SPEAKER BIOS

Mika Dahiya will be graduating in May 2020 with her M.A. from the Middlebury Institute (MIIS), where she is pursuing a specialization in Financial Crime Management. She recently became CAMS certified and was a beta tester for the new sanctions compliance exam offered by ACSS (the Association of Certified Sanctions Specialists). Mika is currently acting as a project manager, helping to organize the 2020 Monterey Threat Financing Forum, a conference discussing the latest trends in cyber-enabled financial crime. Mika also works as a graduate assistant for the Export Control and Nonproliferation Program (XNP) at the James Martin Center for Nonproliferation Studies at the Middlebury Institute of International Studies in Monterey, California. This past summer, Mika interned in Washington, D.C. with the Bureau of Industry and Security (BIS), in the Investigative Analysis Division (IAD). She acted as a Junior Investigative Analyst Intern, where she was able to investigate and target certain countries and entities of concern. In addition to studying Arabic, she is fluent in Portuguese and Spanish, and has lived, worked or studied in Brazil, Spain, Morocco, Egypt and Tunisia.

Mike Donnelly is currently an MA candidate in Nonproliferation and Terrorism Studies at the Middlebury Institute of International Studies (MIIS), where he is also pursuing a Financial Crime Management Specialization. Additionally, he works as a Graduate Research Assistant at the Institute’s Center on Terrorism, Extremism and Counterterrorism (CTEC). His academic research has focused on terrorist financing, extremist propaganda, and terrorist use of the internet, among other things. His language of study at MIIS is Spanish, which he has used to conduct research and analysis on Latin American security issues. Prior to coming to the Middlebury Institute, Mike earned a bachelor's degree in Criminal Justice from California State University Sacramento, while working as an investigative aide with the Sacramento Police Department's Office of Investigations. Shortly after, he worked as an intern intelligence analyst for Northern Mexico and the Southwestern U.S. border region with Intelligence Fusion, a private intelligence firm based in the UK.

Joules Barragan is a Certified Anti-Money Laundering Specialist (CAMS) and experienced open source intelligence analyst from Los Angeles, California. He recently completed his Master's Degree in Nonproliferation and Terrorism Studies with a specialization in Financial Crime Management at the Middlebury Institute of International Studies at Monterey. He currently works as a Financial Crimes and Compliance Analyst for leading cryptocurrency intelligence firm CipherTrace. In his free time, he produces the financial crimes podcast CashOnly, which he manages with two fellow MIIS alumni. Despite being hard-of-hearing, Joules is a lover of languages and has professional experience working in both Spanish and Russian, both at home and abroad.

Sam Whitefield will graduate from the Middlebury Institute in December 2020, with a specialization in Financial Crime Management. After working in financial consulting, Sam spent two years trading cryptocurrency, a space he has followed closely since 2012. At MIIS, he does open source analysis at the James Martin Center for Nonproliferation Studies and is writing a proliferation financing simulation for the Center on Terrorism, Extremism, and Counterterrorism. This summer, Sam interned on the Policy and Compliance team at Bank of the West, where he helped write policies aligning Bank of the West practices with those of BNP Paribas. Sam speaks fluent French and is preparing to take the CAMS exam in the new year.
BTC-e was once the go-to bitcoin exchange platform for criminal actors, but its operation was clouded in mystery. Recent investigations, arrests, and indictments have shed more light on the extent of the illicit activity that connected this platform to other criminal actors and events.

As a platform, BTC-e was used to launder over $4 billion worth of bitcoin in its 6 years of operation. A significant portion of BTC-e’s business derived from suspicious criminal activity. In the beginning of BTC-e’s operation, there were questions regarding ownership and management of the platform. All that was known was that the platform was possibly based out of Bulgaria or the Seychelles and was affiliated with a Russian phone number and owned by a Seychelles shell company. BTC-e’s web domains were registered to many other countries, further obscuring the true ownership of the platform.

The platform was easily accessible to criminal users. No identifiable information, such as a passport image or utility bill was requested to set up a user account— an email was all that was needed. The BTC-e administration would contact users directly and advise them to wire money to “front” companies in order to avoid SAR reporting requirements. BTC-e never once filed a SAR, even though as an MSB, they were obligated to have a compliance program in place. BTC-e also helped customers layer their transactions by processing funds through a cryptocurrency “mixer”, so the users could make their cryptocurrency transactions largely untraceable.

