THE NEXT TERRORIST FINANCIERS: STOPPING THEM BEFORE THEY START

HEARING

BEFORE THE

TASK FORCE TO INVESTIGATE TERRORISM FINANCING

OF THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

JUNE 23, 2016

Printed for the use of the Committee on Financial Services

Serial No. 114–94

U.S. GOVERNMENT PUBLISHING OFFICE

25–849 PDF WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

HOUSE COMMITTEE ON FINANCIAL SERVICES

JEB HENSARLING, Texas, *Chairman*

PATRICK T. MCHENRY, North Carolina, *Vice Chairman*
PETER T. KING, New York
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
SCOTT GARRETT, New Jersey
RANDY NEUGEBAUER, Texas
STEVAN PEARCE, New Mexico
BILL POSEY, Florida
MICHAEL G. FITZPATRICK, Pennsylvania
LYNN A. WESTMORELAND, Georgia
BLAINE LUETKEMEYER, Missouri
BILL HUIZENGA, Michigan
SEAN P. DUFFY, Wisconsin
ROBERT HURT, Virginia
STEVE STIVERS, Ohio
STEPHEN LEE FINCHER, Tennessee
MARLIN A. STUTZMAN, Indiana
MICK MULVANEY, South Carolina
RANDY HULTGREN, Illinois
DENNIS A. ROSS, Florida
ROBERT PITTENGER, North Carolina
ANN WAGNER, Missouri
ANDY BARR, Kentucky
KEITH J. ROTHFUS, Pennsylvania
LUKE MESSER, Indiana
DAVID SCHWEIKERT, Arizona
FRANK GUINTA, New Hampshire
SCOTT TIPTON, Colorado
ROGER WILLIAMS, Texas
BRUCE POLIQUIN, Maine
MIA LOVE, Utah
FRENCH HILL, Arkansas
TOM EMMER, Minnesota

MAXINE WATERS, California, *Ranking Member*
CAROLYN B. MALONEY, New York
NYDIA M. VELÁZQUEZ, New York
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
MICHAEL E. CAPUANO, Massachusetts
RUBÉN HINOJOSA, Texas
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
DAVID SCOTT, Georgia
AL GREEN, Texas
EMANUEL CLEAVER, Missouri
GWEN MOORE, Wisconsin
KEITH ELLISON, Minnesota
ED PERLMUTTER, Colorado
JAMES A. HIMES, Connecticut
JOHN C. CARNEY, JR., Delaware
TERRI A. SEWELL, Alabama
BILL FOSTER, Illinois
DANIEL T. KILDEE, Michigan
PATRICK MURPHY, Florida
JOHN K. DELANEY, Maryland
KYRSTEN SINEMA, Arizona
JOYCE BEATTY, Ohio
DENNY HECK, Washington
JUAN VARGAS, California

SHANNON MCGAHN, *Staff Director*
JAMES H. CLINGER, *Chief Counsel*

TASK FORCE TO INVESTIGATE TERRORISM FINANCING

MICHAEL G. FITZPATRICK, Pennsylvania, *Chairman*

ROBERT PITTENGER, North Carolina, *Vice Chairman*
PETER T. KING, New York
STEVE STIVERS, Ohio
DENNIS A. ROSS, Florida
ANN WAGNER, Missouri
ANDY BARR, Kentucky
KEITH J. ROTHFUS, Pennsylvania
DAVID SCHWEIKERT, Arizona
ROGER WILLIAMS, Texas
BRUCE POLIQUIN, Maine
FRENCH HILL, Arkansas

STEPHEN F. LYNCH, Massachusetts, *Ranking Member*
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
AL GREEN, Texas
KEITH ELLISON, Minnesota
JAMES A. HIMES, Connecticut
BILL FOSTER, Illinois
DANIEL T. KILDEE, Michigan
KYRSTEN SINEMA, Arizona

CONTENTS

WITNESSES

THURSDAY, JUNE 23, 2016

APPENDIX

THE NEXT TERRORIST FINANCIERS: STOPPING THEM BEFORE THEY START

Thursday, June 23, 2016

U.S. HOUSE OF REPRESENTATIVES,
TASK FORCE TO INVESTIGATE
TERRORISM FINANCING,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The task force met, pursuant to notice, at 10:13 a.m., in room 2128, Rayburn House Office Building, Hon. Michael Fitzpatrick [chairman of the task force] presiding.

Members present: Representatives Fitzpatrick, Pittenger, Ross, Barr, Rothfus, Poliquin, Hill; Lynch, Foster, and Sinema.

Also present: Representatives Garrett and Carney.

Chairman FITZPATRICK. The Task Force to Investigate Terrorism Financing will come to order.

Without objection, the Chair is authorized to declare a recess of the task force at any time. Also, without objection, members of the full Financial Services Committee who are not members of the task force may participate in today's hearing for the purpose of questioning the witnesses.

The Chair now recognizes himself for 4 minutes for an opening statement.

Thank you, everyone, for joining us today for the eleventh and final hearing of the House Financial Services Committee's Task Force to Investigate Terrorism Financing. Today's hearing is entitled, "The Next Terrorist Financiers: Stopping Them Before They Start."

I would like to again thank Chairman Hensarling and Ranking Member Waters, as well as my colleagues here, for their unwavering support as we have investigated the threat of terror finance. I would also like to take a moment to thank Liana Rosen and Martin Weiss of the Congressional Research Service for the invaluable assistance that they have provided to this body.

On June 12, 2016, we watched in horror as a lone terrorist pledging allegiance to ISIS carried out the Nation's worst terror attack since 9/11. As we continue to grieve and pray for those devastated by this attack, we must redouble our efforts to be clear in our resolve to protect our Nation and her citizens from radical Islamic terrorism that continues to target us. Our efforts to combat this radicalism must be carried out on multiple fronts through diplomatic action, military force, and countering the finances used to carry out these attacks.

As chairman of this Task Force to Investigate Terrorism Financing, I have joined with Ranking Member Lynch, Vice Chair Pittenger, and this dedicated bipartisan body to investigate and evaluate the efforts made by the United States to counter and dismantle the financial networks funding these terrorist organizations.

Our investigation has covered a range of topics, including the vulnerabilities of the global financial system, trade-based money laundering, the importance of assisting the developing world, and the sale and trafficking of illicit goods. During this time, it has become evident the United States must be able to work freely with its international partners and seamlessly adapt to evolving money laundering and terror financing tactics.

