USING INTELLIGENCE TO COMBAT TRADE-BASED MONEY LAUNDERING

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE
Financial Threats Council

April 2020

INSA FINANCIAL THREATS COUNCIL

INSA

ACKNOWLEDGEMENTS

INSA appreciates the efforts of members and staff who contributed to the development of this paper.

FINANCIAL THREATS COUNCIL

Leslie Ireland, *Financial Threats Council Chair*

Kelly Brickley, *Capital One;*
Financial Threats Council Vice Chair

Tammy Allen, *Capital One*

John Bienkowski, *Citi*

Kevin Delli-Colli, *Deloitte*

Marcy Forman, *Citi*

David Hamon, *Economic Warfare Institute*

Kristin Reif, *PMI*

David Thompson, *Thomson Reuters Special Services*

Luke Wilson, *4iQ*

INSA STAFF

Suzanne Wilson Heckenberg, *President*

Larry Hanauer, *Vice President for Policy*

Peggy O'Connor, *Director for Communications & Policy*

Caroline Henry, *Marketing & Communications Assistant*

Megan Anderson, *Intern*

EXECUTIVE SUMMARY

Trade-Based Money Laundering (TBML), the smuggling of goods and services for an illicit profit, is a poorly understood and greatly underappreciated threat to U.S. national security. It provides a means of generating income for terrorists and transnational organized criminal syndicates; it undermines U.S. foreign policy objectives by fostering the corruption of foreign officials and reductions in legitimate government revenues; it enables capital flight and erodes legitimate companies' profits and tax payments; and it undermines the integrity of product supply chains, harming both legitimate businesses and consumers. Mitigating the national security threats posed by TBML requires the U.S. government to collaborate more closely with the private sector organizations whose goods are trafficked.

The manufacturers of high-margin goods that are frequently smuggled or trafficked, such as cigarettes, alcohol, and pharmaceuticals, often have their own in-house (or contracted) intelligence gathering apparatuses to collect information on those who illicitly trade in their products. Informed by such intelligence, industry best practices on countering TBML sometimes focus on tactical threats, such as chasing individual containers full of contraband, but more often address strategic threats by identifying and exposing smuggling networks and their ways of operating. Such information is highly valued by U.S. intelligence and law enforcement agencies, which work to combat official corruption, transnational crime, terrorist financing, and other threats that undermine U.S. national security and foreign policy objectives.

However, while some business sectors, such as the financial sector, have formal structures to facilitate information sharing with the government, no formalized mechanism exists for manufacturers of commercial products to share business intelligence regarding TBML threats, actors, and activities with counterparts at federal intelligence and law enforcement agencies. As a result, companies share their TBML intelligence with government agencies only on a less effective ad hoc basis, often drawing on personal relationships rather than institutionalized procedures.

Similarly, no mechanism exists for the federal government to provide manufacturers with information that could help them prevent smuggling by nefarious actors who damage U.S. national security. This information is also shared sporadically, if at all, based on informal relationships. Federal intelligence and law enforcement agencies do not, in any case, focus collection or analysis resources on understanding TBML activities, even though they do attempt to understand and disrupt the transnational criminal and terrorist networks that use TBML techniques to raise funds.

As a member of the Financial Action Task Force (FATF), a 34-nation initiative to counter money laundering, the U.S. Treasury Department helps develop multinational policies to combat illicit financing threats that undermine the integrity of the international financial system. Although FATF has developed a TBML typology and increased awareness of vulnerabilities, none of its 40 anti-money laundering (AML) recommendations specifically address *trade-based* money laundering. A greater focus on TBML by the FATF would promote greater international engagement to counter it.

As an industry-driven association focused on promoting public-private collaboration on defense and intelligence issues, INSA frequently highlights the national security benefits of two-way information sharing between the U.S. government and private sector partners. Toward this end, INSA proposes the establishment of a TBML information fusion center, a robust information sharing exchange at which private companies, intelligence and law enforcement agencies, and non-governmental experts can share actionable information on TBML threats. INSA also recommends that the Intelligence Community (IC) enhance its collection and analysis of information on TBML from both open source and clandestine sources, and that intelligence agencies improve analyst training on TBML issues.

RECOMMENDATIONS

1. U.S. intelligence and law enforcement agencies, working with industries whose products are widely trafficked by threat actors, should establish a TBML information fusion center to enable the two-way exchange of information between government agencies and commercial companies.

