Cryptocurrency and National Security

Carolyn Alfieri

Abstract

The article takes cryptocurrency as an example of how criminals and terrorist groups seek to weaken national security. The decentralized nature of virtual currency along with the lack of regulations foster clandestine operations and illegal activities. Illegal business on dark net marketplaces as well as money laundering can thus be conducted far from law enforcement. Cryptocurrency also serve terrorism financing with the examples of Hamas, al-Qaeda, and ISIS. After analyzing US policy on the matter, this article offers recommendations. Adapting legislation to technological developments appears essential to take back control of cyberspace.

Keywords: Cryptocurrency, National Security, Cyberspace, Financial Crime, Terrorism

Las criptomonedas y la seguridad nacional

Resumen

El artículo toma las criptomonedas como ejemplo de cómo los delincuentes y grupos terroristas buscan debilitar la seguridad nacional. La naturaleza descentralizada de la moneda virtual, junto con la falta de regulaciones, fomentan operaciones clandestinas y actividades ilegales. Los negocios ilegales en los mercados de la red oscura, así como el lavado de dinero, pueden realizarse lejos de la aplicación de la ley. Las criptomonedas también sirven para financiar el terrorismo con los ejemplos de Hamas, al-Qaeda e ISIS. Luego de analizar la política estadounidense al respecto, este artículo ofrece recomendaciones. Adaptar la legislación a los avances tecnológicos parece fundamental para recuperar el control del ciberespacio.

Palabras clave: Criptomoneda, Seguridad Nacional, Ciberespacio, Delitos Financieros, Terrorismo

doi: 10.18278/ijc.9.1.3

加密货币与国家安全

摘要

本文以加密货币为例，展示罪犯和恐怖主义集团如何试图削弱国家安全。虚拟货币的去中心化性质以及相关监管的缺乏为秘密行动和非法活动创造适宜条件。暗网上的非法交易和洗钱因此能在远离执法的情况下进行。加密货币还为哈马斯、基地组织和伊斯兰国等提供恐怖主义融资。本文分析了美国在该事务上的政策，并提供了相关建议。将法律适应于技术开发一事似乎对夺回网络空间控制权而言至关重要。

关键词：加密货币，国家安全，网络空间，金融犯罪，恐怖主义

Introduction

In recent years, cryptocurrency has emerged as a unique national security challenge with its increasing popularity and profitability around the world. Cryptocurrency attracts technological innovators and investors, as it becomes more mainstream and integrated into the legitimate economy. However, cryptocurrency also appeals to illicit actors, such as criminals and terrorist groups who seek to weaken national security and operate within cyberspace to evade law enforcement. Cryptocurrency offers these malicious groups an opportunity to generate revenue from illegal activities and fund their operations in an increasingly clandestine manner. The decentralized nature of virtual currency makes it easier for bad actors to engage in crime without the regulations or detection mechanisms of the traditional banking system. In addition, the ability to conduct financial transactions anonymously or pseudo-anonymously provide enhanced privacy to virtual illicit activities.[1] These two key factors aid criminals and terrorists in conducting illegal operations and undermining national security through the use of cryptocurrency.

The recent popularity, increasing profitability, and growing acceptance of cryptocurrency across different legitimate sectors forces policymakers to address the illegitimate uses of digital currency. This paper will analyze how cryptocurrency has a significant and growing use in different areas of crime and terrorism. By examining U.S. policy towards cryptocurrency, we can better understand how the U.S. should address digital currency as a national security concern, as well as identify challenges to implementing policy. As the threat landscape continues to evolve due to expanding technological innovations in cyberspace, cryptocurrency poses a unique national security threat because of its role in ransomware attacks, illicit activities, and terrorism financing.

Background

Cryptocurrency is a decentralized form of digital currency, meaning that no institution or organization controls or regulates it. The peer-to-peer exchanges are logged in the blockchain, which cryptocurrency expert, Dr. Diana Dolliver, referred to as the encrypted foundation where cryptocurrency exists.[2] The blockchain is a public ledger that records and maintains a history of cryptocurrency transactions. However, the publication, "Fistful of Bitcoins: Characterizing Payments Among Men with No Names," explains that while the blockchain is public, the records are based on the pseudonyms of the users.[3] Real-life identities are not necessary to conduct crypto transactions, allowing users to protect their privacy behind one, or sometimes, multiple pseudonyms with ease. The use of digital wallets also allows users to maintain their privacy, as well as their own crypto.

Digital wallets are a type of software that allows users to store their cryptocurrency. Each user has a wallet address that provides them with pseudo-anonymity.[4] The types of wallets range from hardware to mobile apps, or even a simple piece of paper with a QR code. Some of the mobile apps used to store crypto, such as Coinbase or Binance, also function as an exchange platform, which allows users to buy and sell virtual currencies.[5] As one of the most popular exchanges, Coinbase has an estimated 43 million users and traded over $455 billion dollars of volume.[6] With over 5,500 different cryptocurrencies in existence, licit users can invest in cryptocurrency as a financial asset or use it as a means to purchase legitimate commodities.

Many users choose to invest in cryptocurrency, as its profitability and value have skyrocketed despite its volatility. For example, at the end of 2017, one Bitcoin was valued at around $17,400.[7] One year later, it was worth about $3,212. In March of 2020, Bitcoin garnered attention in the financial sector as its value exceeded $57,000.[8] Months later, the cryptocurrency's value dropped to around $35,000.[9] Unlike fiat money, which is government-issued and regulated, the value of virtual currencies is not in the amount one has. Instead, the value is determined by how much consumers are willing to pay for cryptocurrency using fiat money.[10]

Cryptocurrency can also be used to purchase goods, the same way that much of society uses fiat money. Its increasing popularity appears to be leading to a more mainstream acceptance of its uses. Today, a growing number of companies are creating and improving systems to allow payments using crypto, typically Bitcoin.[11] For example, in June 2020, Mastercard announced its partnership with Bitpay, a bitcoin payment platform in creating a debit card tied to cryptocurrency that could be used at thousands of vendors around the world.[12] Mastercard explained the reasoning for this new debit card was due to the increasing interest and investments in crypto, and that in some countries, up to 20% of the population owns cryptocurrency.[13] In addition, Microsoft, AT&T, and Home Depot are

among the major companies working towards or currently implementing Bitcoin payment systems. This trend will likely continue if the popularity of cryptocurrency continues its current trajectory.

The primary properties of cryptocurrency attract both good and bad actors. Decentralized currencies are not subject to inflation, exchange rates, or international transaction fees because there is no central authority. Also, an absence of regulation means that users are not required to provide information about their identities, which is appealing to those who highly value privacy. Different types of cryptocurrencies have varying levels of anonymity. For example, the two most popular cryptocurrencies, Bitcoin and Ethereum, are nearly pseudo-anonymous.[14] According to the Council on Foreign Relations, this means that while the blockchain does not document names or real addresses, if a wallet's owner is identified, the transactions can be tied back to the user.[15] Other cryptos, such as Monero and Zcash have enhanced security to protect the privacy of users and increase anonymity. While it is not completely impossible to trace a crypto transaction to the user, these layers of privacy protection make it increasingly challenging.[16] Chainalysis's "The 2021 Crypto Crime Report" states that cryptocurrency is attractive to criminals because of its pseudo-anonymity and the ability to transfer money around the world with ease.[17] Although bad actors make up a small portion of crypto transactions, cryptocurrency plays a role in criminal activities that undermine national security.

Cryptocurrency and Ransomware

Ransomware is a type of cyberattack that allows malicious actors to encrypt data and computer systems until the victim pays the ransom for decryption. Ransomware threatens public and private networks around the world and can result in "data loss, privacy concerns, and cost billions of dollars a year," according to the U.S. Cybersecurity and Infrastructure Security Agency (CISA).[18] When ransomware first emerged, hackers would demand money via online cash payment systems. However, this placed a constraint on ransomware hackers who could only conduct these attacks in locations where the cash payment systems were available. [19] For this reason, hackers turned to cryptocurrency, as it offered a way around this limitation. CISA advises ransomware victims against paying the ransom because it funds cybercriminals and incentivizes further ransomware attacks.[20] However, the cost of the ransom is frequently less expensive than the cost of redeveloping systems and data. Therefore, malicious actors often profit off of ransomware attacks, as statistics from the past few years demonstrate.

