COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

Hearing Statement of Intelligence & Counterterrorism Subcommittee Chairwoman Elissa Slotkin (D-MI)

Terrorism and Digital Financing: How Technology is Changing the Threat

July 22, 2021

Over the past several months, the abuse of digital finance platforms and technologies has jumped into public view, as a result of the burst of ransomware attacks that have struck at the heart of day-to-day life in America — from pipelines and meat processing plants, to schools and hospitals. Last month, I held an event in my district with the Secretary of Agriculture that was focused on family farms — just days after a ransomware attack on the world's largest meat processor. And in a room full of Michigan farmers, the first question was about cryptocurrency — asking what our government can do to track and recover digital payments of ransoms to these criminal groups.

Now, let's be clear: there's nothing inherently illicit or illegal about cryptocurrencies or other digital finance technologies, which are used by millions of law-abiding people every day. Nor is there anything inherently suspect about using technologies that aim to protect the privacy of users. But it's our responsibility on this Committee to also understand how these tools could enable malicious activity, that threatens our homeland security — whether that's a ransomware attack, like the one I discussed with those farmers, or our topic today: funding for terrorism. Detecting and preventing terrorist funding — at home, and abroad — has long been a cat and mouse game for federal investigators and the Intelligence Community.

Just like cyber criminals, terrorists consistently seek legal loopholes, illegal pathways, and new technologies to stay one step ahead of governments — especially when it comes to funding their operations. As a former CIA analyst, I know this is far from a new challenge — we've been tracking terrorist financing for decades — and I know firsthand how difficult it can be. While technology has changed, today's terrorist and extremist groups benefit from using many of the same tools that so many of us rely on for our daily, honest activities — just as they exploited commonly-used financial systems, in the past. Some of these online platforms and online technologies allow easy access for thousands—if not millions—of users to donate money through online campaigns. For example, crowdfunding through PayPal, GoFundMe, and Amazon became a popular way in recent years for extremist groups to raise money. To put this into context, according to the Global Project Against Hate and Extremism, from about 2005-2015, just about every extremist group they tracked featured a PayPal button on their website.

Now, even though PayPal and other payment processing platforms became aware of the issue and began to ban extremists from such platforms — at first glance, a promising first step — extremist and terrorist groups have persevered and maintained an online presence. For example, ISIS supporters have recently used Instagram to solicit donations for ISIS-affiliated women being detained in Syria, via PayPal fundraising links. Beyond social media platforms, new financial technologies like cryptocurrencies — which are decentralized, largely anonymous forms of digital money — have enabled terrorists to further expand and disguise their funding efforts.

As these technologies become more and more widely used, we've seen a number of incidents just in the past year that highlight the need for the federal government to understand these technologies, the degree to which they pose a threat, and their impact on terrorist financing. In August 2020, the Justice Department "dismantle[ed] three terrorist financing cyber-enabled campaigns" involving Foreign Terrorist Organizations (FTOs)—ISIS, Hamas' military wing, and al-Qaeda—resulting in the government's largest-ever seizure of cryptocurrency from terrorist organizations. The seizure involved "millions of dollars" spanning 300 cryptocurrency accounts, four websites, and four Facebook pages — underscoring how various digital technologies could be used to help foster fundraising efforts.

Just as nefarious groups changed fundraising tactics after crackdowns by payment processors like PayPal, when law enforcement began following and cracking down on illicit Bitcoin use, terrorist fundraisers advised supporters to use other cryptocurrencies, to avoid detection. This was the case with a pro-ISIS website that requested that its supporters send money via Monero, another cryptocurrency, instead of Bitcoin, because of its privacy and safety features. Properly understanding and effectively combating this threat will require close partnerships between all levels of government, the private sector, and our allies—a task the Department of Homeland Security is well positioned to lead.

Today, I'm hoping our witnesses can help us understand the actual scope and scale of this challenge:

- How much money are we talking about?
- How does it compare to terrorist financing as a whole, or the total amount of cryptocurrency transactions?
- Who's taking advantage of it: domestic or foreign groups?

I'm also interested in understanding how the intelligence and law enforcement approach to illicit digital financing compares to your historical work on terrorist funding, and the steps you're taking to combat it. It's clear that our law enforcement and intelligence community face an uphill battle in understanding and tackling this threat — as the examples I've outlined show, the technology is changing rapidly, as their adoption only continues to increase.

Our Subcommittee stands ready to help the Department take on this challenge, and we're pleased to welcome our witnesses today. I look forward to hearing from you about the trends the Department is currently monitoring on this issue and the novel ways it is working to counter terrorists' use of digital financing.

# # #

Media contact: Adam Comis at (202) 225-9978