2. To better combat the financing of terrorists, criminal groups, and other threat actors, the U.S. Intelligence Community should enhance its own collection and analysis of information on TBML from both open source and clandestine sources.

3. To make better sense of the ways in which threat actors generate revenue through TBML, the IC should enhance analyst training in TBML.

4. The U.S should strengthen engagement in the multilateral Financial Action Task Force (FATF) as means of promoting international solutions, training, and information-sharing mechanisms using TBML intelligence and assessments from both government and industry.

INTRODUCTION

TBML, the smuggling of goods for an illicit profit, undermines U.S. foreign policy objectives and damages U.S. national security. TBML provides a means of generating income for terrorists and transnational organized criminal syndicates; undermines U.S. foreign policy objectives by fostering the corruption of foreign officials and reductions in legitimate government revenues; enables capital flight and erodes legitimate companies' profits and tax payments; and undermines the integrity of product supply chains, which harms both legitimate businesses and their consumers.

> INSA proposes the establishment of a TBML information fusion center, a robust information sharing exchange at which private companies, intelligence and law enforcement agencies, and non-governmental experts can share actionable information on TBML threats.

Manufacturers of oft-smuggled goods – generally high-margin items like tobacco, alcohol, and pharmaceuticals – have in-house intelligence-gathering apparatuses that collect information about the corrupt actors behind the trafficking and the means by which they generate illicit profits for terrorist groups, transnational criminal networks, and corrupt government officials. However, these companies have no formalized mechanism to share such business intelligence with the U.S. intelligence and law enforcement agencies who could take steps to stop such nefarious activities. Greater public-private information-sharing on TBML would enable both government and industry to take action against those whose illicit economic pursuits undermine the stability of foreign governments and threaten U.S. interests.

HOW TBML OCCURS

Increasingly effective mechanisms to counter money laundering have hindered criminal organizations' ability to transfer money through legitimate financial institutions. As a result, many such organizations have turned to fraudulent commercial transactions to transfer value across international (or even U.S. state) borders, a practice referred to as trade-based money laundering. TBML is, in essence, the misrepresentation of the price, amount, or value of goods concealing the goods' true value, which enables the difference to be transferred across borders without payment of taxes or fees. Certain industries are at greater risk for TBML involvement, including cargo services, shipping services, and money service businesses.[1]

The scale of TBML is enormous. A 2016 Citi report asserts that trade-based money laundering amounted to $1.1 trillion in 2013.[2] Yet only a portion of these transfers are noticed by the formal banking system. A 2010 report by the Treasury Department's Financial Crimes Enforcement Network (FinCEN) noted that over a five-year period, more than 17,000 suspicious activity reports (SARs) revealed potential TBML activity totaling $276 billion – an average of $55 billion per year.[3] Clearly, individual transactions that misrepresent the true value of traded goods – concealed among more than $19 trillion in global merchandise trade[4] – are difficult to identify without good intelligence.

One of the simplest forms of TBML is under-or over-invoicing.[5] In cases of over-invoicing, a seller will invoice a buyer for a price above market value, resulting in the buyer transferring value to the seller. When parties engage in under-invoicing, the seller invoices the buyer for goods at a price below market value, effectively letting the buyer resell the goods at market value and receive an excess profit (while also avoiding taxes on the goods' true value).

TBML is frequently driven by large price differentials that exist between neighboring countries, often because of differences in state subsidies, taxes, or market prices. Most TBML activities involve imports or exports of goods across international borders. On a small scale, criminal organizations often engage in "low volume, high frequency" smuggling, in which travelers regularly transfer small amounts of goods from a zone in which prices are low to one in which prices are higher, often due to differences in taxation between two countries.[6]

At a larger scale, corrupt customs or border officials can facilitate the transfer of very large quantities of goods. They may knowingly falsify records regarding the quantity or value of goods being shipped or they may permit the transfer of containers of goods that they know to be improperly documented. Corruption even by low-level officials can erode confidence in government and facilitate the illicit shipment of large amounts of goods.

