Threat Financing, Financial Crimes, and Money Laundering In Latin America

Dr. Christopher L. Eddy
Senior Supervisory Intelligence Analyst,
Miami Division of the Federal Bureau of Investigation

Disclaimer: *The views and opinions expressed are solely those of the author and do not necessarily reflect those of the Latin American and Caribbean Center or Florida International University.*

Introduction

Threat finance, financial crimes, and money laundering are often interrelated and frequently used synonymously, although each has its own distinct definition, threat, and mitigation actions. This paper reviews each of these threats and outlines vulnerabilities and areas of existing and potential cooperation throughout Latin America and the United States (U.S.). The paper also reviews ongoing compliance and law enforcement efforts and emerging threat areas for policymakers, lawmakers, and law enforcement to consider.

Threats

The International Monetary Fund's (IMF) 2019 World Economic Outlook report highlighted Argentina and Venezuela as having distressed economies and projected slower growth for the entire Latin American region in 2019.[1] An April 2020 IMF report detailed a 5.2% contraction in regional GDP due to effects of the Coronavirus on worldwide economies.[2] While Latin America has long struggled with governance, corruption, and lawlessness, these economic realities increase the risk of crime in the region.

Each of the threats outlined below incorporates the use of computer systems and networks to conduct criminal activity. This is technically different from "cybercrime." Although federal and private agencies define it differently, cybercrime involves areas where the computer is the intent of the crime—intrusions, malware, ransomware, intellectual property theft, identity theft, etc. The threats below focus on the movement of illicit money by nefarious actors to hide

[1] International Monetary Fund (2019). World Economic Outlook, October 2019: Global Manufacturing Downturn, Rising Trade Barriers. October 15, 2019.
[2] International Monetary Fund (2020). World Economic Outlook, April 2020 -- Chapter 1: The Great Lockdown. April 6, 2020.

the true source or destination of the funds. The growth of anonymous apps, encryption, and peer-to-peer payment applications (i.e., Venmo, Zelle, PayPal) only complicate government efforts to deter, detect and defend against all financial crimes.

Threat Finance

Threat finance incorporates all covert efforts to "move profits of illicit acts or funds that will support illicit acts."[3] This traditionally has been defined to mean primarily terrorist activity; however, its definition includes a broader array of threats. The terrorist threat in Latin America historically focused on the Revolutionary Armed Forces of Colombia (FARC), Hizballah fundraising activity (although it has also carried out terror attacks), and, to a lesser extent, Colombia's National Liberation Army (ELN), Peru's Sendero Luminoso, and al Qaeda and Islamic State of Iraq and Levant (ISIS) sympathizers. However, in terms of illegal finance, the FARC and Hizballah have been and continue to be preeminent. While the FARC kept most of its illicit proceeds in Colombia[4], obviating the need for vast international finance networks, Hizballah relied on the drug trade and other unlawful means, legal businesses, and familial connections to raise and move money out of Colombia and other countries in Latin America. In his January 30, 2020 testimony before the 116th Congress, Admiral Craig S. Faller, Commander, U.S. Southern Command stated "Some Hezbollah supporters cache weapons and raise funds, often via charitable donations, remittances, and sometimes, through illicit means, such as drug trafficking and money laundering."[5]

[3] A Guide to Counter Threat Finance Intelligence, by Marilyn B. Peterson, 2009.
[4] Cook, Thomas R. (2011). "The Financial Arm of the FARC: A Threat Finance Perspective." Journal of Strategic Security 4, no. 1: 19-36.
[5] Faller, C. S. (2020). United States Southern Command: Posture Statement (Washington, D.C.).

The U.S. and its allies continue to push for nations to designate Hizballah as a terrorist organization. Some countries historically designated only Hizballah's military arm as terrorists, leaving its political and fundraising sections separate. However, in January 2020, Colombia and Honduras formally designated Hizballah as a terrorist organization, following Argentina's and Paraguay's earlier designations.[6]

The U.S. Department of the Treasury (DoT) and U.S. law enforcement agencies continue to see funds flow from Latin America to Hizballah-supported individuals and institutions in the Middle East. U.S. sanctions against Iran and successful operations against Iranian militias in Iraq and Syria definitely impacted Iran's ability to continue to fund Hizballah at previous levels. In March 2019, Hizballah leader Hassan Nasrallah bemoaned the organization's "financial situation and called on his supporters to increase donations, echoing his previous call for a 'jihad of money'."[7] To provide the scope of funding from Latin America to Hizballah, in 2019, the U.S. DoT designated Kassem Chams and his Chams Exchange, based in Lebanon, for money laundering on behalf of Hizballah. The threat finance network moved **tens of millions of dollars** monthly **across several Latin American countries** on behalf of Colombian narcotraffickers.[8]

In 2018, Latin American officials disrupted a long-term Hizballah fundraising and money laundering organization headed by the Barakat family. Brazil arrested Assad Ahmad Barakat, accusing him of laundering **ten million dollars** through a casino in Argentina. In addition,

[6] U.S. State Department (2020). The World Confronts Terror of Iran-backed Hizballah. January, 29, 2020.
[7] Billingslea, M. (2019). Remarks by U.S. Treasury Department Assistant Secretary on Hizballah and Iran's Illicit Networks to the Atlantic Council. September 13, 2019.
[8] U.S. Treasury Department (2019). Treasury Sanctions Lebanese Money Launderer Kassem Chams Who Moves Money on Behalf of Narcotics Trafficking Organizations and Hizballah. April 11, 2019.

Argentina froze assets related to 14 members of the Barakat family.[9] Barakat was already on the U.S. DoT's Specially Designated Nationals list.