A number of research reports examining the link between cryptocurrency and ransomware conclude that the use of crypto in this type of cyberattack is becoming more frequent. It also provides malicious actors with an opportunity to generate a significant amount of revenue. The 2018 academic article "Tracking

Ransomware End-to-End" studied the broader structure of ransomware attacks over a two-year period. It was estimated that from 2015-2017, hackers extorted over $16 million from about 20,000 ransomware victims.[21] After hackers receive payments via cryptocurrency, they were able to cash out through a crypto exchange for fiat currency. To further hide their identities, some hackers deposited their funds into "mixers," which are services that disguise the source of crypto by mixing the transaction pathways with other transactions from different origins.[22]

Chainalysis's crime report explains how ransomware had a higher growth rate in 2020 than every other category of crypto-related crime, including dark net marketplaces and scams.[23] The total amount that ransomware victims paid "increased by 311% . . . to reach nearly $350 million worth of cryptocurrency."[24] This is partially due to the COVID-19 pandemic as people around the world migrated to telework and distance learning. Ransomware attacks provide malicious actors, including state-sponsored hackers and cybercriminals, with the opportunity to generate profits through the extortion of victims for cryptocurrency.[25]

The Democratic People's Republic of Korea (DPRK) utilizes ransomware attacks and other cybercrimes as a means to steal money. The *New Yorker* article, "The Incredible Rise of North Korea's Hacking Army," explains the growing cyber threat from the isolated country. North Korea is the only nation in the world that executes hacking operations and cybercrimes for the sole purpose of earning revenue.[26] Ironically, less than 1% of North Korean citizens have access to the internet, yet the government has recruited and trained some of the best hackers in the world.[27] Kim Jong Un believes that advanced cyber capabilities are essential for a strong defense arsenal. He even stated that cyber capabilities are an "all-purpose sword that guarantees the North Korean People's Armed Forces ruthless striking capability, along with nuclear weapons and missiles."[28]

North Korea's military intelligence agency, the Reconnaissance General Bureau (RGB), is trained to conduct a variety of cybercrimes, including ransomware attacks and the theft of cryptocurrency from exchanges. In 2017, North Korean hackers carried out the WannaCry 2.0 ransomware attack that impacted 200,000 victims in 150 countries, demonstrating North Korea as a true cyber threat.[29] WannaCry 2.0 impacted several industries around the world, including Boeing, the National Health Service in Britain, and Germany's railways.[30] The hackers exploited a vulnerability in the WindowsXP operating system and demanded $300 worth of cryptocurrency to unlock the system. Overall, about $143,000 in Bitcoin was paid to the hackers.[31]

In February 2021, three North Korean hackers were indicted by the U.S. District Court in Los Angeles in connection to the WannaCry 2.0 ransomware incident. The three hackers were also indicted for a range of other cybercrimes related to cryptocurrency, such as the "creation and deployment of malicious cryptocurrency applications" and "targeting of cryptocurrency and theft of cryptocurrency"

from a number of companies.[32] Theft of crypto exchanges is the most dependable source of income for the country.[33] In 2017, the hackers stole $75 million from a Slovenian cryptocurrency company and in 2018, stole $24.9 million from an Indonesian cryptocurrency company.[34] In total, theft from crypto exchanges have earned North Korea an estimated $1.75 billion in digital currency.[35] This alone could pay for about 10% of North Korea's defense budget.[36] In addition, a United Nations report claims that the $2 billion generated from North Korea's cybercrime activities was allocated to its weapons of mass destruction program to enhance its nuclear capabilities.[37] This demonstrates how state-sponsored crypto-related crime undermines national security by worsening existing security threats. Ransomware hackers can also weaken the security of critical infrastructure.

Ransomware incidents targeting critical infrastructure have increased in recent years, however the identities and state-alliances of these hackers are often unknown. The potential for high rewards incentivizes criminals to engage in this relatively low risk illicit cyber activity. For example, in 2019 hackers locked the municipal computer systems of Lake City, Florida and demanded around $460,000 worth of Bitcoin to release them.[38] The attack, which froze the email accounts of city workers and hindered the ability for residents to pay their bills online, forced the city to send a Bitcoin payment to an anonymous wallet. This type of attack on municipalities is not uncommon. In 2019, hackers targeted the municipal computer networks of Atlanta, Baltimore, Albany, and smaller towns in Florida, Georgia, and Massachusetts.[39] Although U.S. federal agencies urge victims not to pay the ransom so as not to provide incentives for future hackers, recovery efforts frequently cost significantly more than the initial demand. In Atlanta, hackers demanded $51,000 in cryptocurrency for the decryption of its files. Although the city refused to pay the ransom, reconstruction efforts totaled an estimated $17 million.[40] Baltimore faced a similar situation when the refusal to pay a $76,000 ransom cost the city over $18 million by the end of its recovery.[41] While ransomware attacks have been on the rise, 2020 saw an especially high number of incidents partially due to the COVID-19 pandemic and the migration to telework and distance learning.

The dramatic shift in the reliance on virtual private networks and online systems left data and computer networks vulnerable to exploitation by malicious actors. According to Chainalysis, this is demonstrated in the 60% increase in the average ransom payment between the first quarter and the second quarter of 2020. During the second quarter, the average ransom payment increased from $111,605 to $178,254.[42, 43] The education and healthcare sectors were particularly vulnerable, as hackers capitalized on society's desperate reliance for school systems and healthcare facilities to operate effectively. For this reason, there was greater opportunity in these two areas for cybercriminals to maximize their revenue.

Recently, ransomware attackers have targeted other essential sectors in the U.S. In May 2021, the cybercrime group, DarkSide, executed a ransomware attack

against Colonial Pipeline, a major U.S. pipeline operator.[44] The attack shut down the company's computer systems and led to gasoline price hikes, panic buying, and fuel shortages along the East Coast.[45] To resume its stalled operations, the pipeline company paid the hackers about 75 Bitcoin, which at the time valued almost $5 million.[46] Since the attack, U.S. investigators tracked a number of electronic transactions linked to DarkSide and were able to seize around $2.3 million worth of Bitcoin from the hackers.[47] A *New York Times* article explains how the Eastern European cybercrime group has potential links to Russia, as DarkSide provides ransomware services and earn a portion of the extorted profits. [48] DarkSide's possible connection to Russia grants the Russian government "a layer of plausible deniability" regarding cyberattacks, such as the Colonial Pipeline incident, while also providing protection to cybercriminals.[49]

Weeks after the ransomware attack on Colonial Pipeline, JBS, the world's largest meat processor, was also impacted by a cyberattack, demonstrating another recent case of ransomware disrupting the supply and production chains of vital U.S. commodities.[50] The attack targeting JBS, which processes about one-fifth of the U.S.'s meat supply, forced a temporary shutdown of all nine of JBS's beef plants located in the U.S. The shutdown led to production changes for its poultry and pork plants, as well as canceled shifts for around 2,500 employees.[51] To prevent further price spikes and meat shortages, JBS paid a ransom of $11 million in Bitcoin.[52] Similar to the ransomware attack on Colonial Pipeline, there are suspicions that the unnamed cybercriminal group had connections to Russia. White House Deputy Press Secretary, Karine Jean-Pierre, stated that the ransom originated from "a criminal organization likely based in Russia."[53] These two cases show how cybercriminals with potential nation-state connections can generate cryptocurrency through extorting important U.S. industries.

The use of cryptocurrency in ransomware attacks provide state and non-state cybercriminals an additional layer of anonymity as it is extremely difficult to identify the actors and track payments. In addition to the expense of recovery efforts, cryptocurrency's role in ransomware attacks weakens the security of essential infrastructure. As COVID-19 forced large populations to work and learn from home, the education and healthcare sectors experienced tremendous stress. In addition, recent ransomware attacks demonstrate how cybercriminals are willing to disrupt the supply and production chains of vital U.S. commodities. The pressure to function efficiently and continuously makes these sectors attractive, and potentially profitable targets for ransomware attacks. The possible connections to Russia in the Colonial Pipeline and JBS ransomware attacks exemplify how a U.S. adversary can use cybercriminals to its advantage to extort critical industries for cryptocurrency and weaken U.S. security. On a larger scale, the North Korean case demonstrates how state-sponsored hackers can utilize ransomware and cryptocurrency to fund the DPRK's nuclear program. This not only severely undermines U.S. national security, but the security of nations around the world.