Criminal organizations and corrupt companies that abet them (often wholesalers or other middlemen[7]) often take advantage of limited government inspections and oversight in Free Trade Zones (FTZs) to modify product labels, shipping paperwork, and planned destinations of products. As the OECD report, "Criminal networks have found ways to abuse lax oversight in FTZ to smuggle or divert illicit products to the domestic market, set up production facilities for counterfeit and contraband goods, and facilitate the transit of illegal goods." Such actions in FTZs fund a veritable rogues' gallery of criminal enterprises, including trafficking in narcotics, small arms, timber, and illegal wildlife products.[8]

Criminals can also generate profits through TBML within the United States. Cigarettes purchased in a U.S. state with low taxes on tobacco products, for example, can be sold at a profit in a neighboring state with much higher taxes, generating large profits for the smuggler and tax losses for the neighboring state. The terrorist group Lebanese Hezbollah took advantage of these tax differentials by organizing an interstate cigarette smuggling ring that generated $2 million in profits – funds that supported its international operations.[9]

At senior levels of government, corrupt officials may authorize (or provide cover for) TBML activities, generating profits for themselves at the expense of their countries' rule of law. Many such officials will attempt to place their ill-gotten gains in the U.S. financial system, from which the funds can be used for a virtually infinite range of transactions in the United States and around the world. The use of U.S. financial institutions to launder gains from TBML prevents host nations from accessing ill-gotten funds and undermines confidence in the U.S. banking sector.[10]

IMPACTS OF TBML ON NATIONAL & ECONOMIC SECURITY

TBML impacts U.S. interests and national security in four principal ways:

1. **TBML funds terrorism and transnational organized crime.** Terrorist and criminal groups use the funds raised by TBML to fund recruiting, influence activities, drug smuggling, and physical attacks. In 2003, the Government Accountability Office (GAO) identified a wide range of ways in which terrorist groups use "alternative financing measures," such as cigarette smuggling and misusing charitable donations, to fund their operations.[11] Groups as varied as Lebanese Hezbollah, Hamas, Al-Qaeda, the Irish Republican Army (IRA), the Basque Fatherland and Liberty Party (ETA), and Palestinian Islamic Jihad have raised extensive amounts of money from cigarette smuggling.[12] Noting the widespread use of TBML by terrorist organizations around the world, money laundering expert John Cassara asserted in 2016 testimony to the House Financial Services Committee:

> *In discussing terror finance, TBML is also intertwined with hawala, the misuse of the Afghan transit trade, Iran and Dubai commercial connections, the tri-border region in South America, suspect international Lebanese-Hezbollah trading syndicates, non-bank lawless regimes such as those in Somalia and Libya, the ISIS regime in Syria and Iraq, and many more.*[13]

> Products greatly affected by TBML include highly taxed products (such as cigarettes, alcohol, and electronics) and products for which large price differentials exist between countries (such as pharmaceuticals and consumer goods).

Narcotics smugglers and criminal organizations also frequently invest their proceeds in products that can be exported to countries where they convert the value into cash, with significant differentials between the transactional price and the true value being used to pay bribes and fund continued operations. As just one example, in 2011, Mexican drug smugglers laundered $25 million in U.S. profits by purchasing perfume in the United States and exporting it to Mexico, where it could be sold and the proceeds could be deposited in the drug organization's accounts as "legitimate" proceeds from trade.[14]

2. **TBML contributes to official corruption, reduces government revenues, and undermines good governance in foreign countries, which often undermines U.S. foreign policy objectives.** To cite an example, the smuggling of 7.4 billion illicit cigarettes into Tunisia in 2015 resulted in a loss to the government of $391 million in tax proceeds – almost three percent of public revenues – that otherwise might have been available to provide critical services to Tunisian citizens.[15] To enhance accountable governance in Tunisia, the U.S. Agency for International Development (USAID) supports the Tunisian government's efforts to improve public financial management in tax collection and administration[16] – so the Tunisian government's failure to collect such revenues undermines what the United States is working to accomplish there. Worldwide, the State Department estimates that governments lose between $40 billion and $50 billion each year from the smuggling of cigarettes alone.[17]

   The large amounts of money involved often attract involvement by corrupt government officials at senior levels and field postings alike, undermining public confidence in government, as well as its effectiveness. Jordan's former customs director, for example, has been indicted for accepting bribes in exchange for permitting cigarette counterfeiting, an effort that helped the manufacturers evade $760 million in taxes.[18]

3. **TBML enables capital flight, which reduces funds for domestic investment and affects legitimate companies' profits and tax payments, both in the United States and overseas.** Capital flight occurs when money is rapidly drained from a country, leaving less capital behind to facilitate domestic investments and economic activity. Under-invoicing of exports – which permit the buyer to resell them abroad at a much higher profit, thereby transferring the goods' value – is a leading means of transferring value out of developing countries into developed countries, where the resulting profits can be used more flexibly.[19] Mispriced exports from developing countries into the United States and Europe deprives those economies of the benefits of domestic investment.