While the FARC signed a peace treaty with Colombia late in 2016, remnants of the organization continue criminal activity, including the cultivation and trafficking of narcotics to fund illicit activity. Colombia's Prosecutor's Office determined between 1995 and 2015, the FARC reaped $6.25 billion dollars through drug trafficking, protection, extortion, kidnapping, and other criminal actions. FARC leaders "laundered their money through multiple businesses from agricultural and animal farms to small shops and billiards, including 577,000 hectares of land. It was also found that they owned properties mainly in Central America, in countries such as Panama, Cuba, and Mexico."[10]

Violence against former FARC members, frustration at the slow pace of reintegration, and FARC leader Ivan Marquez's call to return to arms could derail the treaty and increase violence and, along with it, threat finance activity. In addition, coca cultivation in Colombia remains historically high due, in part, to the Colombian government's recalcitrance to eradicate and its reliance on former guerrillas to assist in eradication efforts. In early 2020, Colombian President Iván Duque Márquez vowed to diminish the cultivation by 50% by the end of 2023 (reducing it to 2013 levels) by entering into a joint agreement with the U.S. for assistance.[11]

Following the September 11, 2001 terrorist attacks in the U.S., most nations passed legislation making terror financing a criminal act. Terror (or threat) financing "is a more complex phenomenon to identify because the funds used in the financing of terrorism can come

[9] Sales, N.A. (2019). Counterterrorism in the Western Hemisphere, Remarks to the U.S. Department of State. December 10, 2019.
[10] Latin American Post (2018). Colombia: Where is FARC's Money? October 12, 2018.
[11] U.S. White House (2020). United States and Colombian Officials Set Bilateral Agenda to Reduce Cocaine Supply. March 5, 2020.

from assets of unlawful origin, but they may also be derived from assets of legal origin that have been channeled through various operations in the legal financial system."[12] Using legal businesses and legal fund transfers makes following the money much more challenging for analysts and investigators.

The Financial Action Task Force (FATF) is an inter-governmental consortium, with over 200 nations represented, responsible for setting policy standards. It serves as the global money laundering and terrorist financing watchdog. Highlighting the regional progress made over the past several years, no country in Latin America and the Caribbean remains on the FATF list of countries with a high risk of money laundering or terrorist financing; however, Nicaragua and Panama remain as monitored jurisdictions.[13]

Financial Crimes

Financial crimes incorporate nearly every crime involving money, including fraud relating to telemarketing, identify theft, elder financial exploitation, credit cards, etc. There is no set definition of financial crime but white-collar crimes are generally considered to be a sub-set of financial crimes and normally involve higher-level frauds relating to stocks, health care, insurance, bankruptcy, banks, real estate, and corporations. Latin America has the same financial crimes as other nations; however, there are a few which stand out.

One common credit card fraud in the region, called **Compras or Carding**, involves the open advertisement and use of stolen credit cards to pay bills and purchase goods and services.

[12] Zapata Sagastume, W.; Moreno-Brid, J.C; Garry, S. (2016). Money Laundering and Financial Risk Management in Latin America, with Special Reference to Mexico. January-June 2016. http://www.izt.uam.mx/economiatyp/ojs
[13] Financial Action Task Force website (2020).

Hundreds of websites advertise significant discounts on purchases and payments. For example, a website may offer to pay a bill for a client at a discounted rate (i.e., $50 for a $100 phone bill). The criminal pockets the $50 while paying the $100 with a stolen credit card. This fraud is so prevalent, airlines have started asking for the credit card used to purchase the ticket upon check-in. The most common source of stolen credit cards is from insider theft.[14]

Figure 1: A Private Facebook Compras Group (Source: INTSIGHTS)

Illicit travel agencies are common in Latin America. They offer to plan trips at significant discounts for clients, using **stolen reward points**. These points, available on the Dark Web or through insider theft, are used to pay for the entire trip, while the "agent's fee" is taken from the funds provided by the complicit or innocent traveler. One of the reasons for the increase in stolen reward points is banks and credit card agencies are getting better at detecting fraudulent access and most individuals do not check their point balances regularly.[15] [16]

Binero fraud involves detecting the specific Bank Identification Numbers (BINs) which are not properly validated by online payment processors.[17] The BIN numbers are the 4-6 digits at

[14] INTSIGHTS (2020). The Dark Side of Latin America: Cryptocurrency, Cartels, Carding, and the Rise of Cybercrime.
[15] NBC News (2019). Hackers are Stealing Loyalty Rewards. Are Your Air Miles or Hotel Points at Risk? November 12, 2019.
[16] Trip Astute (2019). Credit Card Points Stolen? Yes, Points Theft Is on the Rise.
[17] "BINs have a purpose in limiting fraud and speeding up payments by matching transactions to an issuing institution, which receives the authorization request related to a transaction." (Threatpost.com).

the beginning of a credit card (see Figure 2). Banks don't always accept every credit card and they need to update their processors to accept some and reject others. Because of this, there are sometimes vulnerabilities on websites which accept credit cards. Once a website is discovered which will accept the four to six digits, the other numbers are fabricated and purchases are made with the invented card.[18] There are many online sources in Latin America, including Facebook, WhatsApp, and the Dark Web, which discuss methods and successful online payment processor acceptances.

Figure 2: Decoding Credit Card Numbers (Source: Merlot.org)

The Financial Action Task Force of Latin America (GAFILAT), a regional group under the international FATF umbrella, seeks to develop and implement "a comprehensive global strategy to combat money laundering and terrorist financing."[19] GAFILAT's Risk Analysis and Financial Inclusion Working Group (GTARIF) noted a number of additional financial crimes in Latin America which, in addition to aiding illicit organizations, contribute to public skepticism of established financial systems and disregard for societal norms. These crimes included drug

[18] Malware.news (2019). Fraud and Cybercrime in Latin America: An Evolving Threat Landscape. April 19, 2019.
[19] Financial Action Task Force of Latin America (GAFILAT) website (2020).

trafficking, public corruption and bribery, illegal smuggling of goods, counterfeit products, tax offenses, and pharmaceutical crimes.[20]

Most Latin American nations have Financial Intelligence Units (FIU) based on the FATF model.[21] Referred to as the Egmont Group[22], an informal network of over 160 FIUs worldwide, FIUs serve as a nation's clearinghouse for suspicious transaction reports and other pertinent information relating to terror financing and money laundering. They perform analysis and ensure reports and notifications are sent to the appropriate offices, both internal and external to that country.

Figure 3: Financial Intelligence Unit Locations (Source: EgmontGroup.org)

[20] Organization of American States (2018). Technical Assessment-Comparative Analysis of Typologies and Patterns of Money Laundering and Terrorism Financing in Three Free Trade Zones in Latin America.
[21] Ellis, R. E. (2018). Transnational Organized Crime in Latin America and the Caribbean: From Evolving Threats and Responses to Integrated, Adaptive Solutions. United States: Lexington Books.
[22] Named after the Egmont Arenberg Palace in Brussels where the group was formed in 1995.