For this reason, the task force will be proposing a series of bills which aim to improve communication and coordination amongst various government agencies, allow for increased information sharing, and ensure the Treasury is properly supported and recognized for its role in our Nation's national security strategy. These bills, coupled with the report containing the task force's findings, will provide a clear blueprint for the United States so it may continue to evolve and improve in its fight to ensure terror groups are unable to financially support their operations.

Today, for the eleventh and final hearing of this task force, we will recap what we have learned with these five expert witnesses who have previously lent their voices to this discussion in past hearings. Together, we will discuss the necessary changes Congress must consider to better enable U.S. agencies in our fight.

At this time, I would like to recognize a member of the bipartisan task force, Ms. Sinema of Arizona, our colleague, who has been a valuable asset and trusted friend during the course of these hearings, for an opening statement.

Ms. SINEMA. Thank you, Chairman Fitzpatrick.

Over the course of the past 10 hearings, this task force has found that U.S. Government efforts to counter the financing of terrorism lack sufficient coordination, and that the United States has no unified national strategy to guide our counterfinancing efforts. We need a whole of government CTF strategy that enhances detection, deterrence, and prosecution, and ultimately furthers our broader national security goals.

I appreciate the witnesses' testimony in past hearings, and agree that the Federal Government must change its approach and mindset to counter the financing of terrorism. I look forward to hearing more from our witnesses today about ways to improve the effectiveness of our counterterrorism financing efforts and to better align these efforts with our broader national interests.

Thank you to Chairman Fitzpatrick and Ranking Member Lynch for their leadership on this task force. I look forward to continuing our work with colleagues on both sides of the aisle to keep money out of terrorists' hands and build on our progress to strengthen America's security.

I yield back.

Chairman FITZPATRICK. At this time, I would like to recognize the vice chairman of the task force, Mr. Robert Pittenger of North Carolina, who was one of the first Members of the House to bring

ideas on CTF and on money laundering proposals to the full House Financial Services Committee. I recognize Mr. Pittenger for an opening statement.

Mr. PITTENGER. Thank you, Mr. Chairman. I deeply appreciate your great leadership on this important task force. And Mr. Pinder, thank you for your supportive role in all that we do.

And thank you, distinguished panelists, for the critical role that you play with us—for some of you, this will be your second or third time to be with us—and the counsel that you provide to us. We recognize better the importance of terrorism financing. This is an important tool for us to be able to defeat the Islamic terrorists.

This week, I just returned from a forum with over 100 members of Parliament and other government officials from 30 countries. As we seek to collaborate with them on issues of terrorism financing and intelligence and cybersecurity matters, the one thing that I have observed is that our partners around the world generally seek to work with us, but they don't have the tools. They don't have the understanding. And they need the resources that must be provided. So the input that you provide this task force has really been critical.

So I welcome your input today and your advice, and frankly, the experience that you have had, observations, even since the last time we met. So thank you for being with us. We look forward to our further dialogue.

I yield back.

Chairman FITZPATRICK. We now welcome our witnesses.

Mr. Juan Zarate is chairman and senior counselor at the Center on Sanctions and Illicit Finance at the Foundation for Defense of Democracies. Mr. Zarate served as the Deputy Assistant to the President and the Deputy National Security Adviser for Combating Terrorism from 2005 until 2009, and was responsible for developing and implementing all aspects of the U.S. Government's counterterrorism strategy. Mr. Zarate was the first ever Assistant Secretary of the Treasury for Terrorist Financing and Financial Crimes. He is also a former Federal prosecutor who served on terrorism prosecution teams prior to 9/11, including the investigation of the USS Cole attack in Yemen.

Mr. Zarate is a graduate of Harvard College and Harvard Law School, and is a former Rotary International Fellow at the University of Salamanca in Spain. Mr. Zarate testified before the task force's April 22, 2015, hearing entitled, "A Survey of Global Terrorism and Terrorist Financing."

The Honorable Jimmy Gurule is a law professor at Notre Dame Law School. Mr. Gurule joined the Notre Dame Law School faculty in 1989, and became a full professor in 1996. The professor has also worked in a variety of high-profile public law enforcement positions, including Under Secretary for Enforcement at the U.S. Department of the Treasury from 2001 until 2003; Assistant Attorney General for the Office of Justice Programs at DOJ from 1990 until 1992; and Assistant U.S. Attorney, where he served as Deputy Chief of the major narcotics section of the Los Angeles U.S. Attorney's Office from 1985 to 1989.

He earned his bachelor's degree from the University of Utah in 1974, and his juris doctorate from the University of Utah College of Law in 1980.

Mr. John Cassara is a former United States Intelligence Officer and Treasury Special Agent. He has over 26 years of experience in the Federal Government intelligence and law enforcement communities. An expert in anti-money laundering and terror financing, Mr. Cassara invented the concept of international trade transparency units, and recently released a book on the topic this past fall entitled, "Trade-Based Money Laundering: The Next Frontier in International Money Laundering Enforcement." He has lectured around the world on a variety of transnational crime issues, and is currently an industry adviser.

Mr. Cassara holds a master's degree in international management from the American Graduate School of International Management in Phoenix, Arizona. He graduated magna cum laude from the University of California San Diego, with a bachelor's degree in political science.

Professor Celina Realuyo is a professor of practice at the William J. Perry Center for Hemispheric Studies at the National Defense University. Prior to joining the National Defense University in 2007, Ms. Realuyo served as the State Department Director of Counterterrorism Finance Programs in the U.S. Secretary of State's Office of the Coordinator for Counterterrorism. She has also cochaired the terror financing work group. Professor Realuyo has previously been a private banker in London with Goldman Sachs International, and also previously had a distinguished career as a United States foreign service officer.

She holds an MBA from the Harvard Business School, an M.A. from Johns Hopkins University School of Advanced International Studies, and a bachelor's degree from the Georgetown University School of Foreign Service.

Mr. Douglas Farah is president of IBI Consultants LLC, and is also a senior non-resident associate for the Americas Program at the Center for Strategic and International Studies. From 1985 to 2005, Mr. Farah worked as a journalist, primarily as a foreign correspondent and investigative reporter for The Washington Post. Since leaving the Post in 2004, Mr. Farah has worked as a consultant to the United States Government on national intelligence reform, nonstate armed actors, critical infrastructure protection, criminal terrorist pipelines, bulk cash smuggling to Mexico, as well as other topics. He is also the author of two books, and he appears regularly in a national and international medium, and has been published in more than a dozen journals and magazines.

Mr. Farah graduated from the American Cooperative School in La Paz, Bolivia. He also received a bachelor's degree with highest honors from the William Allen White School of Journalism at the University of Kansas, with a bachelor's in honors in Latin American studies from the University of Kansas.