Cyrptocurrency and Illicit Activity

There is a considerable amount of debate surrounding the scale of cryptocurrency's involvement in criminal activity. A *New York Times* article explains that although only 1% of Bitcoin transactions is linked to crime, there are a few concerning trends.[54] First, while 1% is an extremely small portion of transactions, this is actually an increase from the previous year, indicating a growing criminal use of Bitcoin. Second, the amount of criminal activity linked to Bitcoin remains relatively unchanged by fluctuations in value.[55] This means that despite Bitcoin's volatility, criminals continue to use it. Additionally, the anonymity provided by both cryptocurrency and the dark net makes it extremely challenging to estimate how much cryptocurrency is connected to illicit activity compared to its overall usage. Criminals use crypto to their advantage in the illegal drug trade on dark net marketplaces and to launder money due to the lack of oversight and regulations. The use of cryptocurrency in various illicit activities undermines the broader threat landscape by facilitating and expanding transnational crime.

The Illegal Drug Trade

Criminal activity on the dark net is able to stay out of the public eye with unique software, such as Tor. According to Mark Goodman, Tor is the "closest thing to actual anonymity on the internet." [56] Tor reroutes web connections through thousands of computer servers to disguise the origin and destination of the web traffic, preventing anyone, including law enforcement, from tracing the web traffic back to the user.[57] Tor and other anonymizing software make it possible for criminals to access dark net marketplaces with a lesser risk of detection and identification. Similarly, when marketplaces use this software, their site is only accessible to those who also use it. The use of cryptocurrency, combined with Tor, further protects the identities of the criminals engaged in the buying and selling of illicit goods.

Dark net marketplaces, also referred to as cryptomarkets, are primary examples of the intersection between cryptocurrency and illicit activity. These illegitimate marketplaces provide an opportunity for criminals to buy and sell an extraordinary supply and range of unlawful products. Buyers can find an extremely wide variety of weapons, explosives, illegal wildlife parts, child pornography, hitmen, cybercrime products, and much more.[58] In particular, drug sales have had tremendous success on dark net marketplaces. The first major dark net marketplace, Silk Road, elevated the drug trade and the use of cryptocurrency to a higher level of transnational crime.

Silk Road was founded in 2011 by 29-year-old Ross Ulbricht, who operated under the pseudonym "Dread Pirate Roberts."[59] While the site sold almost every illicit product imaginable, it was most well-known for its sale of illegal drugs. Marijuana was the most popular drug on Silk Road, with transactions worth over $46

million.[60] Cocaine accounted for 82,582 transactions amounting to $17.4 million.[61] Heroin followed marijuana and cocaine with sales worth an estimated $8.9 million.[62] The combined sales of other popular drugs including meth, LSD, ecstasy, and narcotics, such as oxycodone and fentanyl, generated an estimated $19.2 million.

Silk Road was the largest online criminal marketplace for the two and a half years that it operated. During its lifetime, Silk Road brought in approximately 9.5 million Bitcoin in revenue.[63] The site intentionally only accepted Bitcoin as payment. The combination of Bitcoin and Tor software was purposely designed to hide the site from law enforcement and align with Ulbricht's libertarian beliefs. A Department of Justice press release states that the use of cryptocurrency "served to facilitate the illegal commerce conducted on the site, including by concealing the identities and locations of users transmitting and receiving funds through the site."[64] Ulbricht earned an estimated $13 million through the illicit sales until the FBI seized the site in 2013.[65] Ulbricht was arrested and convicted of seven offenses, including distributing narcotics by means of the Internet, engaging in a continuing criminal enterprise, and conspiring to commit money laundering. Ulbricht was sentenced to life in prison.[66] Unfortunately, Silk Road was only the beginning of the rise in dark net marketplaces.

Other dark net marketplaces quickly emerged to fill the void left by Silk Road. Silk Road 2.0 was developed about 5 weeks after Silk Road's takedown and was essentially identical to the first version. Similar to its predecessor, the site consisted overwhelmingly of drug listings. The site operated for about one year and brought in around $8 million a month in illicit sales until the FBI shut down the site.[67] While Silk Road was the first marketplace of its kind, AlphaBay surpassed Silk Road as the largest dark net marketplace for drugs. AlphaBay was about 20 times larger than Silk Road, with approximately 350,000 listings for illicit goods and services.[68] Shortly prior to its shutdown, AlphaBay had over 21,000 listings for opioids and more than 4,100 for fentanyl and similar substances.[69] Law enforcement seized AlphaBay in the summer of 2017. In the time that AlphaBay operated, the site conducted transactions worth over $1 billion in Bitcoin and other forms of digital currency.[70]

Dark net marketplaces have given users easy access to the buying and selling of unlawful products. Law enforcement has seen a significant increase in drug-related overdoses since the existence of these marketplaces. According to a *New York Times* article on the U.S. opioid crisis, the sale of drugs via the internet, including over dark net marketplaces, has greatly increased the accessibility of illegal substances, such as fentanyl and other potent synthetic opioids.[71] Not only is the increased volume of distribution a major challenge for law enforcement, but the role of cryptocurrency hinders efforts to combat the illegal drug trade. The use of cryptocurrency on these marketplaces is a tactical strategy to protect the identities of those engaged in illicit activities. Countless dark net marketplaces emerge faster

than law enforcement can shut them down. In addition, cryptocurrency's role in conducting unlawful transactions presents another significant challenge for law enforcement, as it already struggles to address criminal activity on the dark net.

Money Laundering

There are a number of instances of Silk Road users laundering hundreds of millions of dollars generated from illicit activities through cryptocurrency.[72] One example involves 60-year-old Hugh Haney. Haney was a member of a collection of drug vendors on Silk Road who engaged in the large-scale trafficking of narcotics, including OxyContin, heroin, and fentanyl.[73, 74] Silk Road's payment system functioned in a manner where each user had to have a Bitcoin account internal to the site to conduct transactions.[75] Vendors could then transfer profits from their Silk Road Bitcoin address to their personal Bitcoin address once transactions were complete. This allowed Haney to launder his illegal drug profits with cryptocurrency.

According to a Department of Justice press release, Haney transferred his Silk Road Bitcoin profits to an account with a cryptocurrency exchange.[76] Through the exchange, Haney converted the Bitcoin to cash and falsely asserted that the Bitcoin came from his own crypto mining activity. In total, Haney laundered an estimated $19 million with cryptocurrency from his Silk Road drug transactions.[77] In 2020, Haney was sentenced to three and a half years in prison for money laundering charges.[78] Cryptocurrency-based money laundering is not uncommon and criminals outside of dark net marketplaces also engage in this illicit activity.

Organized crime groups use cryptocurrency to launder their criminal profits. For example, a 2020 *Reuters* article explains how cryptocurrency-based money laundering is increasing among Latin American drug cartels. The article states that smuggling drug profits to cartels is the "only thing tougher than smuggling drugs."[79] Large amounts of cash are difficult to transport due to the weight of the bulk. It also increases the risk of detection when moving money internationally due to the regulations of financial institutions.

The head of Mexico's financial ministry's financial intelligence unit, Santiago Nieto, explained how these criminals usually deposit small amounts of illicit profits into several bank accounts to minimize the risk of raising red flags.[80] Then, they use the money in these accounts to purchase small amounts of Bitcoin. Purchasing Bitcoin makes it even more difficult to track the illicit funds while making it easier for these crime groups to send money internationally throughout their networks. According to the Drug Enforcement Administration (DEA), the number of cash seizures decreased over the past few years. In 2011, cash seizures totaled $741 million but fell to $234 million in 2018.[81] The DEA partly attributes this decrease to cryptocurrency-based money laundering. It is expected that cartels and other transnational criminal organizations will increasingly use cryptocurrency to launder illicit profits.[82]

Cryptocurrency's involvement in illicit activities, including the selling and purchasing of drugs on the dark net, and as a means to conduct money laundering, undermines national security as well as the security of communities. Modernizing the drug trade via dark net marketplaces can have devastating effects far beyond the transaction between the buyer and seller. Although the same argument could be made for drug transactions involving cash, the use of cryptocurrency on dark net marketplaces allows for the transport of significantly more volume at a much lesser risk. For example, about 20% of drug users in the U.S. purchased narcotics on Silk Road when the site was at its peak, demonstrating the prevalence of purchasing drugs via Silk Road.[83] Cryptocurrency makes it increasingly difficult for law enforcement to counter the rapid and large-scale movement of drugs, while criminals are able to expand their networks and send money internationally with ease and little risk.