Money Laundering

Money laundering, the act of disguising financial assets so they can be used without detection of the illegal activity which produced them, is a multi-stage process involving the placement, layering, and integration of illicit funds.[23] With new technologies, including cryptocurrencies and encryption methods, it is getting increasingly difficult to deter, detect, monitor, and prosecute these crimes. Legislation, even in the best of times and in modern nations, lags new methods by years. Money laundering only became a crime in the U.S. in 1986.[24] Despite the broad scope of money laundering activity in the U.S., since 2002, only 34 financial institutions pled guilty or reached settlements with the Department of Justice for actions involving money laundering, and some of those were for administrative issues such as the failure to file Suspicious Activity Reports or the lack of a money laundering program.[25]

While FATF, GAFILAT, and the FIUs provide awareness and recommendations on addressing these issues within Latin American nations, the sheer volume and complex schemes make money laundering very difficult to prosecute. While the FATF did not include Latin American nations on its list of high risk money laundering and terror financing countries, other institutions are less optimistic. The last publicly available U.S. International Narcotics Control Strategy Report (INCSR) from 2016 lists (Figure 4) the Latin American countries as being of Primary Concern for major money laundering (by way of comparison, there are 67 nations of Primary Concern (including Canada and the U.S.), 69 of Concern (including the Holy See), and

[23] Financial Crimes Enforcement Network (2020).
[24] The Money Laundering Control Act of 1986.
[25] ICLG.com

75 Monitored.[26] The disparity between the two reports is caused by the four year difference in report dates and different assessment methodologies.

Argentina	Belize	Bolivia	Brazil	Colombia	Costa Rica
Guatemala	Mexico	Panama	Paraguay	Uruguay	Venezuela

Figure 4: Latin American Nations of Primary Concern for Money Laundering (Source: U.S. State Department)

Figure 5 shows Latin American nations included in the 2019 Basel AML (Anti-Money Laundering) Index, published annually by the Basel Institute of Governance, which ranks nations based on 15 indicators including transparency, rule of law, corruption, and financial standards.[27] The higher the score, the lower a country ranks, indicating the country is more susceptible to money laundering. Mozambique finished last in the 2019 rankings with an overall score of 8.22. The lowest ranking Latin American nation is Paraguay with 6.74.

[26] U.S. State Department (2016). 2016 International Narcotics Control Strategy Report. March 2016.
[27] Basel Institute of Governance website (2019). August 2019.

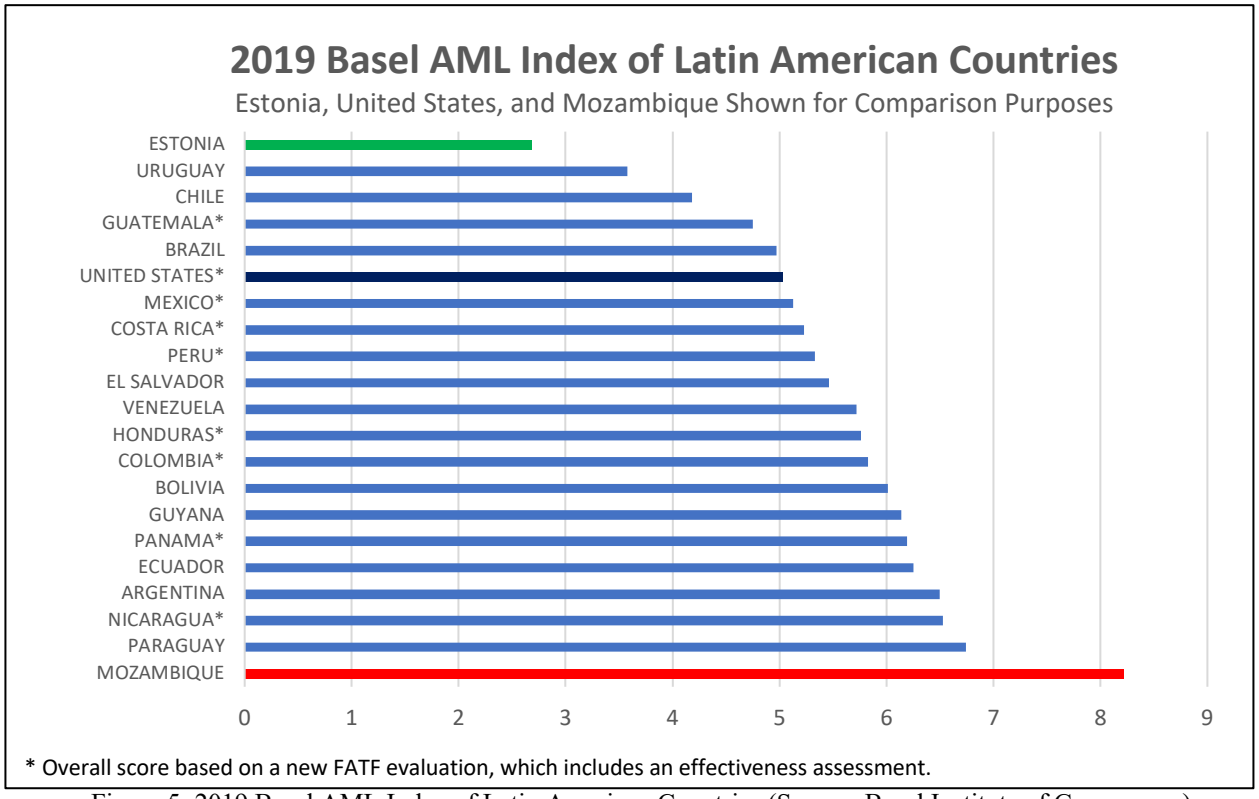

Figure 5: 2019 Basel AML Index of Latin American Countries (Source: Basel Institute of Governance)

While Colombia has been awash with drug proceeds over the last several decades, the Basel Index does not consider the *amount* laundered, only the country's structures and its ability to mitigate the risk. Other significant items from the report:

- Colombia took the biggest drop from 2018, decreasing 1.41 points, primarily due to an updated FATF evaluation completed with new methodologies.
- Uruguay finished in the top 10 for legal and institutional frameworks and the ability of its financial and economic system to mitigate money laundering risks.
- Venezuela finished last and Nicaragua finished in the bottom 10 in bribery and corruption.
- Venezuela also scored poorly (next to last) in legal and political risks.