The witnesses will now be recognized for 5 minutes each to give an oral presentation of their written testimony.

And without objection, the witnesses' written statements will be made a part of the record.

Once the witnesses have finished presenting their testimony, each member of the task force will have 5 minutes within which to ask questions.

For the witnesses, on your table are three lights, which you are familiar with. Yellow means you have 1 minute remaining. Red means your time is up.

At this point, Mr. Zarate, you are now recognized for 5 minutes.

STATEMENT OF JUAN C. ZARATE, CHAIRMAN AND CO-FOUNDER, FINANCIAL INTEGRITY NETWORK; AND CHAIRMAN AND SENIOR COUNSELOR, CENTER ON SANCTIONS AND ILLICIT FINANCE, FOUNDATION FOR DEFENSE OF DEMOCRACIES

Mr. ZARATE. Mr. Chairman, thank you for that kind introduction. Ranking Member Lynch, Vice Chairman Pittenger, distinguished members of this task force, I am honored to be before you yet again to testify on the evolving threats and issues tied to terrorist financing and illicit financing. I am especially honored to be with this panel, all of whom I consider friends and from whom I have learned quite a bit throughout their careers.

Let me begin by commending this task force for not only your diligence but your bipartisan efforts to focus on these issues. Over a year ago, when many thought that this issue did not have relevance, I think much has happened over the last year to not only prove the relevance of this task force but the importance of your work. And I want to thank your committee staff, including Joe Pinder, for his continued efforts over the course of many years in this regard.

But there have been many things that have happened since we last met. Terrorist organizations and criminal networks have continued to leverage local and regional economies and the global commercial system to profit and evade scrutiny. Growing regional and proxy battles in the Middle East, South Asia, and Africa have increased the risk that terrorist and militant groups are taking advantage of crises to create for-profit militancy and networks. Terrorist infiltration and control of urban environments in places like Mosul, Sirte, and Raqqa have complicated how the U.S. Government and our allies attempt to disrupt terrorist financing, putting a premium on dislodging terrorist organizations physically from key sites and resources.

The application of U.S. law and pressure from targeted sanctions to exclude Hezbollah from the Lebanese financial system has created enormous pressure in Lebanon, with Hezbollah leadership speaking out against the closing of Hezbollah-related bank accounts and a bomb exploding just recently in front of Blom Bank in Beirut.

The Panama Papers and tax-related leaks have raised important questions about the limits of financial transparency and accountability, and whether the current anti-money laundering system globally is effective. Complications and burdens on the legitimate financial community in the application of sanctions and financial crime risk management have continued to abut against the public policy needs for financial inclusion.

New technologies enabling the digital economy are providing not only enormous opportunities for innovation and access, but illicit

actors are also finding ways to leverage tools like digital currency to create illicit bazaars via the Internet and access capital without scrutiny, as we saw in the Silk Road and Liberty Reserve cases. And continued and significant cyber attacks by state and nonstate actors on the financial sector have demonstrated yet again that the financial system remains at the heart of the cyber storm.

These are just a few of the examples and recent developments that continue to illuminate and complicate the terrorist and illicit financial landscape. Billions of dollars in illicit trade and money laundering continue to reach the hands of criminals and illicit actors, despite best efforts. More needs to be done. And I know this task force has done quite a bit of work, but let me suggest seven categories of work to focus on.

First, we need to continue to sharpen the tools that we use in our toolkit. The playbook that we have used since 9/11 must remain strategic, its implementation focused on effectiveness. And it must be reinforced with a strengthened and committed international system devoted to the protection of the international financial system and our collective security.

Two, the United States must find strategic ways of using targeted unwinding of sanctions to our strategic benefit. We are seeing the challenges of this now with Iran, Cuba, and even Burma. The United States should ensure that it is using its power of unwinding the way that we use the power of targeted sanctions to full effect.

Three, we must have a more aggressive information-sharing system between public and private authorities, within sectors, and across borders. We are working on a 20th Century model that is crashing up against the 21st Century economy and expectations. We need to think differently about how information is shared, analyzed, and used to protect the financial system.

Fourth, we have to balance financial exclusion and inclusion by finding ways of sharing the risk. The twin goals of financial integrity and inclusion can be met with some creative collaboration.

Fifth, we must focus on the effectiveness of the AML/CFT and sanction system. And we should not be shy about leading the world in its enforcement and in judging the world in terms of effectiveness.

Sixth, we must realize and address the convergence of cyber and financial warfare. As I said, the financial community is now at the center of the cyber storm, and the recent bank heist involving the SWIFT network was a wake-up call for the attack on the trust and integrity of that system. There needs to be a more aggressive approach to private sector defense of its systems and public-private collaboration to defend critical financial systems.

And finally, we need the resources to be able to regulate and enforce. This means resources not just for Treasury, OFAC, and FinCEN, the usual bodies, but also the IRS, CID, and others that are forced and need to enforce these laws and regulations.

Finally, Mr. Chairman, these are tools and strategies that need to be embedded in a broader strategy of national and economic security. And this is not just confined to the quiver of economic sanctions or targeted financial measures. This has to include the development of strategies of financial inclusion that use elements of U.S.

economic influence, private investment to benefit good behavior and to promote what our allies are trying to do around the world. It also involves developing defensive economic strategies with our allies to counter the potential economic influence and pressure that countries like Russia and China are already wielding.

In the 21st Century, Mr. Chairman, economic security underpins the Nation's ability to project its power and influence. And the power to affect the budgets of America's enemies is an enormous power that needs to be tended carefully and wielded wisely. And America's enemies, especially nimble terrorist organizations that often blend with criminality, will continue to find ways to work around the international pressure and strictures put upon them.

This is why the campaign against terrorist financing is not a static venture, but instead, an ongoing and critical part of the challenging terrorist and international security landscape. The U.S. Government must continue to innovate and find new ways and partners to make it harder, costlier, and riskier for terrorist groups around the world to raise and move money.

Mr. Chairman, thank you again for the privilege of testifying today. I would be happy to answer any questions you or your colleagues may have.

[The prepared statement of Mr. Zarate can be found on page 87 of the appendix.]

Chairman FITZPATRICK. Thank you.

Professor Gurule, you are recognized for 5 minutes.

STATEMENT OF THE HONORABLE JIMMY GURULE, LAW PROFESSOR, UNIVERSITY OF NOTRE DAME LAW SCHOOL

Mr. GURULE. Chairman Fitzpatrick, Ranking Member Lynch, Vice Chairman Pittenger, and other distinguished members of the Task Force to Investigate Terrorism Financing, permit me to begin by thanking you for inviting me to testify on the important and timely topic of, "The Next Terrorist Financier: Stopping Them Before They Start."

