CLEIMUN19

"Collaboration in a Polarized World: Hope for the Future?"

A Research Report

COMMITTEE: Economic and Environmental Committee

QUESTION OF: The Use of Cryptocurrency to Fund Cybercrime and Terrorism

AUTHOR: Jared Schlachet

Introduction and Background

In the year of 2018, Cybercrime is estimated to make 1.5 trillion US dollars. As of January 2016, the online drug trade is between 12 million and 21.1 million US dollars per month. The largest part of cybercrime is the arms trade, which is valued at between 1.7 and 3.5 billion US dollars. In 2017, there were 1,579 data breaches, which is 4 or 5 every day, and a 45% increase in the number of data breaches. Almost all of the breaches were done by paid hackers or terrorists trying to gain more money. The payment for the drugs, arms, and hackers, along with the easiest way to shift the gained funds, is through Cryptocurrencies (shortened to Crypto) such as Bitcoin, Ethereum, and Ripple. While this is a very new issue, arising only in the past 7 or so years, and thus is only 5 to 15% of the trade value compared to the in person transactions of the same goods and services, but the difficulties associated with this issue make it very important to be addressed

before it grows too big. This issue affects every nation in the world, but is especially problematic in the US, Canada, Australia, Japan, and Western Europe.

What is Cryptocurrency?

This question is vital due to the sudden explosion of Bitcoin, so Cryptocurrency is known to most people, but very few understand it. Crypto is a digital paper currency, with the first being Bitcoin in 2009, but is very different to paper currency. A crypto gets its value just like a diamond does, where the value comes from it being highly desired and being very difficult to obtain, along with a limited supply (for diamonds, a choked supply). So, the value comes from the scarcity of it and its difficulty to create/mine in the first place, which is basic supply and demand. Also, value comes from permanent and public transaction records and balances, giving people the exact knowledge of the supply and demand. On the other hand, modern currency has its value based on debt and the money being a substitute for material value, which material value comes with diamonds and crypto.

The mechanism behind Crypto is essentially a web of peers, a peer being one who owns a crypto, and every peer knows every transaction to ever occur with that crypto. When a new transaction occurs, everyone hears about it but it is not confirmed, as only miners can confirm transactions. When confirmed, that transaction is fully permanent and enters the “ledger” of all transactions to have ever occured, which is known as a blockchain. Going back to miners, for confirming the transaction, they are given the crypto, which is how the limit increases and how new crypto is added. However, for security purposes, miners must trade cpu for bitcoin, as

confirming transactions requires computers to solve intricate puzzles, with more bitcoin coming from more cpu-intensive puzzles. When a puzzle is completed, they receive a proof of work done, and get their crypto payment.

What Makes Crypto So Hard to Regulate?

The first revolutionary part of crypto is that their transactions can never be altered; they are known forever. This does make transactions trackable along with every peer knowing each other's balances, however another revolutionary part of crypto, and the biggest issue, is its anonymity. Bitcoin are sent to and received by addresses which have no connection to real people. A good analogy for this is to imagine a paper trail which clearly defines how it is all connected, but there are no details connecting the trail to anyone or anything despite this. Thus, addresses can be identified as belonging to terrorists or criminals, but the specific person is unknown. Another feature is the fact that transactions are instantaneous, due to being over the internet, so they are impossible to stop once able to be confirmed. Another feature, one realized the hard way by government agencies such as the NSA, is that they are nigh on impenetrable, as crypto is locked behind extremely well done coding, making it inefficient and pointless to crack, so hacking them is a impractical approach to find who accesses the bitcoin addresses. One advantage to crypto is that there is always a limit to the amount that exists, and the limit is always known, so transaction patterns can be quickly tracked as being suspicious due to amount and frequency compared to total crypto in existence, leading to addresses being identified as belonging to criminals and terrorists.

Where is Crypto Most Commonly Used for Cybercrime and Terrorism?

The answer is the Dark web, a specific part of the deep web that requires special software to access, and contains all of activities discussed in the Introduction and Background. The most common software by far is The Onion Router (TOR), which is what the darknet statements are based on. Due to TOR routing one's connection through a multitude of other computers, it creates anonymity that is very difficult to break due to the roundabout path used. Also, these sites are "restricted" access, as someone has to want to be on the darkweb as they download a software to do so. The preferred currencies are cryptos, for the same reasons why the dark web is used. A way to think of this is that cryptos provide financial security as the dark web provides communicative security. The dark web is a much safer route, as the surface web and social media are heavily monitored by governments, and easily connected to real people, so the things that happen on the dark web are purposely done to be out of the government's eye. For this reason, many criminals use the dark web to communicate and buy and sell goods/services (services include hacking, stealing identities, and assassinating others). As for terrorists, they use the dark web for communication as well, but also do it to spread propaganda and to recruit others. Also, terrorists use it to solicit crypto transactions, as crypto is their ideal currency, and it allows them to better protect terrorist benefactors, and also gives them an easy way to trade funds for arms, but not the legal goods like food and housing that they may need.