In 2015, the Latin American GTARIF identified **narcotics trafficking as the greatest regional money laundering threat.**[28] This illegal activity also impacts ancillary crimes such as tax evasion, human and cargo smuggling, corruption, and violent activity. Cash remittances from the U.S. and other western nations remain the preeminent method for the laundering of drug proceeds, followed by bulk cash smuggling. Remittances are sent through commercial and private banks as well as money services business.

The region's over 600 free trade zones with nearly 11,000 registered companies[29] also pose another vulnerability with the one incorporating the Tri-Border Area (TBA)[30] long regarded as a haven for illicit trade. Free trade zones offer tax and other incentives to businesses and streamline local and national regulations to support economies, exports, and foreign direct investments. Hizballah financiers and sympathizers have long used the TBA as a haven to raise, launder, and transfer funds. The U.S. DoT has been focusing assets on the TBA and has had limited success in identifying and extraditing individuals linked to money laundering; however, the scope of the problem, the lack of transparency in the TBA, the complexities of the schemes, and the long-term investigative process hinder any significant impacts.

Some of the more complex money laundering schemes include:

- Illegal mining: While illegal mining has always been common in Latin America, criminals are now using the illegally extracted gold as a means to wash their illicit proceeds. Due to lax enforcement and a growing international market, this gold can be obtained,

[28] GAFILAT (2015). Analysis of Regional Threats on Money Laundering. December 2015.
[29] Asociación de Zonas Francas de las Americas (The Free Trade Zones Association of the Americas) (2020). https://www.asociacionzonasfrancas.org/en/
[30] A Free Trade Zone linking Argentina, Brazil, and Paraguay.

transported, transferred, and transformed with “little oversight, “as gold is not a financially negotiable instrument.”[31]

- Trade Based Money Laundering (TBML): The U.S. DoT reports this method as “one of the most challenging forms of money laundering to investigate because of the complexities of trade transactions and the sheer volume of international trade.”[32] TBML involves the over- or under-invoicing and/or shipment of goods and services. This could involve multiple invoicing, paying from different institutional accounts, manipulating the shipment of good, or falsifying the goods and services provided on contracts or bills of lading. U.S. law enforcement agencies believe TBML is more prevalent as a result of increased reporting of suspicious activity from the banking sector.

[31] Organization of American States (2018). Technical Assessment-Comparative Analysis of Typologies and Patterns of Money Laundering and Terrorism Financing in Three Free Trade Zones in Latin America.
[32] U.S. Government Accountability Office (2019). Countering Illicit Finance and Trade: U.S. Efforts to Combat Trade-Based Money Laundering. December 30, 2019.

- Black Market Peso Exchange: This scheme falls within TBML with drug proceeds earned in the U.S. paying for an import company's debt obligations from another country.

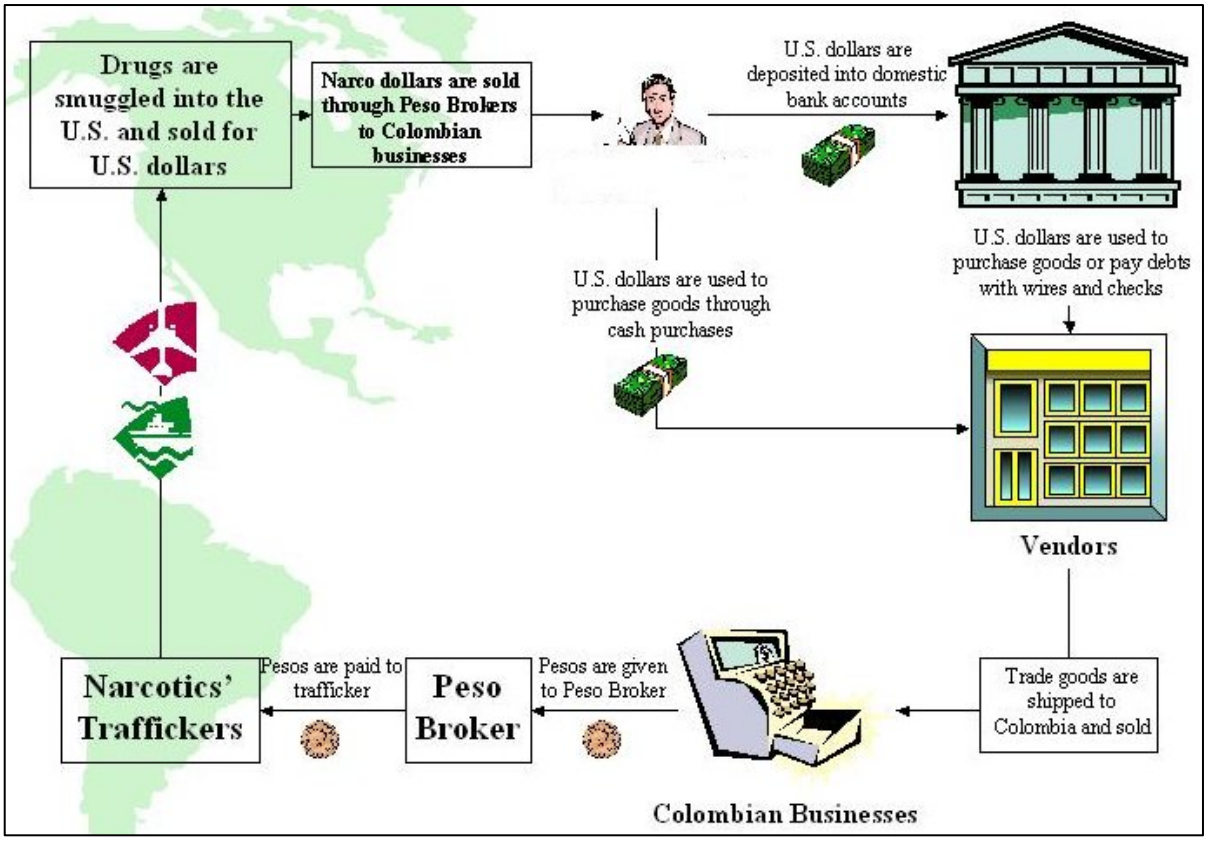

Figure 6: Black Market Peso Exchange (Source: Moneycompliance.com)

- Money Brokers: This process helps the traffickers avoid the dollar deposit restrictions in Mexican banks and assists the Chinese in the U.S. who are limited in funds they can withdraw from Chinese banks. Mexican drug cartels send cash to Chinese nationals residing in the U.S., who will then launder the money in the U.S. or send money through the Chinese banking system for eventual transfer back to Mexico.[33]