As we approach the 15-year anniversary of the 9/11 terrorist attacks that tragically took the lives of approximately 3,000 innocent civilians, it is imperative that the U.S. Government continue to evaluate and enhance the effectiveness of such counterterrorism measures as curtailing terror financing in order to protect national security and save innocent lives. To that end, I would like to propose four recommendations to the task force and the broader committee to strengthen the U.S. Government's counterterrorist financing efforts.

The first recommendation deals with economic sanctions. Shortly after the 9/11 terror attacks, President George W. Bush signed Executive Order 13224. It authorizes the President as delegated to the Secretary of the Treasury to designate individuals and entities as specially designated global terrorists (SDGT's). That designation has important legal implications.

First, any assets located in the United States of such individuals and entities have to be frozen. Second, U.S. persons are prohibited from doing business with the SDGTs, the specially designated global terrorists.

Initially, the executive order designated 12 individuals and 15 entities as SDGTs. At present, there are now over 1,000 such individuals, such SDGTs. And while the executive order has been an effective tool in curtailing the funding to Al Qaeda, which relies largely on support from external donors and corrupt charities sympathetic to their cause, it has been less effective with respect to the Islamic State.

The Islamic State poses a different terrorist financing challenge. It obtains its money primarily from external sources, including the sale of oil and gas, extortion and taxation, kidnapping for ransom, looting banks, selling stolen equities, and human trafficking—selling young girls and women as sex slaves. The Islamic State's annual budget has been estimated to be as high as $2 billion.

The reason why the executive order again has been less effective with respect to the Islamic State is that the individuals who have been targeted under the executive order, members of the Islamic State, senior leaders of the Islamic State, do not have resources in the United States. They don't have assets in the United States to be blocked. Furthermore, there is no evidence that U.S. persons are doing business with such individuals.

I don't want to diminish the importance of being designated under the executive order, but in large part it becomes more symbolic in kind of highlighting and identifying these individuals as bad actors than actually curtailing the funding of the Islamic State. And so what I propose, in addition—not in place of but in addition to—would be that Congress pursue a model similar to that which has been used against Iran, and which is focused not only on primary sanctions but secondary sanctions.

Primary sanctions prohibit U.S. persons from doing business with the target. Secondary sanctions prohibit foreign persons and foreign entities from doing business with the entity. And I think we need a sanction regime that is similar to the Comprehensive Iran Sanctions and Accountability and Divestment Act of 2010, which does exactly that: prohibits foreign businesses from contributing to the energy sector of Iran. And we need something similar for the Islamic State.

My second recommendation deals with the criminal enforcement and, specifically, the material support statute. I think the Department of Justice has a very checkered record of prosecuting major, underscoring major, terrorist financiers. I think to that end the efforts could be enhanced if Congress amended the terrorist financing statute 18 U.S.C. 2339C to lower the scienter threshold from requiring the government to prove that the defendant knowing and with the intent—or intended the funds to be used to finance violent crimes.

Instead, it seems to me that it should be a crime if an individual donates to, let's say, a lone wolf terrorist knowing that individual is engaged in terrorist acts or intends to engage in terrorist acts. That type of conduct should be prohibited under the statute, and currently it is not.

My third recommendation deals with the Justice Against Sponsors of Terrorism Act (JASTA). On May 17, 2016, the U.S. Senate unanimously passed JASTA. I think that it plays an important role. Civil actions play an important role with respect to deterring

terrorist behavior and going after the funding of terrorism. I think it is important that any state that sponsors acts of terrorism on U.S. soil should be held accountable. And the Act seeks to accomplish that objective.

And then lastly, my fourth recommendation deals with the development of a national counterterrorist financing strategy to effectively go after the money of Al Qaeda, the Islamic State, and the next major terrorist organizations. It is imperative that the United States develop a comprehensive, coordinated counterterrorist financing strategy. Unfortunately, no such strategy exists today.

The counterterrorist financing strategy needs to be adaptive. It needs to anticipate different methods of raising money and moving money globally. It needs to be, again, proactive on the front end, not simply reacting to the crisis of the day.

So with that, thank you very much, and I look forward to answering questions during the question-and-answer session. Thank you.

[The prepared statement of Mr. Gurule can be found on page 62 of the appendix.]

Chairman FITZPATRICK. Thank you, Professor.

Mr. Cassara, you are recognized for 5 minutes.

STATEMENT OF JOHN A. CASSARA, FORMER U.S. INTELLIGENCE OFFICER AND TREASURY SPECIAL AGENT

Mr. CASSARA. Chairman Fitzpatrick, Ranking Member Lynch, Vice Chairman Pittenger, and members of the task force, thank you for the opportunity to testify today. It is an honor for me to be here and, in particular, to be included on this panel with friends and such distinguished colleagues.

In 2008, I wrote an essay published by the Department of State entitled, "Mobile Payments—A Growing Threat." Eight years later, that threat has materialized. The growth of access to cellular devices is breathtaking. In 1990, there were approximately 11 million mobile phones worldwide. In 2016, the number of mobile lines and service has surpassed global population. There are now approximately 410 million mobile money accounts in the world, with approximately 270 mobile money services operating in 93 countries. More than 1 billion mobile money transactions were processed in December 2015. We should cheer these developments.

The G20 included financial inclusion on its priority agenda to help over 2 billion adults around the world who have limited access to financial institutions. I know many task force members have traveled extensively in the developing world. Undoubtedly, you have observed how easy access to M-payments via the ubiquitous cell phone is transforming lives by providing a much-needed link to financial services at a very reasonable price.

Users are not required to have a bank account or a credit card. Countries without modern financial infrastructures are able to leapfrog directly into cutting edge networks. M-payments allow the purchase of products and services. Salaries and government benefits can be credited to cellular devices. M-payments have empowered small business creation, and remittances from migrant workers are sent home via the use of cell phones.

However, this wonderful development is going to have some very dangerous side effects. I would like to explain how M-payments are used in the three stages of money laundering.

The first stage is placement of illicit cash into financial institutions. One of the most prevalent techniques is structuring or smurfing. For example, a professional money launderer takes a large amount of drug dollars and divides it into small amounts. He gives the small sums to runners or smurfs to deposit. The transactions are done in ways that attempt to avoid mandated financial transparency reporting requirements.

M-payments offer criminals a new way to place the proceeds of crime. For example, runners are recruited and given proceeds of criminal activity or even charitable or terror finance contributions. They are given instructions to go to M-payment establishments and use the illicit funds to load up their cell phones with e-value under the maximum threshold level. The runners are then directed to forward the mobile money credit to master accounts controlled by the money launderer. This technique has been called digital smurfing.