4. **TBML affects the financial health of a wide range of U.S. companies.** Products greatly affected by TBML include highly taxed products (such as cigarettes, alcohol, and electronics) and products for which large price differentials exist between countries (such as pharmaceuticals and consumer goods). U.S. companies in these sectors lose sales and profits due to counterfeiting and illicit transfers of goods between markets.

TBML THREATS

Three types of actors generally engage in TBML in ways that undermine U.S. national interests: transnational criminal organizations, terrorist groups, and corrupt foreign officials whose illicit activities undermine good governance in their homelands.

TRANSNATIONAL ORGANIZED CRIME

Transnational Criminal Organizations (TCOs) and Drug Trafficking Organizations (DTOs) engage in TBML to launder their illicit revenue, often by purchasing goods for export which can then be sold through legitimate-appearing businesses to generate "clean" profits.[20] The goods are typically undervalued so as to provide opportunities for brokers and other middlemen to profit as well. By providing a way for criminals to legitimize their profits, TBML helps to fuel drug smuggling, human trafficking, and many other illicit activities.

TERRORISM

Terrorist organizations exploit the same gaps and vulnerabilities in the financial systems as criminal actors to raise and launder funds in support of their activities. Terrorist organizations may engage in different criminal activities to raise money, including illegal activities like organized fraud, narcotics, counterfeiting, and cultural antiquities theft. They then leverage trade-based money laundering techniques – such as inaccurate invoicing, falsifying documents, and tax evasion – to transfer their assets in legitimate-appearing ways into countries where they plan to operate. These funds then become available to carry out operations, which include everything from recruitment and travel to the purchase of lethal equipment and the execution of deadly attacks.

CORRUPT FOREIGN OFFICIALS

Corrupt foreign officials play a major role in the smuggling of illicit goods. With their increased access to information and procedures, government officials are able to prevent the implementation of measures to deter such behaviors. According to a report by the Association of Certified Anti-Money Laundering Specialists (ACAMS), "Corruption is among the most significant contributors to proceeds of crime that become available for money laundering."[21]

In some states, such as Qaddaffi's Libya, government officials' control of regional trafficking routes and favoritism of select smuggling networks led to state control over criminal markets. The illicit income derived from public officials' collusion with smugglers facilitated bribes to more senior officials and established local power centers (particularly in border areas and port cities), thereby undermining the legitimacy and effectiveness of the government. As scholars from the U.S. Institute of Peace wrote, "The increasing fusion of crime and governance… has shown to be highly detrimental to building a stable democratic state predicated on the rule of law."[22]

PUBLIC & PRIVATE SECTOR ACTIONS TO ADDRESS TBML

The U.S. government undertakes a range of policy and enforcement measures to understand and mitigate TBML activities. Large corporations also undertake both internal management controls and international outreach to rein in TBML activities that affect their products.

U.S. GOVERNMENT

At a policy level, the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) is responsible for administering and enforcing economic and trade sanctions based on U.S. foreign policy and national security goals. OFAC has imposed sanctions against countries, specially designated foreign nationals, and other entities in an effort to mitigate TBML threats.

The Treasury Department contributes to the development of multinational policies to combat illicit financing threats that undermine the integrity of the international financial system through its participation in the Financial Action Task Force (FATF), a 34-nation initiative to combat money laundering. FATF has been very successful in persuading countries to implement more robust anti-money laundering standards by developing a TBML typology, increasing awareness of TBML vulnerabilities, identifying best practices, encouraging countries to increase TBML cooperation, and evaluating member countries' anti-money laundering initiatives. That said, although FATF has issued 40 recommendations to counter money laundering writ large, none of them specifically address trade-based money laundering.[23]

The Financial Crimes Enforcement Network (FinCEN), a Treasury Department regulatory agency, reviews all TBML-related Suspicious Activity Reports (SARs) that are filed by financial institutions. FinCEN can also utilize Geographic Targeting Orders (GTOs), which requires any U.S. financial institution with operations within a geographic area to report on transactions any greater than a specified value. FinCEN has the ability to analyze this data and identify typologies, patterns, and trends, which could serve as feedback to both law enforcement and the private sector. This information is valuable as it provides law enforcement with leads to initiate new investigations, advance current investigations, and enhance intelligence-gathering efforts.