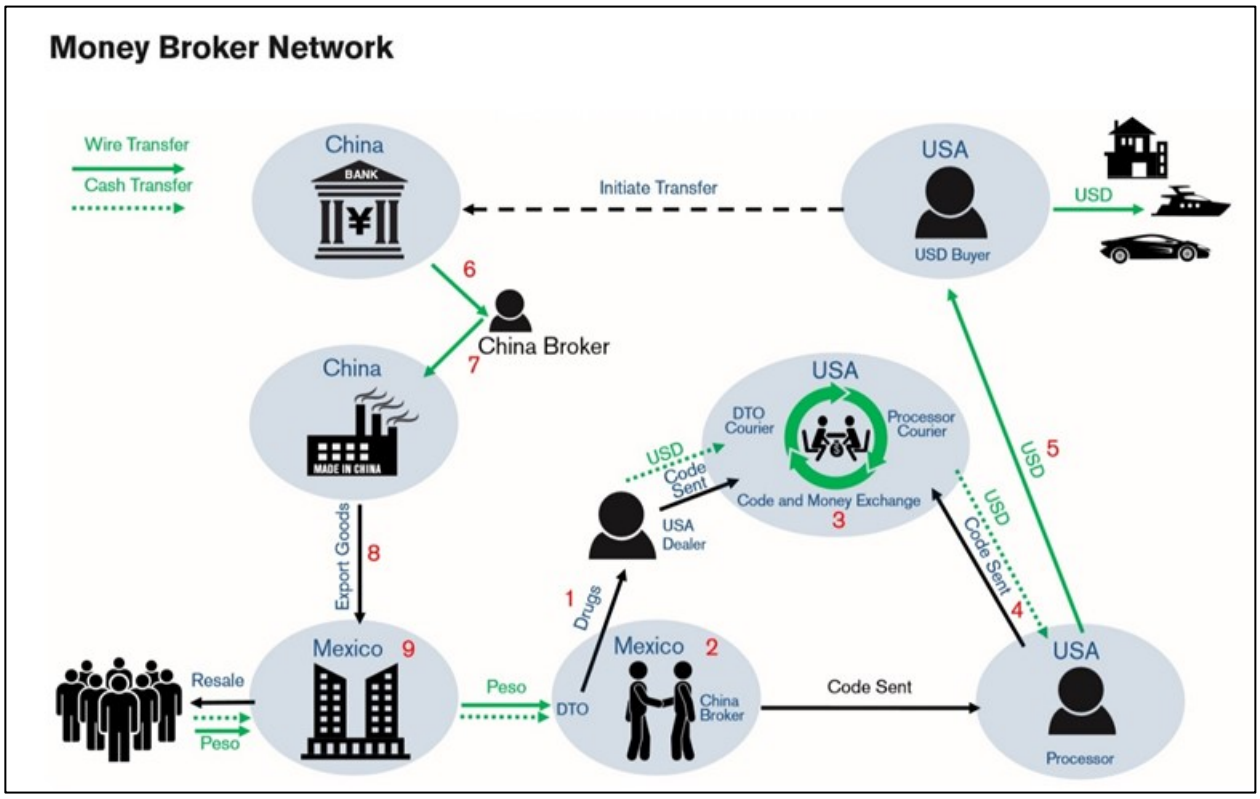

Figure 7: Mexico-U.S.-China Money Broker Network (Source: U.S. DoT National Strategy)

- Prepaid Cards: While the bulk transfer of cash has restrictions and reporting requirements, there are no such limitations regarding prepaid debit or credit cards. This scheme has been around for at least 15 years and was highlighted during the trial of

[33] RegTech Consulting LLC (2020). Chinese Money Brokers – The First US Case Involving an Identified Threat to the US Financial System? February 6, 2020.

Sinaloa leader, Joaquín Guzmán Loera (El Chapo). They are easy to smuggle and just as easy to convert back into currency at any location.

- Money Services Business (MSB): Consisting of currency dealers, remittance agencies, traveler check issuers, and check cashing operations, these organizations are legally obliged to register with the U.S. DoT. However, few actually do. This provides an opening for money launders who entice MSBs, either knowingly or unwittingly, to help launder proceeds.
- Trusts: Many jurisdictions don't require any registration for trusts, making them vulnerable to exploitation. "The use of trusts has increased in recent years, especially in jurisdictions that have virtually no identification requirements, as is the case of the Cook Islands and St. Kitts and Nevis. There have been transactions of this nature linked to corruption in some Latin American countries."[34] Money launderers create multiple shell companies and trusts which are then used to purchase insurance companies in other nations. Funds from these insurance companies are then withdrawn into other financial accounts, leaving policyholders empty handed. Money launderers are also known to purchase term life insurance policies since these are often offered through brokers who do not usually do due diligence in verifying the origination of the funds. The money launderers will then cancel the policies early, paying the early withdrawal fee.
- Shell Corporations: As seen in the 2016 Panama Papers scandal, money launderers use shell corporations in tax havens due to the lack of registration requirements and due

[34] Zapata Sagastume, W.; Moreno-Brid, J.C; Garry, S. (2016). Money Laundering and Financial Risk Management in Latin America, with Special Reference to Mexico. January-June 2016. http://www.izt.uam.mx/economiatyp/ojs

diligence. Many of these companies have unnamed owners with multiple layers of corporations and anonymity between the true owners and the funds. In February 2017, the U.S. DoT sanctioned Venezuelan Vice President, Tareck El Aissami, for his involvement in the drug trade. El Aissami created dozens of shell companies to launder money, including some based in Miami. Hizballah supporters and members of Colombian and Mexican cartels used these companies to launder money. El Aissami may have also facilitated the creation of fraudulent passports issued to 173 Middle Eastern individuals, including some connected to Hizballah.[35] A U.S. DoT study "of adjudicated IRS cases from 2016-2019 found legal entities were used in a substantial proportion of the reviewed cases to perpetrate tax evasion and fraud." With over two million corporations and limited liability companies formed in just the U.S. annually, shell companies provide a proven way to hide illicit funds.[36]

- Casinos: Casinos seem to be an obvious choice to launder money; however, many have strict currency controls. Most also provide other financial services, similar to Money Services Businesses, such as foreign exchange, check cashing, credit, and fund transfers. Online gaming is a vulnerability since those sites provide an extra layer of anonymity and are difficult for law enforcement and regulators to investigate.