The next objective is to layer the dirty money by multiple transfers, thereby confusing the paper trail and adding multiple levels of venue and jurisdiction. With M-payments, layering will be taken to new levels. In most jurisdictions, mobile value can be transferred from person to person and account to account, and then directed to a financial institution or money service business either in the host country or perhaps sent to another country or even an offshore haven. Mobile value could even be credited to an online account or perhaps used to purchase virtual currencies in cyberspace. Informal value transfer systems such as hawala can also be added to the equation.

Finally, a criminal organization uses the place and layered funds to integrate them into the economy by purchasing, say, for example, property, equities, and commercial enterprises. For example, the daughter of one of the worst kleptocrats in Africa has invested in cell phone carriers and M-payment providers in multiple countries.

While there are currently few documented cases of money laundering and terror finance related to M-payments, in large part this is because the countries where M-payments are present and our terrorist adversaries operate, have few, if any, anti-money laundering or terrorist-financed prosecutions and convictions. I believe we should move quickly to engineer new forms of data collection and analytic tools into M-payment systems, and put in place effective regulatory and enforcement countermeasures. Please see my written testimony for more details, including recommendations.

Thank you again for the honor of being here. I look forward to answering any questions you may have.

[The prepared statement of Mr. Cassara can be found on page 42 of the appendix.]

Chairman FITZPATRICK. Thank you.

Professor Realuyo, you are now recognized.

STATEMENT OF CELINA B. REALUYO, PROFESSOR OF PRACTICE, WILLIAM J. PERRY CENTER FOR HEMISPHERIC DEFENSE STUDIES, NATIONAL DEFENSE UNIVERSITY

Ms. REALUYO. Thank you, Chairman Fitzpatrick, Vice Chairman Pittenger, Ranking Member Lynch, and task force members, for the opportunity to appear before you again today to discuss improving efforts to combat terrorist financing through more public-private partnerships. I am honored to be here alongside those of us who started the financial front of the war on terror in the wake of 9/11.

Today, we face a broad spectrum of threats such as global terrorism, transnational organized crime, and cyber attacks that requires a multidisciplinary approach to comprehend and counter. The convergence of terrorism and crimes threaten state sovereignty and our economy. Governments can no longer guarantee the security, prosperity, and rule of law that their people expect. Average citizens who see something and say something are often the first to identify threats. They know their industries and their communities best. Therefore, governments need to actively engage the public to detect, dismantle, and deter illicit actors. By fostering robust public-private partnerships, together we can better counter terrorism and crime at home and abroad.

This is particularly true for threat financing, since funding is the most critical of enablers for terrorism, crime, and corruption. We have witnessed how financial intelligence, economic targeting, and sanctions have helped us to counter threats around the world since 9/11. This is the case of our current campaign against ISIL, where we see momentum on both the financial and military fronts in Iraq and Syria.

Since I last appeared before this committee in May 2015, following the money trail has been instrumental in degrading ISIL's ability to generate revenue and fund its criminalized caliphates. Defense Secretary Ash Carter, as recently as Monday here in Washington, said, "We have seen results in targeting ISIL's leaders and finances through Operation Inherent Resolve. Our attacks on its economic infrastructure, from its oil wells to its stashes of cash, are putting a stranglehold on the group."

As we speak here today, ISIL is on its heels in Iraq and Syria, as Iraqi forces have just begun to liberate Fallujah and prepare to move on Mosul. But ISIL, unfortunately, is proving to be a very adaptive adversary. Terrorism expert Jean-Charles Brisard said that despite constant coalition air strikes, ISIL still has a $2 billion empire. As oil revenues have decreased by 30 percent, it is more reliant on taxation in the territories that it still occupies. Therefore, reestablishing control of those territories is paramount to defeating ISIL militarily, financially, as well as psychologically.

ISIL has expanded its reach beyond Iraq and Syria, as we have seen with the tragic attacks in Paris and Brussels. It is present in 19 countries, including a new caliphate in Libya. And ISIL's influence has reached our own shores. FBI Director Comey says that upwards of 200 Americans have traveled or tried to fight for ISIL. And the FBI has some 1,000 ISIL-related cases open nationwide. It has inspired homegrown terrorists like those responsible for the deadly attacks in San Bernadino and Orlando.

For the FBI and joint terrorism task forces that I train on terrorist financing, financial forensics are a critical component of all of their investigations. While these latest attacks don't cost very much money, the public can assist law enforcement in identifying suspicious activities before terrorist attacks occur rather than afterwards.

Since the 1970s, the U.S. Government has worked with the private sector to pursue financial crimes, like tax evasion and money laundering. Since 9/11, we have seen constructive public-private partnerships. The financial intelligence and information-sharing working group imparts case studies and red flags for financial crimes. Similarly, the Financial Services Information Sharing and Analysis Center disseminates timely physical and cyber threats to alert its members, reflecting the changing nature of the domain that is cyber.

Over the past decade, we have definitely increased our ability to detect terrorist financing, levied effective economic sanctions against both state actors as well as terrorist groups, and raised awareness on how our evolving financial system can be exploited to fund terrorism and crime. But we could do more to thwart future terrorist financiers with the following five measures that I propose.

Number one, integrate the financial instrument of national power more deliberately into U.S. strategies to counter emerging threats. Number two, strengthen domestic and international financial intelligence and information-sharing mechanisms to counter threat financing. Number three, dedicate more human financial and technological resources to those responsible for pursuing terrorist financing across the U.S. Government. Number four, research the drivers of the illicit economy and anticipate how new financial innovations could be used by future terrorist financiers. And lastly, empower the public and private sector, and more importantly, individuals, to actively detect and support our counterterrorism financing operations.

In a chapter that will be coming out in a book that we are publishing called, "Beyond Convergence," next month, I write about something called C3 through P3, and it is that we need to communicate, cooperate, and collaborate through public-private partnerships to counter the complexity of threats and safeguard our national security, whether it is talking about terrorist financing, countering violent extremism, or the new threats that we face in the cyber domain.

Thank you, Mr. Chairman and task force members, for your time and attention, but more importantly, for highlighting the importance of the financial instrument of national power that those of us on this panel have been advocating for the last 15 years. And I look forward to your questions.

[The prepared statement of Ms. Realuyo can be found on page 71 of the appendix.]

Chairman FITZPATRICK. Thank you very much, Professor.

And Mr. Farah, you are now recognized for 5 minutes.