Law enforcement agencies undertake a range of enforcement actions to rein in TBML activities, including interdiction of goods, arrests, and the destruction of contraband. A Department of Homeland Security (DHS) initiative, the Homeland Security Investigations' (HSI) Trade Transparency Unit (TTU), has addressed many of these challenges. The TTU exchanges and analyzes trade data with other countries' respective customs agencies, which it then analyzes to identify trade anomalies and financial irregularities that indicate potential TBML, customs fraud, contraband smuggling, or tax evasion. HSI or its foreign counterparts can then investigate the leads generated by this analysis.[24]

Multiple U.S. law enforcement agencies have authority to investigate TBML-related illicit activity, including HSI, Customs and Border Protection, the FBI, the Drug Enforcement Administration, and the IRS. In the absence of a TBML-specific information-sharing mechanism, this wide range of agencies, which may each employ different techniques to combat and investigate TBML under different legal authorities, can complicate the development of a clear picture of TBML activities.

International intelligence collection and sharing efforts surrounding TBML have proven to be challenging, as the proceeds of illicit activity are often disguised through legitimate trade transactions. Many nations' law enforcement agencies are unfamiliar with the intricacies of international trade. Moreover, law enforcement authorities in different countries must work together under varying legal frameworks and international agreements (such as Mutual Legal Assistance Agreements), which can complicate the exchange of intelligence across borders.

INDUSTRY

Industry addresses TBML through three principal initiatives: (1) preserving the integrity of the supply chain, (2) training law enforcement agencies to build awareness about TBML, and (3) advocating for regulatory frameworks that may reduce TBML.

First, preserving supply chain integrity requires the implementation of strong 'know your customer and client' policies.[25] Such due diligence is complemented by analyses of purchases to detect fraud by, for example, monitoring customer orders to ensure they are commensurate with demand in the intended market and detecting unusual purchasing patterns that may reflect diversion somewhere in the supply chain. Supply chain security is strengthened through the implementation of track and trace systems that allow companies to follow the movement of products as they change hands. Using an item's unique identifier, products can be traced back through the supply chain to identify potential points of diversion.

Second, large corporations train law enforcement agencies to provide officers with information, tools, and mechanisms to identify TBML risks and common TBML *modus operandi*. While U.S. government agencies train their foreign law enforcement counterparts to address a wide range of threats – including terrorism, drug trafficking, and transnational crime – they typically do not provide training on TBML techniques. Companies affected by TBML have helped fill the void by sharing information and best practices with both U.S. and foreign law enforcement agencies.

Lastly, many commercial companies advocate for greater regulatory frameworks of high-volume Free Trade Zones (FTZs), which due to more limited state controls and oversight and a resulting lack of transparency, often facilitate the illicit manufacture and import/export of products. Greater transparency regarding FTZ operations and the implementation of clear guidelines for FTZ operators will help limit illicit activity.

SOLUTIONS & RECOMMENDATIONS

The threats posed by TBML could be addressed by more robust cooperation between government agencies and affected companies. Such cooperation would require intelligence and law enforcement analysts to develop a better understanding of how TBML works and how threat actors make use of it.

1. **Government and industry should create, operate, and fund a joint public-private TBML Fusion Center.**

   Because TBML activities take place in multiple jurisdictions and affect multiple business sectors, any solution must include formalized mechanisms to share information. However, because the corporations affected by TBML often have information that complements data held by government agencies, TBML information-sharing mechanisms must include both public and private sector entities. Such a mechanism must take measures to protect sensitive information – both classified or investigative data held by government agencies and proprietary business data held by companies.

   A public-private partnership to create an analysis fusion center could create a space where government and industry can work together in a trusted, secure environment, with the results benefiting all participants. A TBML center would benefit from close collaboration in real time with personnel contributions from government intelligence and law enforcement agencies, financial crimes experts, commodity experts, threat analysts, and criminal behavioral experts, among others, working in a common physical space alongside industry experts from the private sector. This environment would integrate public and private efforts to understanding current and emerging threats, craft ways and means to counter these threats, and communicate results to all participating members.