GAFILAT reviewed Latin American money laundering cases from 2009-2016 and assessed the top economic activities used by money launderers in the region (see Figure 8) with banking and real estate leading the list.

[35] U.S. Senate (2019). Hearing Before the Committee on Banking, Housing, and Urban Affairs. Outside Perspectives on The Collection of Beneficial Ownership Information. June 20, 2019.
[36] U.S. Department of the Treasury (2020). National Strategy for Combating Terrorism and Other Illicit Financing.

Economic Activity/Sector	# of Cases Where It Is Present	% of Cases Where It Is Present
Banks	56	71%
Real Estate Companies	23	29%
Money Transfer Companies	14	18%
Exchanges	14	18%
Automotive Companies	13	16%
International Trade	11	14%
Notaries	7	9%
Casinos	7	9%
Financial Institutions	5	6%
Savings and Credit Cooperatives	5	6%

Figure 8: 2009-2016 Primary Economic Activities Used for Money Laundering (Source: GAFILAT)

Money laundering, threat finance, and financial crimes are quickly evolving as the use of the Internet expands in Latin America. **As of June 2019, there were over 450 million internet users in the region, a 50% increase in just six years**. Brazil leads the way with an online population of nearly 150 million people, far ahead of second place Mexico's 88 million users. In South America, 72% of the population have access while Central America shows 66% internet penetration (worldwide, approximately 59% have access; see Figure 9).

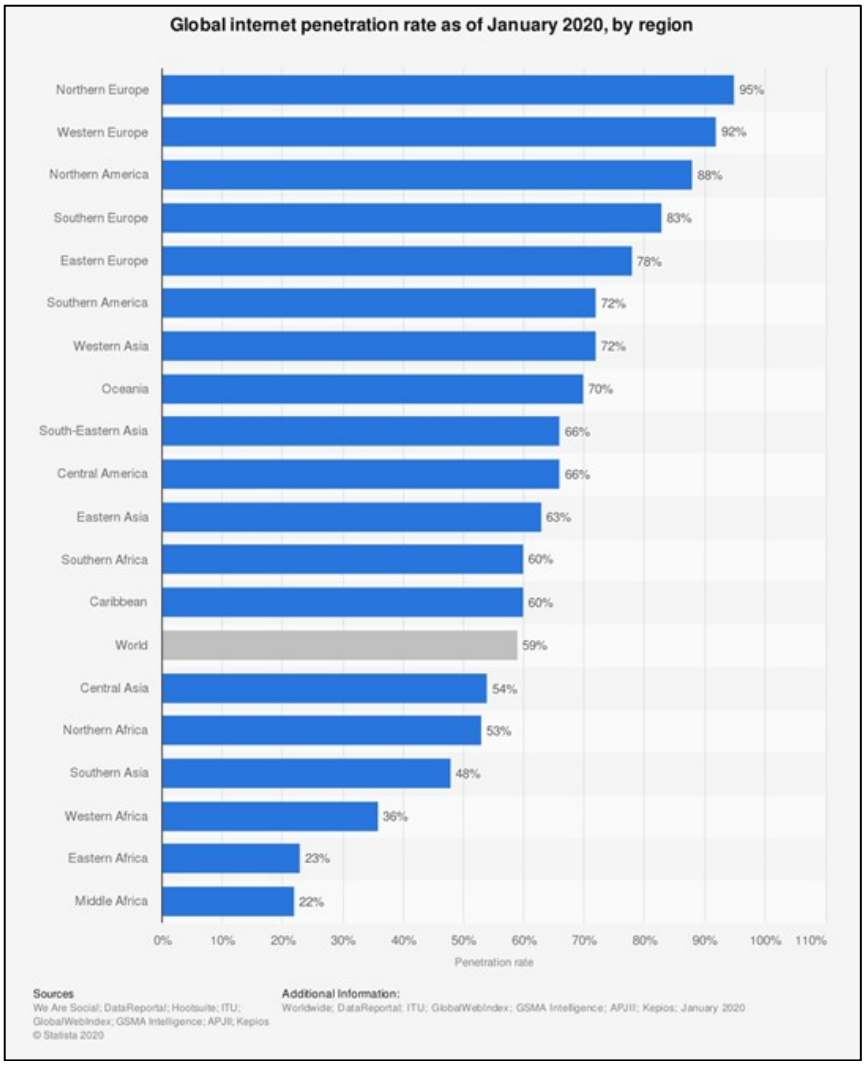

Figure 9: Global Internet Penetration (Source: Statista)

Emerging Threat: Cybercrime

The growth of the Internet increases vulnerabilities for governments and opportunities for criminals to raise and move illicit funds. Cybercrime, the use of the computer to conduct illicit activities is growing worldwide. As the Internet penetration grows in Latin America, the region's ability to protect against cybercrimes will have to improve as well. Below are current and emerging threats related to cyber activity.

- Cryptocurrencies: Organized crime and other groups attempting to launder their proceeds are turning to cryptocurrencies. While even cryptocurrency exchanges are expected to follow financial regulations such as Know Your Customer, many do not. One estimate showed after cryptocurrency was cleaned through exchanges to obscure the ownership, 97% of it ended up in countries with lax regulations and enforcement, "with Latin American economies topping the charts."[37] **Latin America leads the world in cryptocurrency users with five of the top seven spots held by regional nations.**[38]