Past Efforts to Solve This Problem

There are no international resolutions on crypto in cybercrime and terrorism. UN action against cybercrime is by analyzing and databasing cybercrimes to learn and educate for the future, and also by educating police forces in nations worldwide and increasing transnational communication. Cyberterrorism is fought using typical counter-terrorist actions, along with asking nations to adapt laws to include online versions of the same crimes, filter the internet and the content on it, and give investigative power for cybercrime departments. However, the EU has started discussion of this specific topic, and the EU sees the key to this being tight regulation of crypto and thorough monitoring of the transactions in order to find the route it travels and potentially connect it to people. One action they are taking is changing laws so crypto-based institutions have to follow the same rules banks do, such as report suspicious transactions and keep tight records of what happens.

As for fighting the marketplaces where crypto is used, the FBI and NSA of the United States have taken down the biggest at the time in October 2013. The FBI tried every method in the book to take down the Silk Road over two years, but it did not work. The FBI has not disclosed how they took down the Silk Road, but evidence points to the FBI hacking servers and having them disclose their locations, some being in Latvia and Romania, and having the police seize these servers. This is the most difficult part due to the impenetrable encryption on the servers, so it is considered unbelievable that they cracked the coding. As for finding its creator, they found old blog posts that used the same email he used for Silk Road, and were able to track his internet usage, and found his most common access point to be in a library in San Francisco. Then, the FBI did a sting and created a ploy to arrest him with his computer logged on, so they

could download the hard drive. Thus, the FBI had a wealth of information, which allowed them to arrest a multitude of other criminals. So, the key to taking down dark web marketplaces is by finding a way to find the servers and get the information from them, which is "easiest" by hacking them.

Possible Solutions

As there are no treaties on this topic, delegates can proceed on the topic as they wish. There are two ways to address this issue, directly focusing on the cryptocurrencies, or indirectly by focusing on dark web marketplaces and the medium by which the bitcoin travels to get to criminals and terrorists, or both. Either way, this topic very quickly turns into an issue of sovereignty or personal privacy. For example, in the Silk Road takedown, the FBI had to hack the creator's servers to find information, and then copied his personal computer's hard drive to find information and arrest more criminals, both of which are violations of one's personal privacy. Based on the difficulties of the Silk Road, finding an easier way to gain information on transactions and the marketplaces is a major focus of this issue that needs to be addressed. Another thing that should be addressed is that the dark web is not just marketplaces, but also chat rooms for dissidents and a place for journalists to communicate with sources. These things may want to be stopped by some governments, despite their right to free speech and free press, so these people should be protected under any resolution if the dark web approach is used, as whatever is done may completely destroy the benefits of the dark web along with the detriments.

Works Cited

Mills, Brad, et al. “What Is Cryptocurrency: Everything You Need To Know [Ultimate Guide].” *Blockgeeks*, Blockgeeks, 1 Jan. 1968, blockgeeks.com/guides/what-is-cryptocurrency/.

Weimann, Gabriel. “Going Darker: Challenge of Dark Net Terrorism.” *Scribd*, Scribd, 2018, www.scribd.com/document/380971367/Going-Darker-Challenge-of-Dark-Net-Terrorism.

“'Much Work to Do and No Time to Waste' in Cybercrime Fight, Says UN Chief | UN News.” *United Nations*, United Nations, 14 May 2018, news.un.org/en/story/2018/05/1009692.

Al-Muthir, Taqi'ul-Deen. “Bitcoin and the Charity of Violent Physical Struggle.” *Bitcoin and the Charity of Violent Physical Struggle*, krypt3ia.files.wordpress.com/2014/07/btcedit-21.pdf.

Keatinge, Tom, et al. “Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses.” *Study for the TERR Committee*, European Union, May 2018,

www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf.

"2017 Data Breaches." *Identity Theft Resource Center*, James Https://Www.idtheftcenter.org/Wp-Content/Uploads/2018/06/32smWideLogo_edited-1-300x71.Png, 2018, www.idtheftcenter.org/2017-data-breaches/.

"The Use of the Internet for Terrorist Purposes." *United Nations Office on Drugs and Crime*, UN, Sept. 2012, www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.

Hoorens, Stijn, et al. "Online Drugs Trade Growing but Still Dwarfed by Traditional Markets." *RAND Corporation*, RAND Corporation, 8 Aug. 2016, www.rand.org/randeurope/research/projects/online-drugs-trade-trafficking.html.

McCarthy, Niall, and Felix Richter. "Infographic: Where Guns Are Sold Through The Darknet." *Statista*, Statista, 23 Mar. 2018, www.statista.com/chart/13327/where-guns-are-sold-through-the-darknet/.