   As with any endeavor that addresses a national security problem, the availability of actionable intelligence is essential. The U.S. intelligence and law enforcement communities must work on ways and means to share information with industry on TBML actors, operations, trends and other useful data collected as part of their broader money laundering and illegal banking monitoring. Industry must share business sensitive information as it impacts TBML even if there is risk of this information falling into the hands of competitors.

“A TBML center would benefit from close collaboration in real time with personnel contributions from government intelligence and law enforcement agencies, financial crimes experts, commodity experts, threat analysts, and criminal behavioral experts, among others, working in a common physical space alongside industry experts from the private sector.

Information Sharing and Analysis Centers (ISACs) provide a potential model for a TBML public-private fusion center. ISACs are non-profit organizations that gather information on cyber threats to sector-specific critical infrastructure and provide two-way sharing of information between the private and public sectors. ISACs assist federal and local governments and critical infrastructure operators by providing information on current and potential cyber threats.

The Treasury Department's Office of Intelligence and Analysis (OI&A), as the Intelligence Community's lead for financial intelligence, should develop a proof-of-concept blueprint as a step toward operationalizing a TBML fusion center.

2. **The Intelligence Community should enhance its own collection and analysis of information on TBML from both open source and clandestine sources.**

Economic and commercial data is not among the U.S. government's highest intelligence collection priorities. However, the government nevertheless gathers a great deal of relevant information by targeting terrorist groups, drug cartels, transnational criminal organizations, corrupt foreign officials, and others engaged in TBML. The intelligence and law enforcement communities should issue guidance to compile and disseminate this data in a methodical manner that can be used by government and industry analysts.

Separately, the Treasury Department's Office of Intelligence and Analysis, as the lead IC component for threat finance, should dedicate analytic staff to TBML threats. Identification of TBML schemes through analysis of economic and commercial data could enhance the Intelligence Community's ability to uncover – and thus disrupt – activity that threatens U.S. national security, such as terrorist plots, drug trafficking, and official corruption.

3. **The Intelligence Community should enhance analyst training in how TBML works and why it is important.**

Because TBML is not a high priority for the Intelligence Community, TBML is not well understood by intelligence analysts. Analyst training could include industry subject matter experts providing TBML instruction and case studies to employees. This may encourage understanding of what constitutes TBML, what a TBML case would look like, and how TBML can be identified through information acquired by both government and industry sources. Finally, the incorporation of more TBML risk-based training could provide a hands-on interaction for employees. If employees are provided with this improved training, it will better prepare the IC to detect, monitor and deter such illegal activities.

4. **Strengthen U.S. engagement in FATF as means of promoting international solutions, training, and information-sharing mechanisms using TBML intelligence and assessments from both government and industry.**

FATF has been largely successful in carrying out its inter-governmental mandate by its members, but there is still more to do to address trade-based money laundering. FATF should encourage members' financial intelligence units (FIUs) to collect, analyze, and share TBML intelligence and investigative leads across borders through mechanisms such as the 164-nation Egmont Group of FIUs, which was formed to combat money laundering and terrorist financing through the sharing of financial intelligence.[26] As discussed previously, sharing financial and trade information across borders – even among jurisdictions with appropriate international agreements in place – is a challenge. Where countries have TTUs in place, the FIUs could further assist by adding analytical resources and matching the trade data discrepancies with financial transactions.

FATF should also consider partnering with private sector subject matter experts on the use of emerging technology to address TBML suspicious transactions. With the advancement of process robotics and artificial intelligence, patterns and algorithms consistent with TBML activity could be better developed and used by interested parties to more effectively address this global trade vulnerability.