BTC-e was later connected to other cryptocurrency exchanges such as Mt. Gox and Liberty Reserve. Mt. Gox, once the world’s largest bitcoin trading platform before 2014, announced bankruptcy due to the mysterious disappearance of $450 million worth of bitcoins. It was later discovered that hackers had gained access to users’ private keys (essentially their wallets). What was BTC-e’s role in this hack? It helped launder the stolen funds.

BTC-e was also connected to Liberty Reserve, another bitcoin exchange platform that was shut down for laundering $6 billion in illicit funds. BTC-e and Liberty Reserve had a special relationship which resulted in their creation of a program for their shared customers, most of whom were criminals. After Liberty Reserve was shutdown, BTC-e failed to disclose its relationship and took on many of Liberty Reserve’s former customers, including drug traffickers, arms dealers and child pornographers.

BTC-e also emerged in the Mueller Investigations, through a Russian cyber-espionage group called “Fancy Bear.” Fancy Bear, also known as APT-28, and believed to be behind the DNC hack, is a group linked to Russian Intelligence. It used BTC-e as an intermediary to move funds.

BTC-e has now been shut down, and its operators have either fled to Russia, or in the case of Alexander Vinnik, remain in detention in Greece. It remains to be seen whether he will be extradited to the US, France or Russia.
Arrests & Indictments

21-count indictment against BTC-e and Alexander Vinnik for:

- Failure to register as an MSB,
- Failure to Establish AML programs and procedures,
- Failure to file SARs
The current global regulatory environment allows for multiple loopholes that terrorists can exploit to raise, move and send money. Multiple terrorist groups have already used cryptocurrency to solicit donations from supporters. Mechanisms presently available to track terrorist use of cryptocurrency, especially on obfuscated blockchains, are limited. Anonymous and decentralized exchanges allow their users to trade currency with a high degree of anonymity. Even public cryptocurrency ledgers like Bitcoin are susceptible to terrorist activity when used with anonymity applications like Dark Wallet, which allows users to mask their identity on the blockchain by using one time cryptographically generated addresses to mask transactions. Dark Wallet also serves as an encrypted peer-to-peer exchange environment, where users can mix tainted and clean coins among themselves.

Regulation of cryptocurrency ATMs is also inconsistent from country to country. While some countries require valid ID to be presented for use, others have no such requirement, or the appropriate hardware to allow for KYC/AML upgrades.

Although terrorist use of cryptocurrency has been relatively limited, they have proven to show that they can be innovative. Both the Islamic State and Hamas have used one-time wallet address generators and, terrorist groups can continue to exploit regulatory loopholes until they are closed.

It will be imperative for countries to adopt regulations and legislation in line with FATF’s new Travel Rule. Even more important will be the enforcement of said regulations. Sanctions, seizure of domains, arrests, cyber operations and military operations are all methods of enforcement that will be available to the U.S. government. It is also important that the government work with the private sector to ensure that their approach is comprehensive and effective.
Generates an entirely new wallet address every time the URL is refreshed.

Used by Hamas' Izz ad-Din al-Qassam Brigades

ENFORCEMENT

- New legislation & regulations?

- Sanctioning uncooperative exchanges and actors?

- Cyber strikes! US military cyber forces went after ISIS with Operation Glowing Symphony, which disrupted communications, seized and destroyed mounds of data, some of which was financial in nature.
North Korean Cryptocurrency Scams

How the Kim regime made millions (?) riding the 2018 cryptocurrency wave

In 2018, North Korea's incessant pursuit of hard currency led the Hermit Kingdom into the uncharted waters of cryptocurrency scamming. Sam Whitefield (MIIS 2020) explains the mechanics of two of these moneymaking schemes: a "Staking Scam" involving Stellar/Interstellar/HOLD/HUZU coin, and a more straightforward fraudulent investment scam called Marine Chain Token.

Stages of a Staking Scam

Announce new coin

Hold locked presale

Take money and run

Attempt to generate interest

Announcements should be made on forums, social media, talk rooms

Also should include incentives like airdrops and bounties to generate excitement and buzz

Sell coins that can't be traded (yet)

Make it so that only certain wallets (yours) are able to trade for a time

Can be legitimate: prevents stampede price movements

Cell: 818 - 312 - 2992 Em ail: Sam.Whitefield@gmail.com