Chainalysis calls money laundering the "key to cryptocurrency-based crime."[84] Cryptocurrency-based money laundering undermines national security, as it gives criminals the opportunity to generate funding, hide its sources, and operate outside of regulatory authorities. Money laundering, whether through more traditional channels or through crypto, helps keep criminals in business by ensuring financial stability and the ability to reinvest their "clean" funds to continuously expand their profits, networks, and operations. Cryptocurrency adds additional layers of anonymity to money laundering and makes it easier for criminals to hide capital around the world while evading law enforcement. Cryptocurrency-based money laundering also undermines the legitimate economy, banking systems, borders, and the rule of law. The benefits of using cryptocurrency for illicit activities, such as purchasing drugs on the dark net and money laundering, suggests that criminal groups will continue using crypto to their advantage.

Cryptocurrency and Terrorism Financing

Similarly to how cryptocurrency's anonymous and decentralized nature attracts cybercriminals, dark net drug dealers, and money launderers, crypto also appeals to terrorist groups. As the U.S. prioritized counterterrorism efforts after 9/11, revenue streams financing terrorist operations began to dissolve. As a result, terrorist groups were forced to adapt and diversify their activities by engaging in other criminal activities and soliciting donations from supporters. The article, "Illicit Trade and Terrorism," states that cryptocurrency serves as a facilitator for terrorism financing.[85] Last year, law enforcement organizations around the world detected and prosecuted a record number of cryptocurrency-related terrorism financing cases.[86] In the U.S. alone, over $1 million was recovered from Bitcoin addresses linked to terrorist groups.[87] While terrorist attacks themselves cost a relatively small amount of money, terrorist groups require a significant amount of funds for operational costs, such as recruitment, training, weapons, bribes, and payments

to families of suicide bombers.[88] Cryptocurrency provides terrorist groups a way to send and receive funds around the world quickly, often with little chance of detection. Groups engaging in crypto-related terrorism financing include Hamas's military branch, an al-Qaeda affiliate, and ISIS.[89]

Hamas's military branch, the Izz ad-Din al-Qassam Brigades (AQB) was behind "one of the largest and most sophisticated cryptocurrency-based terrorism financing campaigns ever seen," according to Chainalysis.[90] In 2019, AQB attempted to solicit donations from supporters using Bitcoin and adapted its methods each time law enforcement impeded its efforts. AQB requested donations from supporters via a QR code on the group's website that directed the user to a Bitcoin address. However, after a short time, law enforcement was able to freeze the account and investigate its owner and the account's activities. AQB adjusted and replaced the QR code Bitcoin address with one that was connected to a private wallet. Although AQB believed this private wallet increased anonymity, Chainalysis explains that analysts were able to trace the wallet's transactions and donations to the group.[91] The wallet was eventually shut down.

AQB once again changed its method of collecting Bitcoin donations. This time, the website created an individual Bitcoin address for each donor to send money.[92] The website even had an instructional video to guide donors on how to contribute while maintaining maximum anonymity. The instructions included two donation options: hawala or a private Bitcoin wallet.[93] Hawala is an informal money transfer system founded on trust.[94] If they chose this option, they could provide the Bitcoin address and the donated amount in fiat currency. The hawala would then send the fiat currency amount in Bitcoin to the address. The video also informed donors that they could create a private Bitcoin wallet, choose from a recommended crypto exchange to purchase Bitcoin, and then transfer their donation.[95] This complex system made it increasingly difficult to trace funds. AQB earned over $10,000 in donations until U.S. authorities seized the donation campaign webpage in 2020.[96] AQB not only used crypto to its advantage, but it demonstrated its ability to adapt when law enforcement impeded its efforts. ISIS and an al-Qaeda affiliate also relied on cryptocurrency schemes to generate funds.

In September 2020, 29 people were arrested by French authorities for a cryptocurrency-related terrorism financing scheme for groups in Syria, including ISIS and an al-Qaeda affiliate. The cryptocurrency scheme had been active since 2019 until French government authorities uncovered a web of financial transactions sent to French extremists in Syria.[97] The scheme involved the purchase of cryptocurrency coupons. Recipients in Syria were sent the details of the coupons and then used the details to collect money through cryptocurrency exchanges.[98] Prosecutors explained that dozens of people located in France anonymously purchased cryptocurrency coupons worth 10 to 150 euros or $11 to $165.[99] The crypto coupons were credited to accounts abroad that were opened by extremists who

could then convert the credited amount into cryptocurrency. It is believed that this scheme allowed members of ISIS and the al-Qaeda affiliate hiding in Syria to collect hundreds of thousands of euros.[100] This crypto scheme demonstrates another case where terrorists use the ease and anonymity of cryptocurrency to their advantage for the purpose of funding their extremist operations.

In addition to the two cases discussed above, there are also instances of al-Qaeda and affiliated groups laundering cryptocurrency and soliciting crypto donations through social media.[101] There was another case where a 27-year-old from Leicestershire, England, transferred Bitcoin abroad for the purpose of helping ISIS members escape from prisons controlled by the Kurds in Northern Syria.[102] ISIS also capitalized on the COVID-19 pandemic by selling counterfeit personal protective equipment (PPE) to generate revenue. A Department of Justice press release explains how Murat Cakar, an ISIS facilitator, operated the website, FaceMaskCenter.com.[103] The site claimed to have an ample supply of FDA-approved N95 respirator masks, as well as other PPE, despite shortages.[104] The scheme also involved the use of Facebook pages in order to help facilitate sales of the counterfeit products. [105] This case, along with al-Qaeda and affiliated groups soliciting cryptocurrency donations on social media platforms and the AQB donation campaign, resulted in the "largest-ever seizure of cryptocurrency" related to terrorism financing.[106] U.S. authorities seized millions of dollars and more than 300 cryptocurrency accounts, as each terrorism financing campaign made use of digital currency. In response to the seizure, Attorney General William Barr stated, "it should not surprise anyone that our enemies use modern technology, social media platforms and cryptocurrency to facilitate their evil and violent agendas."[107] Cryptocurrency not only aids in financing extremism abroad, but it is suspected of playing a role in funding a domestic extremist incident in the U.S.

On January 6, 2021, growing domestic tensions reached a boiling point when alt-right groups stormed the U.S. Capitol to protest the certification of the 2020 election results. A single Bitcoin transaction worth approximately $522,000, is under investigation by the FBI for its potential connection to the event. On December 8, 2020, the transaction transferred Bitcoin to 22 crypto addresses, many of which belong to far-right activists.[108] Chainalysis notes that the popular alt-right internet personality and podcaster, Nick Fuentes, received the largest donation of $250,000.[109] The donor was allegedly a French computer programmer who committed suicide the same day the donation was made. According to a suicide note published on his personal blog, the man seemingly committed suicide due to health issues. However, he also highlighted a number of alt-right viewpoints in his note, such as the decline of Western civilization and the hatred of Western "ancestors and heritage."[110] Given that international extremists use cryptocurrency to fund their activities, it is not impossible for domestic groups to do the same.