REFERENCES

[1] *Sen. Bill Cassidy, "Trade Based Money Laundering: An Asymmetric Threat With Ties to Terror and Drugs," white paper, no date, p. 2. At https://www.cassidy.senate.gov/imo/media/doc/TBML%20White%20Paper.pdf.*

[2] *Citi, Trade-Based Money Laundering: Your Guide to Understanding It, Detecting It, and Preventing It, 2016, p. 3. At https://www.citibank.com/tts/insights/eSource_academy/docs/thought_leadership/1461942122-Citi-Trade-Based-Money-Laundering-Whitepaper.pdf.*

[3] *Financial Crimes Enforcement Network (FinCEN), "Advisory to Financial Institutions on Filing Suspicious Activity Reports regarding Trade-Based Money Laundering," FIN-2010-A001, February 18, 2010. At https://www.fincen.gov/sites/default/files/advisory/fin-2010-a001.pdf.*

[4] *According to the World Trade Organization (WTO), global merchandise trade in 2018 totaled $19.5 trillion. World Trade Organization, "Global Trade Growth Loses Momentum as Trade Tensions Persist," press release, April 2, 2019. At https://www.wto.org/english/news_e/pres19_e/pr837_e.htm.*

[5] *U.S. Immigration and Customs Enforcement, "Money Laundering," web site, updated January 3, 2018. At. https://www.ice.gov/money-laundering.*

[6] *Phillip Morris International, Anti-Diversion Governance Committee Progress and Outlook Report, 2016-2017: Supply Chain Protection, September 2017, p. 11. At. https://www.stopillegal.com/docs/default-source/anti-diversion/anti-diversion-governance-comittee-report-2016-17.pdf?sfvrsn=b8973d7_2.*

[7] *Department of Treasury, National Money Laundering Risk Assessment 2015, p. 4. At https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf.*

[8] *OECD, "Online public consultation on the draft OECD Guidance to Counter Illicit Trade, Enhancing Transparency in Free Trade Zones," website, September 2018, At https://www.oecd.org/governance/online-public-consultation-draft-guidance-enhancing-transparency-in-free-trade-zones.htm. See also FATF, Money Laundering Vulnerabilities of Free Trade Zones, March 2010, pp. 2-3, 19-20. At https://www.fatf-gafi.org/media/fatf/documents/reports/ML%20vulnerabilities%20of%20Free%20Trade%20Zones.pdf. See also Phillip Morris International, Fighting Illicit Trade: Free Trade Zones, May 2018. At https://www.stopillegal.com/docs/default-source/position-papers/ftz-position-paper-may-2018.pdf?sfvrsn=4dee70d7_2.*

[9] *Matthew Levitt, "Hezbollah's Criminal Networks: Useful Idiots, Henchmen, and Organized Criminal Facilitators," in Hillary Matfess and Michael Miklaucic, eds., Beyond Convergence: World Without Order (Washington, DC: National Defense University, 2016), pp. 158-159. At https://www.washingtoninstitute.org/uploads/Documents/opeds/Levitt20161025-NDU-chapter.pdf.*

[10] *U.S. Immigration and Customs Enforcement, January 3, 2018.*

[11] *GAO, U.S. Agencies Should Systematically Assess Terrorists' Use of Alternative Financing Mechanisms, GAO-04-163, November 2003. At https://www.gao.gov/new.items/d04163.pdf. See also Matthew Levitt, Hezbollah: Financing Terror Through Criminal Enterprise, Testimony to the Committee on Homeland Security and Governmental Affairs, United States Senate, May 25, 2005. At http://www.washingtoninstitute.org/html/pdf/hezbollah-testimony05252005.pdf.*

[12] *See, for example, Louise I. Shelley and Sharon A. Melzer, "The Nexus of Organized Crime and Terrorism: Two Case Studies in Cigarette Smuggling," International Journal of Comparative and Applied Criminal Justice, Spring 2008, Vol. 32, No. 1. At http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.920.4138&rep=rep1&type=pdf. See also*

[13] *John Cassara, "Trading with The Enemy: Trade-Based Money Laundering Is the Growth Industry in Terror Finance," Task Force to Investigate Terrorism Financing, Committee on Financial Services, U.S. House of Representatives, February 3, 2016. At https://www.govinfo.gov/content/pkg/CHRG-114hhrg23565/html/CHRG-114hhrg23565.htm.*

[14] *Department of Treasury, National Money Laundering Risk Assessment 2015, p. 32. At https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf.*

[15] *KPMG, Illicit Cigarette Trade in the Maghreb Region, July 26, 2017, p. 27. At https://www.pmi.com/resources/docs/default-source/pmi-sustainability/report-on-the-illicit-cigarette-trade-in-the-maghreb-region.pdf?sfvrsn=67a69ab5_2. Public revenue data from OECD.Stat, Details of Public Revenues – Tunisia. At https://stats.oecd.org/Index.aspx?DataSetCode=REVTUN.*