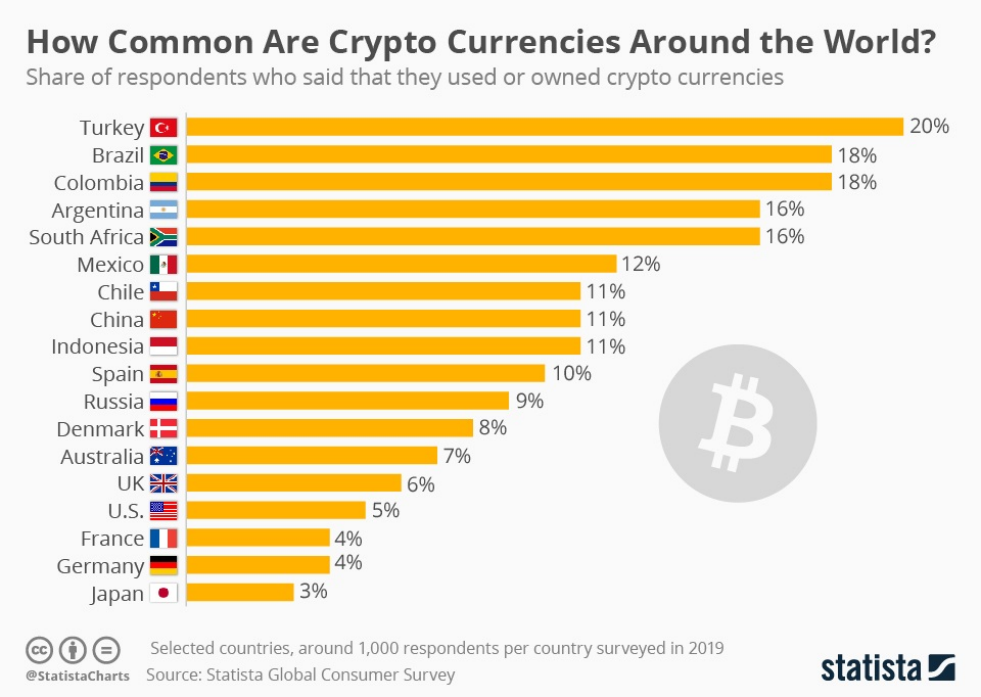

Figure 10: Cryptocurrency Usage (Source: Statista)

[37] INTSIGHTS (2020). The Dark Side of Latin America: Cryptocurrency, Cartels, Carding, and the Rise of Cybercrime.
[38] Bucholz, K. Statista (2019). How Common is Crypto? June 12, 2019.

The peer-to-peer (P2P) Bitcoin exchanges are riddled with unlicensed dealers and represent a growing challenge for law enforcement. Cryptocurrency activity using P2P exchanges exploded in Latin America since 2013. P2P platforms LocalBitcoins, Paxful, and CCoins experienced **rapid growth in volume** across many Latin American countries over the past two years, with Venezuela especially active due to its internal financial struggles.[39] [40]

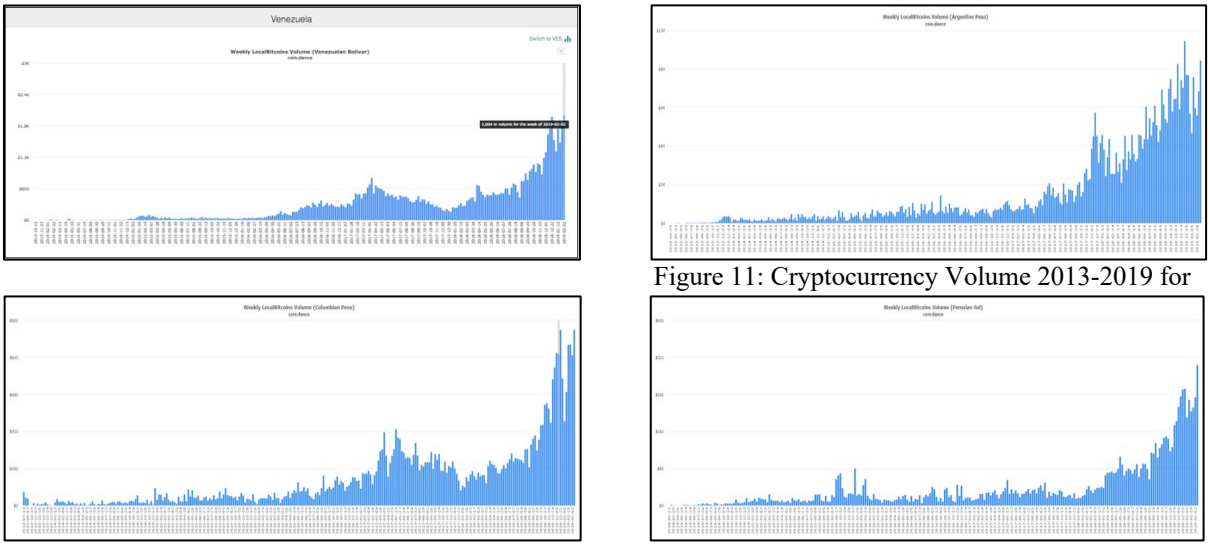

Figure 11: Cryptocurrency Volume 2013-2019 for Venezuela, Argentina, Colombia, and Peru (Source: Bitcoin.com)

- In February 2019, HAMAS received Bitcoin donations via social media, using two separate Bitcoin addresses. In just one month, HAMAS obtained over $5,000 in Bitcoin, all of it virtually untraceable due to the organization providing separate funding addresses for each donation.[41]

[39] INTSIGHTS (2020). The Dark Side of Latin America: Cryptocurrency, Cartels, Carding, and the Rise of Cybercrime.
[40] Partz, H. (2019). Bitcoin Trading Reaches All Time High in Venezuela Amidst Ongoing Economic Collapse. Cointelegraph. February 7, 2019.
[41] Mandelker, S. (2019). Remarks of Sigal Mandelker, Under Secretary for Terrorism and Financial Intelligence CoinDesk Consensus Conference. May 13, 2019.

- In April 2019, Brazil arrested an individual suspected of laundering funds for organized crime or drug traffickers by illegally operating 25 cryptocurrency mining machines.[42]
- In October 2019, the president of Panama-based payment processing firm Crypto Capital was arrested in Greece and extradited to Poland to face charges relating to the launde**ring of $350 million, allegedly on behalf of Colombian drug cartels.**[43]

- Malware/Hacking/Phishing: Like elsewhere in the world, the use of malware and trojans is increasing, both internal to Latin America and exported worldwide. Unlike Russia, China, North Korea, and Iran, the region does not contain state-sponsored advanced persistent threat (APT) groups or military-supported hacking teams. This creates an environment for other financially-motivated groups to fill the void. A 2019 study by IntSights showed very persistent regional cybercriminals "operating extensive schemes targeting banks, hospitality services, and retail businesses for their credentials and their financial assets."[44]
  - In May 2019, eight members of the Mexican Bandidos Revolution Team were arrested for hacking (and paying recruit-for-hire hackers) and using malware to infiltrate electronic interbank payment systems. Funds were withdrawn from accounts and deposited in the accounts of accomplices who were paid

[42] Thenextweb (2019). Police Bust Potential Bitcoin Money Laundering Scheme in Brazil. April 24, 2019.
[43] Krasuski, K. and Kharif, O. (2019). Crypto Capital Official Nabbed in Money Laundering Probe. Bloomberg. October 25, 2019.
[44] INTSIGHTS (2020). The Dark Side of Latin America: Cryptocurrency, Cartels, Carding, and the Rise of Cybercrime.

commissions to remove the money. Viruses were also introduced into systems that controlled ATM machines which then facilitated the illicit withdrawal of thousands of dollars. The operation netted as much as **US$5 million monthly**. One of the vehicles confiscated was a US$30 million Aston Martin.[45]

- Phishing attempts mimicking bank websites are common. In a 2019 scheme targeting North American and Latin American banks, the threat actor established several websites which looked like the real banks, purchased ad words on Google and Bing to redirect customers to those sites, and stole the account and personal information customers entered.