STATEMENT OF DOUGLAS FARAH, PRESIDENT, IBI CONSULTANTS LLC; AND SENIOR NON-RESIDENT ASSOCIATE, AMERICAS PROGRAM, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

Mr. FARAH. Chairman Fitzpatrick, Ranking Member Lynch, and members of the task force, thank you for the opportunity to testify on this important issue of the changing nature of terrorist financing. I speak only for IBI Consultants and myself at this hearing.

I would like to address three main issues today: the emergence of criminalized states; the use of commodities, particularly gold, in the terrorist and criminal financial structures; and the use of offshore havens.

In my 3 decades of focusing on transnational organized crime and illicit money flows, I have found that there is really very little new under the sun. What has changed in recent years is the volume of the streams of illicit money flows in which terrorists and allied transnational criminal organizations can hide their money movements. I believe the emergence of criminalized states in Latin America, Africa, and the former Soviet Union, meaning states where the senior leadership is involved on behalf of the state in transnational organized criminal activity, is a primary factor. The fact that these illicit flows are now embedded within state structures is a key factor in making it difficult to halt such financial flows.

In the Western Hemisphere, it is the involvement of numerous states led by Venezuela in an ongoing criminal enterprise that makes disrupting and dismantling financial networks so difficult. The government of Nicolas Maduro, along with the governments of Evo Morales in Bolivia, Rafael Correa in Ecuador, Daniel Ortega in Nicaragua, and Salvador Sanchez Ceren in El Salvador, grouped under the umbrella of the Bolivarian Alliance for the Peoples of Our America, or ALBA, has actively helped the FARC, Hezbollah, Spanish ETA separatists and other designated terrorists and criminal organizations develop a significant presence not only in Latin America but across the world.

In each of the ALBA nations, as detailed in my written testimony, the leaders control hundreds of millions of dollars that do not pass through the national budget or any other accounting mechanism, and serve essentially as slush funds for the ALBA leadership and their allies in transnational organized crime and, potentially, terrorists.

Within the context of these vast, economically irrational money flows already moving through criminalized states, the growing amount of unusual mining and exporting of minerals, particularly gold in Latin America, must be viewed with concern. The relatively high price of gold, coupled with the ease of movement, placement, and sale, and the striking lack of control over the movement of the commodity make it particularly attractive to both criminal and terrorist groups.

Colombian President Juan Manuel Santos estimated that gold provided $2 billion a year to terrorist and criminal groups in his country, outstripping cocaine as the primary financial asset. While it takes 6 months to grow coca and process a kilo of cocaine, along with significant technical skills, low-cost and low-skill gold mining

in Colombia—in the Colombian jungle can easily yield 2 kilos of gold a month. A kilo of cocaine sells for about $2,570 in the Colombian jungle, while a kilogram of gold can fetch up to 19 times that much. The precious metal is also relatively easy to legalize, while cocaine remains illegal and heavily penalized.

Because the FARC and its allies in Venezuela want to disguise the origin of their gold after it is mined, they often move it through Guyana, Suriname, Nicaragua, and Ecuador to avoid detection of gold entering the market from places that might arouse suspicion of either terrorist or transnational criminal connections. Those using gold often disguise the origin of the gold so that they can avoid detection and paying taxes, thus you have the unusual situation where Peru and others were exporting—they were moving their gold to Colombia and declaring it as Colombian gold as they moved it out so that Colombia on paper was exporting more gold than it actually produced.

The massive leak of internal documents at the Panamanian law firm Mossack Fonseca, now known as the Panama Papers, also gives an unsettling view of just how easy it is to use law firms in certain jurisdictions to incorporate entities where the real owners are never disclosed, and then use those entities to move massive sums of money to offshore havens where the anonymity is not only preserved but enhanced and reinforced.

While privacy issues are real and valid, the current structure represents one of the most glaring weaknesses in the financial structures that are used by a host of illicit actors, including terrorists and transnational criminal organizations. It is easy but dangerous to forget that Al Qaeda and Hamas used extensive offshore structures in the Bahamas to move money around the globe, both prior to and following the attacks of 9/11, something Juan Zarate worked extensively on when he was at the Treasury Department and helped shut down a significant flow of funds at that time.

This opaque world overlaps with the vast unregulated world of gold and other commodity movements, and both intersect in the growing number of criminal state jurisdictions. This amounts to a perfect storm for terrorist financiers and transnational criminal organizations to hide and move cash and cash value across the world in ways that are virtually untraceable.

I offer recommendations on dealing with these issues in my written testimony. And I welcome the chance to answer any questions you may have.

Thank you again for the valuable work of this task force. And thank you for the opportunity to testify again here.

[The prepared statement of Mr. Farah can be found on page 52 of the appendix.]

Chairman FITZPATRICK. Thank you, Mr. Farah.

And thank you to all the witnesses for your testimony here today and your work with the task force, as well as the staff in preparation for the hearings and for the bills that are going to be introduced.

Mr. Cassara, in your written statement, you note that FinCEN's MSB registration process, the money service businesses, have been less than effective. I think you state that they were weak. Can you

identify some specific examples of weakness and then how you would address it, if you were us?

Mr. CASSARA. Just a little bit of background. I was at FinCEN. Before 9/11, the head of FinCEN at the time, Stan Morris, was very concerned about what he called money service businesses (MSBs). He contracted with a accounting firm, one of the Big 8 accounting firms, to do a study. And the numbers came back that there were approximately—at that time; this was about 2000—240,000 MSBs in the United States. Very little was done with that information.

Then, 9/11 happened. The PATRIOT Act was passed. After that, MSBs in this country are supposed to be registered with Treasury's FinCEN, and I think they are supposed to be licensed in 47 or 48 of the 50 States. There are approximately—I haven't been on the site recently—40,000 MSBs that have registered with FinCEN, which means, if that earlier study was correct, that 200,000 are missing.

If you go back to the 2007 national anti-money laundering strategy report, that strategy report says, in effect, that approximately 20 percent of MSBs are registered with FinCEN. In other words, where are the missing MSBs? MSBs, as you all know, are everything from PayPal to mom-and-pop check cashing companies to hawaladars to casas de cambio along the Southwest border. We have not done a very good job of getting them registered. Of course, if they are not registered, they are not filing suspicious activity reports. The program hasn't worked as it was constructed.

Chairman FITZPATRICK. So what would your recommendation be?

Mr. CASSARA. Well, I can defer to my distinguished colleagues here, but the IRS, I believe, has the mandate to work with regulators to go out and ensure that those MSBs are in fact registered. That hasn't been done. In my opinion as well, there should be more outreach to the money service business communities, particularly in the various ethnic communities in this country because, quite frankly, a lot of them don't know that they are supposed to be registered. More work needs to be done in this area.