[16] *U.S. Agency for International Development, Country Development Strategy – Tunisia, web page, updated October 18, 2018. At https://www.usaid.gov/tunisia/cdcs.*

[17] *Senator Roger Wicker, opening statement, Hearing on 'A Hazy Crisis: Illicit Cigarette Smuggling in the OSCE Region,' United States Commission on Security and Cooperation in Europe, July 19, 2017. At https://www.csce.gov/sites/helsinkicommission.house.gov/files/Opening%20Statement%20Cigarette%20Smuggling%20Hearing%20FINAL.pdf.*

[18] *Frank Andrews, "Fake Cigarette Ring Exposes Jordan's Corruption Woes," Organized Crime and Corruption Reporting Project, August 21, 2019. At https://www.occrp.org/en/blog/10533-fake-cigarette-ring-exposes-jordan-s-corruption-woes.*

[19] *Maria E. de Boyrie, James A. Nelson, and Simon J. Pak, "Capital Movement through Trade Misinvoicing: The Case of Africa," Journal of Financial Crime, October 2007. At DOI: 10.1108/13590790710828181.*

[20] *"Advisory to Financial Institutions on Illicit Financial Schemes and Methods Related to the Trafficking of Fentanyl and Other Synthetic Opioids," FinCEN Advisory FIN-2019-A006, August 21, 2019. https://www.fincen.gov/sites/default/files/advisory/2019-08-21/Fentanyl%20Advisory%20FINAL%20508.pdf.*

[21] *Svletlana Agayeva, Examining Anti-Bribery and Corruption Measures in a Single Framework to Combat Money Laundering and Terrorist Financing, Association of Certified Anti-Money Laundering Specialists, 2015, p. 4. At : http://www.acams.org/wp-content/uploads/2015/08/Examining-Anti-Bribery-and-Corruption-Measures-in-a-Single-Framework-to-Combat-ML-TF.pdf*

[22] *Mark Shaw and Fiona Mangan, Illicit Trafficking and Libya's Transition: Profits and Losses, United States Institute of Peace, Peaceworks No. 96, 2014, pp. 7, 36. At file:///C:/Users/lhanauer/Downloads/PW96-Illicit-Trafficking-and-Libyas-Transition.pdf.*

[23] *Rena S. Miller, Liana W. Rosen, and James K. Jackson, Trade-Based Money Laundering: Overview and Policy Issues, Congressional Research Service, Report R44541, June 22, 2016, p. 10. At https://fas.org/sgp/crs/misc/R44541.pdf.*

[24] *U.S. Immigration and Customs Enforcement, "Trade Transparency Unit," website, updated January 3, 2018. At https://www.ice.gov/trade-transparency.*

[25] *See examples of strong "know your customer" and "customer due diligence" steps recommended for financial institutions, many of which are also employed by manufacturers, at Citi, Trade-Based Money Laundering: Your Guide to Understanding It, Detecting It, and Preventing It, 2016, p. 10. At https://www.citibank.com/tts/insights/eSource_academy/docs/thought_leadership/1461942122-Citi-Trade-Based-Money-Laundering-Whitepaper.pdf.*

[26] *Egmont Group, "About Egmont Group," web site, accessed February 27, 2020. At https://egmontgroup.org/en/content/about.*

ABOUT INSA

The Intelligence and National Security Alliance (INSA) is a nonpartisan, nonprofit trade association dedicated to advancing collaborative, public-private approaches to intelligence and national security priorities. Through the application of industry expertise, leading-edge academic research and commercial best practices, INSA seeks to make the Intelligence Community more effective and efficient. Our 160+ member organizations and its 4,000+ individual and associate members include senior executives and intelligence experts in the public, private and academic sectors.

ABOUT INSA'S FINANCIAL THREATS COUNCIL

INSA's Financial Threats Council works to strengthen public-private cooperation and information sharing regarding the broad range of threats faced by government, the financial services sector, and other industries, which include cyber security, money laundering, terrorist finance, transnational organized crime, corruption, and confidence in U.S. and global financial infrastructure.
Learn more at www.insaonline.org/councils

INSA
INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

Building a Stronger Intelligence Community

(703) 224-4672 | www.INSAonline.org