- Ransomware: According to Scitum, the leader in managed security in Latin America, **ransomware was at the top of the list of malware threats** targeting and emanating from the region.[46]
  - Nearly 62% of companies worldwide surveyed by Cyberedge Group experienced a ransomware attack and **Mexico led the world in penetrations with 94% of attacks successful,** followed closely by Colombia at #4 (84% successful), and Brazil at #13 (77% successful).[47] A vast majority of companies pay the ransom to regain access to their data.
  - In March 2020, Costa Rica experienced a ransomware attack called COVIDLock, which claimed to offer interactive maps of the Coronavirus infections. Other

[45] Mexican News Daily (2019). Hackers that stole hundreds of millions of pesos taken down in Guanajuato. May 17, 2019.
[46] INTSIGHTS (2020). The Dark Side of Latin America: Cryptocurrency, Cartels, Carding, and the Rise of Cybercrime.
[47] 2020 Cyberthreat Defense Report (2020). Cyberedge Group.

methods related to the pandemic soon followed, including unemployment benefits, social services, and tax payments.[48]

Cooperative Efforts

Each Latin American nation is either a member of GAFILAT or the Caribbean Financial Action Task Force (CFATF, or GAFIC in Spanish). Some also participate as direct FATF members. The region has progressed in combatting financial crimes over the previous two decades; however, emerging threats require quicker changes. While no Latin American nation remains on the FATF high risk list for money laundering or terrorist financing, most of them are either non-compliant or partially-compliant with more than 50% of FATF recommendations.[49]

Several organizations, including the Organization of American States (OAS) and the Inter-American Development Bank (IDB) assist the FIUs with anti-money laundering trainings. The amount and style of assistance differs and there is often little coordination among the agencies.[50] Through the assistance of the U.S., OAS, IDB, FATF, IMF, the World Bank, and other international institutions, most regional nations adopted legislation to match international standards for money laundering, terror financing, and other financial crimes, thus, making arrests and prosecutions easier.[51]

The U.S.' 2020 National Strategy for Combating Terrorism and Other Illicit Financing builds upon 50 years of anti-money laundering legislation and outlines national priorities using a

[48] Solano, J. (2020). CRHoy.com. Estafas estallan en medio de crisis económica por COVID-19. April 2, 2020.
[49] Zapata Sagastume, W.; Moreno-Brid, J.C; Garry, S. (2016). Money Laundering and Financial Risk Management in Latin America, with Special Reference to Mexico. January-June 2016. http://www.izt.uam.mx/economiatyp/ojs
[50] Moreno-Brid, J. (2014). Prevention of Money Laundering and of the Financing of Terrorism to Ensure the Integrity of Financial Markets in Latin America and the Caribbean. November 2014.
[51] Organization of American States (2018). Technical Assessment-Comparative Analysis of Typologies and Patterns of Money Laundering and Terrorism Financing in Three Free Trade Zones in Latin America.

whole of government approach.[52] The U.S. also continues to support the FATF organization and meaningful participation of its membership. In addition, the Department of Homeland Security's Trade Transparency Unit functions similar to the FIUs and partners with other nations, including the U.S.' largest regional trade partners, to analyze trade data, detect anomalies, and share information.

Outlook

In the short-term, cybercrime is likely to increase during the extended pandemic lockdown. With more individuals working from home and economic conditions worsening, phishing, hacking, and ransomware will become more prevalent, especially in societies with vulnerable technology. Coca cultivation may decrease in Colombia with additional eradication efforts from the government; however, overall regional cultivation will likely remain unchanged as growers shift their crops to other areas and nations to avoid detection. The FARC remains the wildcard in Colombia; it remains to be seen if a majority of its combatants will return to the battlefield and resume illicit operations. Overall, illicit financing from the drug trade is unlikely to be reduced anytime in the near future.

Regional governments will continue efforts at shoring up financial legislation, organizations, and processes but will still likely remain a step behind more nimble criminals. As technology plays more of a role in collecting, moving, and hiding illicit proceeds, governments will have to increase detection, interception, and mitigation efforts. Part of the solution may lie in artificial intelligence and data analytics to detect pattern recognition and improve risk assessments. While the FATF and other organizations provide frequent evaluations and guidance to member countries, enhanced public-private partnerships and improved information sharing

[52] U.S. Department of the Treasury (2020). National Strategy for Combating Terrorism and Other Illicit Financing.

would greatly accelerate the region's ability to effectively respond to, and potentially preempt, financial crimes.

About the Author

Dr. Christopher L. Eddy served 30+ years in leadership roles in four separate U.S. Intelligence Community agencies. He retired from the FBI as the Intelligence Program Manager of the FBI's 5th largest Field Office in Miami, where his program was ranked #1 of 56 nationwide. He also retired from the U.S. Air Force Reserves as a Brigadier General with his last assignment as the Mobilization Assistant to the Air Force's 3-star Director of Intelligence, Surveillance, and Reconnaissance at the Pentagon.

Dr. Eddy earned a Bachelor of Science in Business Administration from Ashland University (OH) in 1986, an MBA in Management from Golden Gate University in 1988, a Master of Science in International Relations from Troy University in 2004, and a PhD in Leadership and Organizational Change from Walden University in 2012. He was an FBI Certified Intelligence Officer and was inducted into the Academic Halls of Fame for Olean High School and Ashland University. He serves as a course developer and adjunct professor for colleges and universities specializing in intelligence, national security, terrorism, and foreign policy matters.

His recent book, *The Hidden Secrets of Leadership Found in Movie Quotes*, is available through Amazon.