Chairman FITZPATRICK. Would any of the other panelists like to add anything to that?

Mr. Zarate?

Mr. ZARATE. I think there are three things that could be done, Mr. Chairman. I think one is the outreach that John has talked about. I think there is always awareness-building that has to be done, not just in the traditional money service business sector, as John mentioned, but also with new digital payment sectors, the bitcoin community, et cetera, which now have to register if they are acting and transacting as money service business. So there is a lot of outreach that still has to be done. Education. So that would help.

Second, is the enforcement of the regulations themselves. As I mentioned in my remarks and in my testimony, the need for resources is very real. The IRS has been given the mandate to go out and regulate on behalf of FinCEN. The Bank Secrecy Act in this sector, frankly, they just don't have the resources to do it at the scale to deal with the nationwide sort of disbursement of the sector. Part of that is also enlisting State authorities a bit more. These are State-regulated entities in many regards.

Third, is that money service businesses now have the challenge of having bank accounts. And I think there is something here to be done in the context of financial inclusion, as I had remarked, to work with the formal financial system, in particular the major global banks, as well as smaller regional banks, to try to work with money service businesses, not only to register them, but to make sure that they have access to the financial system, and understand what their obligations are as a regulated entity under the anti-money laundering rules of this country.

So I think those three categories of activities would take us far afield from where we are and would certainly be an improvement.

Chairman FITZPATRICK. Professor Gurule?

Mr. GURULE. Yes, I would add, I think first there has to be a prioritizing with respect to if there are 240,000, at a minimum, MSBs, I think that resources should be spent on identifying the largest MSBs that are moving the largest amount of money annually to ensure that those particular MSBs are registered. One way to ensure that might be, for example, to require that when the MSB files its tax returns with the IRS, it must submit some statement, some affirmative statement, that they are in fact registered with the Treasury Department. So they have an affirmative obligation to state that. And if they fail to state it, then that should raise a red flag. If they falsely state it, then they could be prosecuted for making a material false statement, which is a Federal violation.

Chairman FITZPATRICK. My time has expired.

I recognize Mr. Lynch for 5 minutes.

Mr. LYNCH. Thank you, Mr. Chairman. At the outset, let me just thank Chairman Fitzpatrick and also Vice Chair Pittenger for the great work, and to all the members on the task force.

And I want to say thank you to this all-star panel. You have all been up here multiple times testifying on various issues, cutting-edge subjects in this area. And I just want to say thank you for all the work you have done. As I said before, you have all been up here multiple times. And in wrapping up this iteration of the task force, we really benefited greatly not only from your testimony today but also from your advice, your counsel, helping us to formulate legislative responses to the problems that we have talked about here. And we have some of those that we will roll out after the conclusion of this hearing. But I just want to say thank you for your service to our country, and thank you for allowing us to be the beneficiaries of your expertise.

The members of this task force are well-traveled. My colleagues, there is nobody on this task force who hasn't put in a lot of frequent flyer miles trying to drill down on this problem. We just came back not too long ago from Nigeria and Tanzania. And there are some wonderful, wonderful things being done, Mr. Cassara, with mobile payments, as you mentioned. And it is incredible what is happening in parts of the Third World where, for example, in Nigeria where mobile payments are now financing a solar energy culture there where electricity is being brought into some of the most remote areas of that country. And with the growth of their population, it has been really incredible what they are doing with very small micro payments, but giving these villages in some pretty re-

mote places the ability to import electricity into their homes. It is revolutionizing that country.

But as you all have indicated, it also presents a real problem for us in trying to track the flow of terrorist financiers. And we have done some work up on the Syrian border. We met with—members of this task force have met with a half a dozen—they are a so-called moderate Syrian rebel groups, but I am not so sure how moderate they really were or are. But the bottom line is they are all using WhatsApp and they are all financing their operations. And these are the rebel groups. And I would bet that their counterparties there, ISIL and other groups there, the al-Nusrah Front, are also using the same mobile apps to finance their efforts as well.

So our ability to drill down on this is really—the pace—well, the velocity of change is so quick, it has been breathtaking. And it has been very difficult for us, because just when you think you are catching up, something new will come out. You know, the last thing we looked at was sort of a model of this bitcoin platform that uses blockchain. And now we are trying to catch up to that to see if this presents another area of vulnerability.

Mr. Cassara, in the area of mobile payments especially, and all the panelists, you have all been working on this, what are the single most persistent vulnerabilities that you see there? We had trouble, for example, getting some of the companies to take down sites where we know there has been chatter. In other cases, we also know that there has been work being done on a video game platform. So they go into these chat rooms, and I am sure that there is—finance is a component of what is going on there as well. How do we—what is the most effective way to get at that problem?

Mr. CASSARA. Thank you for the question. I think the largest threat dealing with M-payments is the simple volume of M-payments. For example, according to experts, there are about 1 billion mobile money transactions in a given month. If only 1 percent of those are suspect, okay, 1 percent, so fraud, money laundering, suspect charitable contributions, terror finance, whatever it is, you are talking about 120 million suspect transactions a year. And you think 1 percent is too high? Break it down. Say it is half of 1 percent. So you are talking 60 million suspect transactions a year. It is overwhelming.

And we, the 93 countries where this is going on, don't have any systematic way to analyze the very volume of these things to put in place red flags so that law enforcement, even the financial intelligence units can get involved with tracking these things.

Another tremendous problem, and something I would like to go into a little bit more detail on, is the fact of where these very systems operate. You mentioned Syria, you mentioned Nigeria, the Philippines, Pakistan, Bangladesh, and Afghanistan. These are some of the areas in the world where we have the very weakest law enforcement. And so there aren't any cases. And this is something that we need to address.

Mr. LYNCH. Okay. Thank you.

My time has expired. I yield back. Thank you, Mr. Chairman.

Chairman FITZPATRICK. The vice chairman of the task force, Mr. Pittenger, is recognized.

Mr. PITTENGER. Thank you, Mr. Chairman. Thank you for, I think, a very sobering analysis. And the scope and impact of what we now clearly see through of the transfers from mobile payments, from bitcoin, from gold is enormously challenging.

We have our own structures inside Treasury with FinCEN and OTA and OFAC. And yet, as I shared earlier, we have our allies, our friends, who seek, for the most part, to cooperate with us, but have very limited resources. What else do we need to be doing to support our own agencies and to broaden their capacities to the extent that they can address the issues that were brought up today and broaden our ability to help our friends around the globe?