There is evidence that domestic extremist groups are moving towards cryptocurrency funding, as discussed in the hearing "Dollars Against Democracy: Domestic Terrorist Financing in the Aftermath of Insurrection" conducted by the Subcommittee on National Security, International Development, and Monetary Policy of the U.S. House Committee on Financial Services. Dr. Daniel Rogers, who is the co-founder and Chief Technical Officer of the Global Disinformation Index (GDI), provided a witness testimony on the use of cryptocurrency for the financing of extremist groups. Dr. Rogers explained how hate groups not only use online platforms to spread hateful ideologies, but they also use cyberspace to garner funding to support their activities.[111] GDI examined how 73 domestic groups, some of which participated in the January 6 Capitol riots, use a variety of online platforms, including five different cryptocurrencies.[112] GDI found evidence of these cryptocurrencies being used to transfer funds to groups. The organization also noticed a trend between the level of extremism of a group and their tendency to use crypto within their fundraising strategy.[113] For example. Dr. Rogers explained how groups who were less extreme relied more on traditional fundraising methods. As the groups were censored or removed from online platforms and became increasingly extreme, they would then migrate to cryptocurrency where pseudo-anonymity protected the identities of these groups.[114] This trend is likely to continue as technology companies continue to confront the issue of censoring users who spread extreme hate and toxic ideology through their online platforms.

While the true extent of cryptocurrency's role in terrorism financing is unknown, it is clear that terrorist groups have the ability to adapt and use technology to further their interests and undermine national security. The various methods these groups deployed to collect Bitcoin, whether through their websites, the use of crypto coupons, or individual donors, demonstrate a clear capacity to evolve their strategies in order to generate revenue and elude law enforcement. Crypto-related terrorism financing allows terrorists to collect money through donors and supporters with a lower risk of detection. As a result, terrorists are able to carry out operations and attacks that threaten the safety of innocent civilians around the world. Well-funded extremists perpetuate conflict and destabilize regions with their violence, putting both national and international security at significant risk. In addition, the suspected connection of Bitcoin to the January 6 Capitol riots demonstrates how crypto could help fund hostile groups within the U.S.

U.S. Cryptocurrency Policy

The decentralized nature of cryptocurrency makes it extremely difficult for policymakers to address how crypto can undermine national security. Cryptocurrency continues to become increasingly valuable and attractive faster than policy can be formulated. In addition, policymakers are faced with the challenging task of countering the national security threats of crypto while understanding that too

much regulation could eliminate the essence of cryptocurrency. In order to make policy recommendations related to crypto, it is important to first examine how the Trump administration and the Biden administration addressed or plan to address cryptocurrency and its appeal to criminals and terrorists.

The topic of cryptocurrency as a national security concern remained relatively unacknowledged throughout Trump's presidency. However, the Department of Justice published the 2020 Report of the Attorney General's Cyber Digital Task Force, which highlights a number of ways that cryptocurrency facilitates crime and undermines national security. The report states that although cryptocurrency has existed for a relatively short amount of time, "this technology already plays a role in many of the most significant criminal and national security threats our nation faces."[115] Yet policymakers faced pushback when the Trump administration proposed reporting requirements for cryptocurrency and digital assets.

A few weeks before the end of Trump's presidency, the Financial Crimes Enforcement Network (FinCEN), a bureau within the Department of Treasury, announced a proposal to counter money laundering for virtual currency transactions. FinCEN proposed that financial institutions, such as banks and money services businesses (MSBs), would be "required to submit reports, keep records, and verify the identity of customers" for transactions that surpass specific thresholds and involve convertible virtual currency.[116] According to the proposal, banks and MSBs would be required to gather information, such as the names and addresses of customers and the type and amount of virtual currency used. In addition, the proposed thresholds include any transfers exceeding $3,000 if the funds are sent to a private crypto wallet.[117] The Treasury Department stated that while it values "responsible innovation," greater transparency and closing loopholes that bad actors can exploit, is required in order to safeguard national security.[118]

Despite its seemingly appealing objective of combating financial crimes, the proposal faced significant pushback. Critics of this proposal include major financial service providers, such as Fidelity Investments, Union Square Ventures, and Coinbase.[119] Cryptocurrency users opposing this proposal pointed out that FinCEN's reporting requirements ultimately take aim at the very essence of digital currency. Both licit and illicit actors are drawn to crypto for the privacy and freedom it offers. Increased reporting requirements would largely remove what makes cryptocurrency attractive. Some critics complained that attempting to identify parties involved in transactions would be expensive and sometimes impossible.[120] Despite its short existence, there is clearly a vocal sector of advocates that wish to protect the freedom and privacy cryptocurrency offers despite its potential national security implications. While the previous administration hoped it would be able to move the proposal forward prior to the end of Trump's presidency, the fate of the proposal now rests with the Biden administration.

In January 2021, President Biden's nominee for treasury secretary, Janet

Yellen, suggested that policymakers "curtail" the use of cryptocurrencies due to its role in facilitating crime, signaling an objective to increase crypto regulations during Biden's presidency.[121] According to a May 2021 *Washington Post* article, the Biden administration is reviewing oversight gaps in cryptocurrency regulation that aid in the facilitation of illegal activity, including tax evasion and terrorism financing.[122] In addition, the Treasury Department released the American Families Plan Tax Compliance Agenda to increase tax revenue through enhanced compliance measures. This includes new reporting requirements for cryptocurrency transactions. The agenda requires businesses and crypto exchanges to report transactions with a fair market value exceeding $10,000 in an effort for businesses to provide the IRS with more information surrounding large cryptocurrency transactions.[123] Although the political future of the Tax Compliance Agenda is uncertain, there seems to be some expectation that the current administration will work towards increased cryptocurrency regulations for the purpose of countering national security threats and financial crimes. Also, as ransomware has become a central national security threat in recent months, it is likely that the Biden administration will, at the very least, be forced to address the role of cryptocurrency in ransomware attacks.

Policy Recommendations

The primary challenge surrounding cryptocurrency is deciding how policy can address the national security threat while balancing crypto's core principles of privacy and decentralization. Because cryptocurrency is used for a number of areas of crime that can undermine national security, there is no "one-size-fits-all" approach. For this reason, the following policy recommendations will be specific to the issues discussed in this paper.

The rise in ransomware over the past few years demonstrates how cryptocurrency plays a major role in the facilitation of cyberattacks and the extortion of victims. Government agencies and policymakers should increase their efforts through informational campaigns to inform citizens and public and private organizations of the risks of ransomware. These informational campaigns should include how to implement defensive measures to protect systems and networks from hackers. This is essential given the shift to virtual work and distance learning due to COVID-19. It is also imperative that government agencies and policymakers deter victims from paying the cryptocurrency ransom. Although CISA and the FBI recommend against paying the ransom, informational campaigns should highlight the potential national security implications if ransomware victims pay hackers. Not only is it important to highlight how paying ransoms can facilitate more crime, but it is essential to underscore how U.S. adversaries, such as North Korea and Russia, can use ransomware and cryptocurrency to their advantage. Russia's potential links to the Colonial Pipeline and JBS ransomware attacks demonstrate

how Russia could be willing to disrupt and extort critical U.S. industries for millions of dollars' worth of cryptocurrency. In addition, North Korea uses ransomware and cryptocurrency as a tactic to circumvent sanctions to fund its nuclear program. This information can help citizens and organizations understand how ransomware contributes to the broader national security threat landscape. It can also dissuade victims from paying the ransom, despite the higher financial cost. Educating the public on the consequences of ransomware is particularly important as the number of incidents is likely to continue increasing as cybercriminals advance their capabilities.

To address the illegal drug trade on the dark net, policymakers should focus on curbing the demand for these unlawful products. In her book *Dirty Entanglements,* Dr. Louise Shelley notes that drugs are a unique illicit commodity in the way that the addictive substances create continuous demand.[124] For this reason, the drug market itself is a major problem. According to an article from the Council on Foreign Relations, some experts believe public health policies would be an effective method to decrease demand.[125] The approach of addressing demand could help counter the drug trade in and out of cyberspace. With the use of dark net marketplaces and cryptocurrency, cyberspace in particular has significantly aided in the facilitation of the illegal drug trade. The use of cryptocurrency hides the identities of buyers and sellers and allows drugs to be sold and distributed around the world at a much faster rate. Therefore, addressing demand could help combat the illicit use of cryptocurrency as well as drug crime on dark net marketplaces.

