STATEMENT

OF

STEPHANIE DOBITSCH
DEPUTY UNDER SECRETARY FOR
INTELLIGENCE ENTERPRISE OPERATIONS

OFFICE OF INTELLIGENCE AND ANALYSIS
DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON INTELLIGENCE AND COUNTERTERRORISM

Thursday, July 22, 2021
310 Cannon House Office Building

Chairwoman Slotkin, Ranking Member Pfluger, and distinguished Members of the Subcommittee on Intelligence & Counterterrorism. Thank you for the opportunity to appear before you today to discuss threats from terrorist use of cryptocurrencies. It is an honor to be here representing the Department of Homeland Security's (DHS) Office of Intelligence and Analysis (I&A), and the dedicated intelligence professionals that keep the Homeland safe, secure, and resilient.

Terrorist Use of Cryptocurrency

As we have learned in our fight against terrorism, terrorists are highly adaptive and have proven successful in exploiting new and emerging technologies to plan attacks against U.S. interests and the Homeland. While some of those technologies, such as drones and 3D printing, pose direct harm, it is often access to sources of funding that are difficult to trace or attribute that allow terrorist groups even greater means to conduct a broad range of operations against the United States. Additionally, as governments and the global financial industry devote more resources to restricting terrorist use of traditional banking systems, the relative ease and anonymity of cryptocurrencies are helping to offset these restrictions, including for other malicious actors seeking to do harm to the United States.

Since at least 2015, we have observed terrorists experimenting with cryptocurrencies to obfuscate their financial activities, procure materials, and solicit donations for their operations. These activities have spanned the spectrum of terrorist ideologies—from racially or ethnically motivated violent extremists (RMVEs), to groups like the Islamic State of Iraq and ash-Sham (ISIS), al-Qaeda, and HAMAS. Using cryptocurrencies may be attractive to terrorists and supporters of violent extremism because they appear to offer a level of anonymity and less government oversight.

We have seen ISIS supporters around the world requesting donations in cryptocurrency and they may have used the donated cryptocurrency to purchase website domains in 2015 and 2018. Since at least 2018, other individuals who support violent extremism abroad, as well as individuals who support RMVE ideologies, have solicited multiple types of cryptocurrency from online donors via social media. Also, receiving payments through cryptocurrency has risen in popularity, especially among Racially or Ethnically Motivated Violent Extremists (RMVE). For example, in March, the FBI arrested a RMVE on a weapons charge who sold merchandise via social media platforms and accepted payment in a variety of ways, including cryptocurrency. Additionally, in June a pro-Al-Qaeda media group overseas offered a reward of one Bitcoin—which was worth around $60,000 at the time—to the first person to kill a police officer in a Western country in response to the announcement.

To date, we are not aware of any specific cases where Domestic Violent Extremists (DVEs) or Homegrown Violent Extremists (HVEs) in the Homeland have leveraged cryptocurrency to directly fund an attack. A review of DVE and HVE violence in the United States reveals that most attacks involved simple, easy to acquire weapons that were personally financed.

There are a handful of examples of DVEs abroad utilizing cryptocurrency to facilitate violence, including a RMVE in Germany who attacked a synagogue in 2019 and received financial support for attack preparation from an unknown individual via cryptocurrency. Additionally, a RMVE attacked a mosque in Christchurch, New Zealand, and claimed in his manifesto to have made money dealing in cryptocurrency, however investigators assess he did not make significant profits. Regardless of what we have witnessed in the United States to date, we know that terrorists historically are adaptive and often seek to embrace new technologies, and activities overseas can often foreshadow developments domestically.

In addition to concerns about terrorists using existing cryptocurrency, we are also concerned about the speed and complexity in which cryptocurrencies develop and advance to improve the user experience, including increased privacy measures, which challenges our collective abilities in the U.S. government to identify and mitigate malicious use of this technology. Bitcoin is the market leader of cryptocurrencies and, unsurprisingly, it is also the most popular cryptocurrency for criminal and terrorist use. However, newer and less popular cryptocurrencies, known as "privacy coins," are increasingly attractive to malicious actors because they include even more stringent privacy and security features. We already know that terrorists affiliated with ISIS, RMVEs, and other violent extremists are using these privacy coins to conduct financial activities while obfuscating their identies.

Finally, it is important to keep in mind that the vast majority of terrorist financing occurs through methods other than cryptocurrency, and most cryptocurrency is used legitimately. But cryptocurrency has some appealing attributes that have already been exploited by terrorists, and we anticipate violent extremists will continue to use this tool to facilitate their terrorist activities, especially as the technology becomes easier to access and more widespread in use in general commerce and the commercial sector. As these technologies become increasingly ubiquitous, the opportunity for malicious actors to exploit them will grow.

I&A Efforts

I&A's mandate and core mission is to provide our state, local, tribal, territorial, and private sector partners with the intelligence and information necessary to secure the Homeland. This includes establishing and running analytic seminars on the illicit use of cryptocurrency and the dark web to inform our partners on the illicit use of the dark web, blockchain technology, major cryptocurrencies used, how criminals are using cryptocurrencies to launder money and make illegal transactions, and key tools and best practices that analysts can leverage in Dark Web and cryptocurrency investigations. And I want to underscore that I&A is committed to strengthening our efforts to identify and communicate threats from foreign and domestic terrorists, including their plans and intentions to exploit emerging technologies such as cryptocurrency through a number of recently published pieces of classified and unclassified analytic production. I&A is also working to support our colleagues across DHS and the Intelligence Community through sharing and analyzing cryptocurrency data to enhance our understanding of the threat across the national security and law enforcement landscape. As with any threat to the Homeland, we are committed to ensuring policymakers and operational decisionmakers have the most robust understanding of the threat that the Intelligence Community can provide.

Conclusion

Thank you again for the opportunity to appear before you today to discuss this critical threat and for your continued support for I&A. We remain committed to keeping the Homeland safe, secure, and resilient by safeguarding the Nation from terrorist, criminal, and other threat actors; protecting the physical and digital borders of the United States from Transnational Criminal Organizations and terrorist networks seeking to exploit and undermine our financial and cyber systems; and we will continue our efforts at home and abroad to uphold the national security and public safety of the United States.