Strategy Session on Non-Kinetic Counterterrorism Tools: Statement for the Record

Paul Ahern
Principal Deputy Assistant Secretary, Office of Terrorist Financing and Financial Crimes, Treasury Department

November 8, 2021

Thanks for the opportunity to join you all and discuss countering the financing of terrorism (CFT). Over the past two decades, Treasury and its interagency partners have recognized a simple truth—that targeting terrorist financing is key to starving terrorism—and developed deep CFT expertise, put in place a robust legal architecture, built international relationships, and drawn upon various authorities in an extensive CFT toolkit, to degrade the financial and support networks of ISIS, Al-Qaida (AQ), Hizballah, and other terrorist groups.

We have built a clear international consensus, enshrined in numerous United Nations Security Council Resolutions and the Financial Action Task Force (FATF) international standards, that countries around the world cannot sit by and let violent extremists plan, finance, and train for attacks that will be carried out elsewhere, but must act as responsible global citizens to stop that threat. We have also empowered our partners in government, the private sector, and throughout the world, with the tools and information to join us in identifying and disrupting the flow of funds that help facilitate these destructive acts.

Let me give you an example of how Treasury's Office of Terrorism and Financial Intelligence (TFI) leverages policy, sanctions, enforcement, regulatory, and intelligence resources to disrupt terrorist financing networks. On September 29, Treasury designated two major Hizballah financiers based in the Arabian Peninsula, along with their associates, who moved tens of millions of dollars to Hizballah through the formal financial system and cash couriers. This action was the result of focused intelligence-gathering and analysis by our Office of Intelligence and Analysis to identify accounts, assets, and transactions involved in this network, followed by the development of targeted and calibrated sanctions measures by our experts at Office of Foreign Assets Control. This was not just a U.S. action; our Office of Terrorist Financing and Financial Crimes, in coordination with the State Department, worked closely with the Government of Qatar to facilitate a coordinated designation and prosecution of these individuals that magnified the impact of our own action by further disrupting the network.

While we have had success in CFT, our work is not done. The terrorism threat continues to evolve and so we must evolve our efforts to meet this challenge.

Domestic Terrorism: While our CFT efforts have primarily been focused overseas, combating domestic terrorism is a priority for the Biden Administration, as articulated in the National Strategy for Countering Domestic Terrorism released earlier this year. We are applying lessons learned from our experience with international terrorism to this evolving challenge, while respecting the vital constitutional protections for all Americans. Primarily led by the Financial Crimes Enforcement Network, TFI works closely with U.S. law enforcement

and engages with financial institutions to help them better detect and report suspicious financial activity. We also collaborate with our State Department colleagues to assess whether foreign organizations and individuals linked to domestic terrorist activities can be designated, such as the April 2020 designation of the Russian Imperial Movement, while engaging with foreign governments to identify and disrupt foreign individuals or entities sending money to, training, or recruiting U.S. persons. At the FATF, we co-led the first comprehensive assessment of how racially or ethnically motivated violent extremists (REMVEs) raise, move, and use funds.

Misuse of Digital Currency: Over the past few years, one of the priorities for Treasury has been identifying and assessing the illicit finance risks associated with digital currency and taking measures to mitigate those risks. We are particularly concerned with encrypted person-to-person transfers that don't require a traditional financial institution intermediary, and the money laundering and terrorist financing risk associated with these types of transactions. While most terrorist groups still primarily rely on the unregulated financial system and cash to transfer funds, within the past two years we have identified several instances of terrorists and their supporters, to include from ISIS, AQ, Hizballah, and REMVE groups, raising funds in digital currency—an indication that these groups are growing more comfortable with using virtual assets in financing their violent purposes.

Barriers to Public Sector Information Sharing: While public-private partnerships have grown over the last two decades, effective and timely information sharing between key government agencies involved in counter-terrorism, with other governments, and with financial institutions remains a significant challenge for many jurisdictions around the world. Financial transactions such as transfers, purchases, and cash withdrawals leave a financial footprint. Sharing this valuable information aids in detecting individuals participating in or supporting terrorist acts and facilitates disruptive action, such as freezing assets and accounts or arresting and prosecuting suspects to prevent future attacks from occurring.

Lack of Effective Implementation: For many countries, having FATF-compliant laws is seen as sufficient to stop terrorist financing. That's not enough, and we need jurisdictions around the world to build a framework that uses these authorities and resources to actually disrupt and dismantle terrorist financial networks. This means, for example, that suspicious transaction reports related to terrorism are not simply filed with the national Financial Intelligence Unit; this information must reach agencies who take action against terrorist financiers. When it comes to financial sanctions, jurisdictions can do much more on actually implementing these powerful tools to target terrorist financial and support networks.

I know Chandana is going to talk about the Administration's focus on anti-corruption, but I did want to say a few words on that. Corruption and money laundering are inextricably linked, and so the response to corruption must also go hand-in-hand with efforts to combat money laundering and terrorist finance.

At Treasury, Secretary Yellen has made implementation of anti-money laundering reforms among her highest priorities, seeking to expeditiously advance policy and regulation that will directly and rapidly counter corruption around the world. Treasury is committed to advancing a number of anti-corruption priorities, namely combating kleptocracy and foreign bribery, enhancing the transparency of legal entity beneficial ownership and real estate ownership, and promoting the role of civil society in the fight against corruption.

While corruption and terrorism present distinct foreign policy and national security challenges, I did want to note an important parallel in countering financial activity associated with each. Foremost, these efforts rest on a bedrock of financial transparency through which Treasury, regulators, and law enforcement can identify the ultimate owners of assets and the trail of transactions and financial networks that support an array of illicit actors. In analyzing this information, we can seize and freeze hidden assets, impose financial sanctions or pursue law enforcement responses, take regulatory action to close loopholes that are being exploited, and share targeted information with financial institutions and foreign governments so they can act or feed back into the information cycle to better detect and report on proceeds associated with corruption, terrorist financing, and the entire scope of illicit activity. So with that, I look forward to the discussion and your questions.