Countering cryptocurrency-based money laundering requires building on existing anti-money laundering legislation. FinCEN's proposal to implement anti-money laundering regulations to close loopholes signifies an effort to do so. Policymakers should incentivize cryptocurrency exchanges to comply with anti-money laundering laws to minimize the number of illicit actors using cryptocurrency and their platforms. U.S. anti-money laundering policies currently require compliance from banks. However, in the last year there have been a significant number of financial institutions faced with fines for noncompliance related to anti-money laundering regulations.[126] Therefore, policymakers should identify and apply lessons learned and best practices from the lack of compliance with traditional financial institutions. By applying these lessons to increase cooperation and compliance, policymakers and exchanges can combat the activities that allow criminals to maintain their capital and evade law enforcement.

Terrorism financing is difficult to address because terrorist groups are expanding their activities to ensure diversified streams of revenue. The use of online platforms to solicit donations and generate funds in the form of cryptocurrency requires enhanced law enforcement capabilities. Greater support for law enforcement can help to identify and seize sites that are linked to terrorism financing, as well as track down facilitators. In addition, countering terrorism financing re-

quires international cooperation and coordination. As the cases in the U.S. and France demonstrated, terrorism financing activities occur around the world. One of the advantages of cryptocurrency is the ease at which terrorists can send money internationally. Therefore, international organizations and federal governments need to combine resources and capabilities to identify facilitators of crypto-related terrorism financing and thwart their efforts.

Conclusion

As technology advancements progress, criminals and terrorist groups will continue to capitalize on innovative capabilities to weaken national security. Cryptocurrency has grown tremendously since it first emerged, and it attracts both illicit and licit actors with its decentralization and near anonymity. It is important to underscore that cryptocurrency does have legitimate uses, especially as digital currency becomes more mainstream. Companies are developing and adopting cryptocurrency payment systems and investors view cryptocurrency as a highly valuable digital asset. However, its anonymity and lack of regulations leave too many opportunities for transnational criminals to evade law enforcement and undermine national security.

Cryptocurrency plays an important role in the extortion of ransomware victims, especially as the number of ransomware incidents has been on the rise in recent years. Ransomware attackers generate a significant amount of cryptocurrency revenue because it often costs victims more not to pay the ransom. These profits incentivize cybercriminals to continue extorting victims through ransomware. The use of cryptocurrency in ransomware attacks protects the hackers' identities and places law enforcement at a disadvantage. This is particularly true when hackers use mixer services to further disguise their transactions when cashing out their ransomware profits. Ransomware attacks can have serious repercussions on national security beyond the initial victims, as exemplified by the DPRK cases, the attacks against municipalities in the U.S, and the targeting of critical U.S. sectors. The use of cryptocurrency in ransomware undermines national security by anonymizing malicious actors, obfuscating the path of funds, and thus making it extremely challenging for law enforcement to identify, charge, and prosecute these cybercriminals.

Cryptocurrency combined with the emergence of dark net marketplaces gave the illegal drug trade and transnational crime the opportunity to expand. Silk Road generated millions of Bitcoin in revenue, largely due to the ease with which drugs could be purchased and distributed. Despite its takedown, Silk Road paved the way for future dark net marketplaces, as more appeared in its place. Although Silk Road was the first of its kind, AlphaBay far exceeded its predecessor's success in the illegal drug trade. The use of cryptocurrency on dark net marketplaces, such as Silk Road and AlphaBay, was an intentional design. Cryptocurrency protected

the site and hid the identities of those engaging in the buying and selling of drugs from law enforcement. Cryptocurrency and dark net marketplaces have also aided in the facilitation of harming individuals and communities through drug addiction, as the U.S. opioid epidemic demonstrates.

Cryptocurrency-based money laundering is not an uncommon occurrence. Dark net vendors and organized criminal groups participate in crypto-based money laundering to hide their profits, avoid detection, and circumvent the regulations of traditional financial institutions. Cryptocurrency-based money laundering makes it more difficult for law enforcement to track illicit proceeds, while making it easier for transnational crime groups to distribute funds throughout their international networks. As is the case with ransomware and dark net transactions, money laundering with crypto hides the identities of criminals. Cryptocurrency-based money laundering undermines national security because it allows criminals to generate funding and disguise its sources. This provides criminals with financial stability, as they are then able to reinvest laundered funds back into their criminal activities. This form of money laundering also weakens the legitimate economy, as well as international borders, the rule of law, and regulations of traditional financial institutions.

The use of cryptocurrency demonstrates how terrorist groups adopt new methods to bring in money. Crypto allows terrorist groups to send and receive funds with ease from around the world. The cases involving Hamas, an al-Qaeda affiliate and ISIS exhibit how terrorists have turned to cryptocurrency to generate revenue through donations. Each case illustrates how terrorist groups deploy various methods to garner funds. Hamas's military branch, AQB, solicited Bitcoin donations through its website, while ISIS and an al-Qaeda affiliate created a scheme involving the purchase of cryptocurrency coupons. Although it is unclear how prevalent cryptocurrency's role is in terrorism financing, it is clear that some groups are adapting to technological developments and have the ability to use it to their advantage. Terrorism financing with cryptocurrency greatly undermines national security because it allows terrorists to generate funds for their violent activities with a relatively low risk of detection. In addition, there is a possibility that cryptocurrency may have funded prominent far-right activists who participated in the January 6 Capitol riots. Cryptocurrency's role in financing both international and domestic extremism presents a major national security concern.

Developing policy to counter criminals exploiting loopholes in crypto regulation is extremely difficult. The Trump administration's proposal to implement reporting requirements and greater regulation would essentially remove the privacy and freedom that cryptocurrency has to offer. While it would potentially combat financial crimes, it would come at the cost of the digital currency's fundamental principles. Moving forward, it is unclear how the Biden administration will confront the national security concern of cryptocurrency. However, Treasury

Secretary Janet Yellen's comments seem to suggest that the administration will at least attempt to address this issue.

Policymakers face a significant challenge in addressing the national security threat of cryptocurrency. Regarding ransomware, policymakers and federal agencies should educate the public, as well as public and private organizations on the risks of ransomware, how to implement protective measures, and highlight the national security concerns of these cyberattacks. Public awareness can deter victims from paying the cryptocurrency ransom if they have a better understanding of how ransomware can greatly undermine national security. Policymakers should address the demand for illegal drugs to combat the use of dark net marketplaces and, by extension, the use of cryptocurrency in illicit trade on the dark net. Addictive substances create a continuous demand, therefore, implementing public health policies could help alleviate the drug epidemic both in and out of cyberspace. To counter cryptocurrency-based money laundering, policymakers should build on existing anti-money laundering legislation. In addition, policymakers should incentivize cryptocurrency exchanges to comply with laws and regulations. They should also examine lessons learned from the failure of traditional financial institutions to comply with anti-money laundering regulations and apply these best practices to increase effective cooperation with crypto exchanges. Lastly, combating cryptocurrency-related terrorism financing requires enhanced law enforcement support to identify and seize sites that engage in terrorism financing. International cooperation and coordination are also required as terrorism financing activities occur throughout the world. Terrorism financing activities easily cross borders and jurisdictions. For this reason, the international community needs to combine its resources to track cryptocurrency transactions and identify terrorism financiers more effectively.

Ransomware attacks, the dark net drug trade, cryptocurrency-based money laundering, and terrorism financing all undermine national security in different ways. Therefore, policymakers cannot rely on a "one-size-fits-all" approach. Instead, policies combating crypto-related crime and the threat to national security should uniquely address each issue. The uses of cryptocurrency will likely expand in the coming years, especially as it becomes increasingly mainstream. Therefore, it is imperative that policymakers urgently address how cryptocurrency can threaten national security before criminals and terrorist groups gain too much of an upper hand.

Notes

1 Sarah Durant and Mangai Natarajan, "Cryptocurrencies and Money Laundering Operations," *International and Transnational Crime and Justice* (June 2019): 74, https://doi.org/10.1017/9781108597296.012.

2 Dr. Diana Dolliver, "Cryptocurrencies and Criminal Investigations: From Transaction to Seizure" (presentation, Criminal Investigations and Network Analysis Center, DHS Centers of Excellence, March 17, 2021), https://cina.gmu.edu/event/cina-virtual-distinguished-speaker-series-diana-dolliver-cryptocurrencies-and-criminal-investigations-from-transaction-to-seizure.

