatives as a predicate crime for online scams.

CONCLUSION

Regulatory bodies and the financial institutions, bank and non-bank alike, hold the front lines in the fight against terrorist financing. If the institutions that constitute the financial community fail to take strong, effective countermeasures to mitigate the terrorist financing risks inherent in emerging high-tech IVTS such as virtual currencies and m-banking, the international community's progress combating terrorist finance post-9/11 could be substantially weakened.

Therefore, one of the most salient questions facing legitimate stakeholders is: How to mitigate the risks of terrorist abuse of emerging money transfer systems while at the same time realizing the promising economic potential that could benefit both legitimate consumers and suppliers alike?

Don't miss the final installment in next month's T-Brief. John Solomon's 3-part series on the inner workings of terrorist financing in the unregulated financial sector is a must-read for compliance professionals!