3 Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage, "A Fistful of Bitcoins: Characterizing Payments Among Men with No Name," *Communications of the ACM* 59, no. 4 (April 2016): 10, EBSCO.

4 Danny Yuxing Huang, Maxwell Matthaios Aliapoulios, Vector Guo Li, Luca Invernizzi, Kylie McRoberts, Elie Bursztein, Jonathan Levin, Kirill Levchenko, Alex C. Snoeren, and Damon McCoy, "Tracking Ransomware End-to-End," *IEEE Symposium on Security and Privacy (SP)* (July 2018): 619, https://ieeexplore.ieee.org/document/8418627.

5 Dr. Diana Dolliver, "Cryptocurrencies and Criminal Investigations: From Transaction to Seizure."

6 "About Coinbase," Coinbase, accessed March 29, 2021, https://www.coinbase.com/about.

7 "Bitcoin," *CoinDesk*, accessed March 30, 2021, https://www.coindesk.com/price/bitcoin.

8 Ibid.

9 Ibid.

10 Isaac Kfir, "Cryptocurrencies, national security, and terrorism," *Comparative Strategy* 39, no. 2 (March 2020): 115, https://doi.org/10.1080/01495933.2020.1718983.

11 Jacob Bernstein, "What Can You Actually Buy With Bitcoin?" *The New York Times,* February 5, 2021, https://www.nytimes.com/2021/02/03/style/what-can-you-actually-buy-with-bitcoin.html.

12 Ibid.

13 "Mastercard Accelerates Crypto Card Partner Program, Making it Easier for Consumers to Hold and Activate Cryptocurrencies," Mastercard, July 20, 2020, https://investor.mastercard.com/investor-news/investor-news-details/2020/Mastercard-Accelerates-Crypto-Card-Partner-Program-Making-it-Easier-for-Consumers-to-Hold-and-Activate-Cryptocurrencies/default.aspx.

14 Ankit Panda, "Cryptocurrencies and National Security," Council on Foreign Relations,

February 28, 2018, https://www.cfr.org/backgrounder/cryptocurrencies-and-national-security.

15 Ibid.

16 "What is Bitcoin," *CoinDesk*, December 4, 2020, https://www.coindesk.com/learn/bitcoin-101/what-is-bitcoin.

17 Kim Grauer and Henry Updegrave, *The 2021 Crypto Crime Report* (Chainalysis, 2021), https://go.chainalysis.com/2021-Crypto-Crime-Report.html.

18 "CISA Launches Campaign to Reduce the Risk of Ransomware," Cybersecurity and Infrastructure Security Agency, January 16, 2021, https://www.cisa.gov/news/2021/01/21/cisa-launches-campaign-reduce-risk-ransomware.

19 Ibid.

20 "Reduce the Risk of Ransomware Awareness Campaign," Cybersecurity and Infrastructure Security Agency, January 2021, https://www.cisa.gov/sites/default/files/publications/Fact%20sheet_Ransomware%20Awareness%20Campaign_20210119_508.pdf.

21 Huang, Aliapoulios, Li, Invernizzi, McRoberts, Bursztein, Levin, Levchenko, Snoeren, and McCoy, "Ransomware End-to-end," 13.

22 Ibid., 2.

23 Grauer and Updegrave, *The 2021 Crypto Crime Report*, 5.

24 Grauer and Updegrave, *The 2021 Crypto Crime Report*, 6.

25 Alan Brill and Eric Thompson, "Ransomware, A Tool and Opportunity for Terrorist Financing and Cyberwarfare," *Defence Against Terrorism Review* 12, (2019): 55, EBSCO.

26 Ed Caesar, "The Incredible Rise of North Korea's Hacking Army," *The New Yorker,* April 19. 2021, https://www.newyorker.com/magazine/2021/04/26/the-incredible-rise-of-north-koreas-hacking-army.

27 Ibid.

28 Ibid.

29 Arjun Kharpal, "How to tell if you're at risk from the WannaCry ransomware and what to do if you have been attacked," *CNBC,* May 15, 2017, https://www.cnbc.com/2017/05/15/ransomware-wanncry-virus-what-to-do-to-protect.html.

30 Caesar, "The Incredible Rise of North Korea's Hacking Army."

31 Ryan Browne, "Hackers have cashed out on $143,000 of bitcoin from the massive WannaCry ransomware attack," *CNBC,* August 3, 2017, https://www.cnbc.com/2017/08/03/hackers-have-cashed-out-on-143000-of-bitcoin-from-the-massive-wannacry-rans

omware-attack.html.

32 Department of Justice Office of Public Affairs, "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe," February 17, 2021, https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and.

33 Caesar, "The Incredible Rise of North Korea's Hacking Army."

34 Department of Justice Office of Public Affairs, "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe,"

35 Caesar, "The Incredible Rise of North Korea's Hacking Army."

36 Ibid.

37 Brill and Thompson, "Ransomware, A Tool and Opportunity for Terrorist Financing and Cyberwarfare," 50.

38 Ibid., 47.

39 Antonio Villas-Boas, "A Florida city was forced to use pen and paper and pay a $500,000 ransom after hackers took control of its computers," *CNBC*, June 27, 2019, https://www.businessinsider.com/lake-city-florida-ransomware-cyberattack-hackers-bitcoin-payment-2019-6.

40 Brill and Thompson, "Ransomware, A Tool and Opportunity for Terrorist Financing and Cyberwarfare," 48.

41 Ibid.

42 Boaz Sobrado, "Bitcoin Is Aiding in the Ransomware Industry," *CoinDesk*, January 19, 2021, https://www.coindesk.com/bitcoin-is-aiding-the-ransomware-industry.

43 "Ransomware Attacks Fracture Between Enterprise and Ransomware-as-a-Service in Q2 as Demands Increase," *Coveware,* August 3, 2020, https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report#1.

44 Katie Benner and Nicole Perlroth, "U.S. Seizes Share of Ransom From Hackers in Colonial Pipeline Attack," *The New York Times,* June 7, 2021, https://www.nytimes.com/2021/06/07/us/politics/pipeline-attack.html?searchResultPosition=1.

45 Ibid.

46 Michael D. Shear, Nicole Perlroth, and Clifford Krauss, "Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers," *The New York Times,* June 7, 2021, https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html.

47 Benner and Perlroth, U.S. Seizes Share of Ransom From Hackers in Colonial Pipeline Attack."

48 Ibid.

49 Ibid.

50 Julie Creswell, Nicole Perlroth, and Noam Scheiber, "Ransomware Disrupts Meat Plants in Latest Attack on Critical U.S. Business," *The New York Times,* June 3, 2021, https://www.nytimes.com/2021/06/01/business/meat-plant-cyberattack-jbs.html.

51 Ibid.

52 Jacob Bunge, "JBS Paid $11 Million to Resolve Ransomware Attack," *The Wall Street Journal,* June 9, 2021, https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781.

53 Creswell, Perlroth, and Scheiber, "Ransomware Disrupts Meat Plants in Latest Attack on Critical U.S. Business."

54 Nathaniel Popper, "Bitcoin Has Lost Steam. But Criminals Still Love It," *The New York Times*, January 28, 2020, https://www.nytimes.com/2020/01/28/technology/bitcoin-black-market.html

55 Ibid.

56 Marc Goodman, "Inside the Digital Underground," in *Future Crimes: Everything is Connected, Everyone is Vulnerable and What We Can Do About It*, (Canada: Doubleday, 2015), chap. 11.

57 Goodman, "Inside the Digital Underground," 198.

58 Erik Silfversten, Marina Favaro, Linda Slapakova, Sascha Ishikawa, James Liu, and Adrian Salas, *Exploring the use of Zcash cryptocurrency for illicit or criminal purposes*, RR-4418-ECC (Santa Monica, CA: RAND, 2020), https://www.rand.org/pubs/research_reports/RR4418.html.

59 Goodman, "Inside the Digital Underground," 197.

60 James King, "Here's a breakdown of the $1.2 billion in Silk Road drug transactions," *Business Insider,* May 29, 2015, https://www.businessinsider.com/heres-a-breakdown-of-the-12-billion-silk-road-drug-transactions-2015-5.

61 Ibid.

62 Ibid.

63 Department of Justice U.S. Attorney's Office Southern District of New York, "U.S. Attorney Announces Arrest and Money Laundering Charges Against Dark Web Narcotics Trafficker," July 18, 2019, https://www.justice.gov/usao-sdny/pr/us-attorney-announces-arrest-and-money-laundering-charges-against-dark-web-narcotics.

64 Department of Justice U.S. Attorney's Office Southern District of New York, "Ross Ulbricht, A/K/A 'Dread Pirate Roberts,' Sentenced in Manhattan Federal Court to Life in

Prison," May 29, 2015, https://www.justice.gov/usao-sdny/pr/ross-ulbricht-aka-dread-pirate-roberts-sentenced-manhattan-federal-court-life-prison.

65 Ibid.

66 Ibid.

67 "Operator of Silk Road 2.0 Website Charged in Manhattan Federal Court," Federal Bureau of Investigation, November 6, 2014, https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/operator-of-silk-road-2.0-website-charged-in-manhattan-federal-court.

68 Louise I. Shelley, *Dark Commerce: How a New Illicit Economy is Threatening Our Future* (Princeton: Princeton University Press, 2018), 70.

69 Nathaniel Popper, "Opioid Dealers Embrace the Dark Web to Send Deadly Drugs by Mail," *The New York Times*, June 10, 2017, https://www.nytimes.com/2017/06/10/business/dealbook/opioid-dark-web-drug-overdose.html?_r=0.

70 "Darknet Takedown: Authorities Shutter Online Criminal Market AlphaBay," Federal Bureau of Investigation, July 20, 2017, https://www.fbi.gov/news/stories/alphabay-takedown.

71 Popper, "Opioid Dealers Embrace the Dark Web to Send Deadly Drugs by Mail."

72 Department of Justice, "U.S. Attorney Announces Arrest and Money Laundering Charges Against Dark Web Narcotics Trafficker."

73 Ibid.

74 Tom Huddleston Jr., "This Ohio man is accused of trying to launder $19 million of bitcoin from the dark web," *CNBC*, July 23, 2019, https://www.cnbc.com/2019/07/23/man-accused-of-laundering-millions-in-bitcoin-from-silk-road.html.

75 Department of Justice, "U.S. Attorney Announces Arrest and Money Laundering Charges Against Dark Web Narcotics Trafficker."

76 Ibid.

77 Ibid.

78 Department of Justice U.S. Attorney's Office Southern District of New York, "Dark Web Narcotics Trafficker Sentenced To 3½ Years in Prison in Connection with Laundering More Than $19 Million," February 12, 2020, https://www.justice.gov/usao-sdny/pr/dark-web-narcotics-trafficker-sentenced-3-years-prison-connection-laundering-more-19.

79 Diego Oré, "Latin American crime cartels turn to cryptocurrencies for money laundering," *Reuters,* December 8, 2020, https://www.reuters.com/article/mexico-bitcoin-insight/latin-american-crime-cartels-turn-to-cryptocurrencies-for-money-laundering-idUSKBN28I1KD.

80 Ibid.

81 Ibid.

82 Ibid.

83 Goodman, "Inside the Digital Underground," 198.

84 Grauer and Updegrave, *The 2021 Crypto Crime Report*, 9.

85 Louise I. Shelley, "Illicit Trade and Terrorism," *Perspectives on Terrorism* 14, no. 4 (August 2020): 14, JSTOR.

86 Grauer and Updegrave, *The 2021 Crypto Crime Report*, 93.

87 Ibid.

88 Louise I. Shelley, *Dirty Entanglements: Corruption, Crime, and Terrorism* (New York: Cambridge University Press, 2014), 177.

89 Grauer and Updegrave, *The 2021 Crypto Crime Report*, 94.

90 Chainalysis, "Terrorism Financing in Early Stages with Cryptocurrency But Advancing Quickly," January 17, 2020, https://blog.chainalysis.com/reports/terrorism-financing-cryptocurrency-2019.

91 Ibid.

92 Ibid.

93 Ibid.

94 Louise I. Shelley, *Dark Commerce*, 144.

95 Chainalysis, "Terrorism Financing in Early Stages with Cryptocurrency But Advancing Quickly."

96 Grauer and Updegrave, *The 2021 Crypto Crime Report*, 96.

97 "French arrest 29 in cryptocurrency scheme to finance jihadis," *AP News,* September 29, 2020, https://apnews.com/article/arrests-terrorism-archive-france-701371a367d1ae26ff057d6e3d082458.

98 Ibid.

99 Ibid.

100 Grauer and Updegrave, *The 2021 Crypto Crime Report*, 94.

101 Department of Justice Office of Public Affairs, "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns," August 13, 2020, https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns.

102 Grauer and Updegrave, *The 2021 Crypto Crime Report*, 94.

103 Department of Justice, "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns."

104 Andy Greenberg, "ISIS Allegedly Ran a COVID-19 PPE Scam Site," August 13, 2020, https://www.wired.com/story/isis-allegedly-ran-a-covid-19-ppe-scam-site/.

105 Department of Justice, "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns."

106 Ibid.

107 Ibid.

108 Grauer and Updegrave, *The 2021 Crypto Crime Report*, 101.

109 Ibid., 102.

110 Ibid., 105.

111 *Virtual Hearing – Dollars Against Democracy: Domestic Terrorist Financing in the Aftermath of Insurrection: Testimony before the Subcommittee on National Security, International Development, and Monetary Policy*, 117th Cong. (2021) (statement of Dr. Daniel Rogers, Co-Founder and Chief Technical Officer, Global Disinformation Index).

112 Ibid.

113 Ibid.

114 Ibid.

115 Department of Justice, *Report of the Attorney General's Cyber Digital Task Force: Cryptocurrency Enforcement Network* (Washington, DC: United States Department of Justice, 2020), https://www.justice.gov/archives/ag/page/file/1326061/download.

116 "The Financial Crimes Enforcement Network Proposes Rule Aimed at Closing Anti-Money Laundering Regulatory Gaps for Certain Convertible Virtual Currency and Digital Asset Transactions," U.S. Department of the Treasury, December 18, 2020, https://home.treasury.gov/news/press-releases/sm1216.

117 David Z. Morris, "Trump and Mnuchin's parting sneak attack on financial privacy," *Fortune,* January 6, 2021, https://fortune.com/2021/01/06/trump-and-mnuchins-parting-sneak-attack-on-financial-privacy/.

118 U.S. Department of the Treasury, "The Financial Crimes Enforcement Network Proposes Rule Aimed at Closing Anti-Money Laundering Regulatory Gaps for Certain Convertible Virtual Currency and Digital Asset Transactions."

119 Joe Light, "Bitcoin Storm Brewing Over Trump's Anti-Money Laundering Push," *Bloomberg*, March 5, 2021, https://finance.yahoo.com/news/bitcoin-storm-brewing-

over-trump-070000416.html.

120 Ibid.

121 Harry Robertson, "Janet Yellen suggests 'curtailing' cryptocurrencies such as Bitcoin, saying they are mainly used for illegal financing," *Business Insider*, January 20, 2021, https://markets.businessinsider.com/currencies/news/bitcoin-price-cryptocurrency-should-be-curtailed-terrorism-concerns-yellen-2021-1-1029985692.

122 Jeff Stein, "White House reviews 'gaps' in cryptocurrency rules as bitcoin swings wildly," *The Washington Post,* May 25, 2021, https://www.washingtonpost.com/us-policy/2021/05/25/biden-bitcoin-crypto-markets/.

123 Jeff Stein, "Treasury targets tax cheats, cryptocurrency in proposal it hopes will bring in $700 billion," *The Washington Post,* May 20, 2021, https://www.washingtonpost.com/us-policy/2021/05/20/biden-tax-compliance-treasury/.

124 Louise I. Shelley, *Dirty Entanglements,* 244.

125 Global Governance Monitor: Crime," Council on Foreign Relations, accessed January 24, 2021, https://www.cfr.org/global-governance-monitor/#!/crime.

126 Jaclyn Jaeger, "Fines against financial institutions hit $10.4B in 2020," *Compliance Week*, December 22, 2020, https://www.complianceweek.com/surveys-and-benchmarking/report-fines-against-financial-institutions-hit-104b-in-2020/29869.article.