I was with President el-Sisi last December. I am going to see him again at the end of next week. And he, in spirit, I believe, wants to be supportive. They lack enormous technological support. We saw that, of course, in South America as well. So speak to that and what we need to be doing resource-wise inside our own financial institutions to support them, to address these prevailing challenges, and how we can better support our allies around the world?

Juan, would you like to start?

Mr. ZARATE. Thank you, that is a great and expansive question. I think the first thing we need to do is make sure we have a system that actually ensures transparency and accountability, that then allows the regulators and authorities that are responsible for ensuring that our system isn't being misused by criminals or terrorists, actually can see what is there. And I think there has been a lot of progress this past year with the issuance of the customer due diligence rule from Treasury, something we had talked about a year ago as being necessary. That is incredibly important to getting to the ultimate beneficial ownership of corporate entities.

The beneficial ownership legislation that has been presented to Congress, I think, needs to be taken up and looked at carefully to determine how best to get at who owns the entities in this country that are acquiring vast amounts of real estate, or perhaps even trying to hide their hand in placement or movement of funds. So I think that is critical, first and foremost. There has to be that.

Second, what I mentioned in terms of information sharing, we do have to move to a more aggressive model of information sharing, in particular with the private sector. The private sector is required to help, by law, they want to help, by now, culture and by being hit over the head with enforcement actions. And we need to find ways of enabling them to be the gatekeepers of the financial system, which helps the government regulate bad behavior. So I think that is critical.

And third, I think we need to be more demanding of our foreign partners. The reality is that the United States, for the last 20 years, has been the only country in the world that has an Office of Foreign Assets Control (OFAC) that is responsible for administering and enforcing sanctions. No other country in the world has had a similar entity. And the reality is, we need our partners around the world to have a discipline around the enforcement of these measures, and it is part of the reason why I argue that we need to continue to push the enforcement of these issues and sanctions, in part because we have been put in a position of driving that international agenda and focus. You have seen it with the

FIFA corruption case; you have seen it with sanctions; you have seen it on terrorist financing. That will remain our role, but we need to be demanding of our foreign counterparts, in particular governments and banking centers that do have capacity and resources to do this well.

Mr. GURULE. Domestically, I think that there needs to be a better job of information sharing between the Federal regulators and DOJ. With respect to HSBC, for example, there are multiple instances where the OCC, which was responsible for auditing and ensuring compliance of HSBC with the Bank Secrecy Act (BSA), found multiple violations where the bank was in noncompliance with the BSA. And the question is, was that information being shared with the FBI? Was that information being shared with DOJ? I think there needs to be a stronger partnership between those two agencies.

The Federal regulators are really on the front lines of auditing these banks to ensure compliance with the BSA and counterterrorist financing regulations, and we need to ensure that once they find a problem, once they find, for example, a failure to file SARs, or an ineffective—or they are in noncompliance with respect to having written policies and procedures to prevent terrorist financing, we need to engage and make sure that the FBI is involved in looking more closely to see whether or not that noncompliance has resulted in money laundering, the use of the bank by drug cartels and terrorists.

And then second, something that I spoke to just briefly in my oral statement, the importance of a counterterrorist financing strategy. So to ensure greater coordination, to ensure—between Federal agencies, interagency coordination, to ensure prioritizing, to ensure that we are not only confronting the current threat, but anticipating the future threats and the future methods which the terrorists are going to use to move money globally. We need to be thinking through that, and ensure that we are not simply reacting to the problem and the crisis of today.

Mr. PITTENGER. My time has expired, but I sure would love to hear more.

Chairman FITZPATRICK. The gentleman from Illinois, Mr. Foster, is recognized for 5 minutes.

Mr. FOSTER. Thank you, Mr. Chairman. And thank you to our witnesses.

When I step back and look at this problem, I think of it sort of in two different levels. The first thing is, can we define a world in which money laundering is impossible? And then what are the essential features of such a world? And then to step back again, do we actually want to live in such a world, because of the implications for the costs and the privacy that will be essential for this.

And so to start with the first part of the question, what are the essential elements of a world where it would be impossible to launder money? Okay. I think at a minimum, you have to get rid of anonymous shell corporations in the United States. And is there anyone who thinks that even needs an asterisk? It is essentially mandatory that you not be able to hide behind that. And that is a big part of this, starting by cleaning up our own house first, that we have to make the United States a model for at least inside the

United States, we would not be able to launder money internally. My predecessor in Congress just started a jail term for failing to attempt to launder money and as part of some other criminal activity.

But another essential part of this has to be mandatory traceability of financial transactions. You simply cannot allow electronic financial transactions where the beneficial owner is not recorded, and it would be some kind of crime not to do that. And is there any way around that as an absolute requirement to a regime that would make it impossible? Well, thank you. I think I agree.

And then you have to—because of the volume problem, you are going to have to have the ability to do big data analytics on this in some way that does not cause privacy concerns, which is a heck of a problem and gets to the second part of my question.

Another essential part, I think, has to be authentication, that you have to know when someone claims he is this person, that he is the beneficial owner, that you have to have something akin to a national digital ID card, where you can't cheat on it to know that you actually know the beneficial owner, and have an electronic record of who that person is and it is not some third party.

So it seems to me that all of these are essential just to clean up the financial part and to make it impossible to launder through the financial system. And then, as has been brought up by our witnesses, there are two more steps. You have to internationalize this, which to me means you are going to have to simply deny access to the United States and the world-regulated financial system to any country that doesn't adopt essentially equivalent rules. I think that is unavoidable.

And then, finally, you have to deal with the commodities problem, that everything from Bitcoin, to gold, to hard-to-value assets will have to come under the same regime that I have just described for financial services. This is a very Draconian set of requirements. I think, however, we can waste a heck of a lot of time and money if we define a system that has gaping loopholes in it that people can immediately drive a truck through. And so, it seems to me that we are really facing a binary choice. Do we want to make it impossible to launder money, or do we want to have all of the things I have just described?

Is there something that is sort of wrong with that big picture analysis? Are there things that I am missing in this? I have to say that I am not convinced which road we want to go down, because you are talking about a world where cash is simply not—the benefits of cash where you can have anonymous transactions would not be allowed, at least electronically. And a lot of people, including me, have a lot of worries about going down that road.

Are there big points that I have missed in that sort of binary choice that we have to make? Mr. Farah, you look like you are reaching for the—

Mr. FARAH. I think that is really a good description of what—sort of the macro questions that we are facing. And I think that, to me, there is something of a middle ground in taking away the really easy advantages that illicit groups have in ways that don't impinge on your privacy or your ability to actually conduct business. I think, as John Cassara was talking about, the sheer volume, most

of it for good stuff, there is a threshold at which if you overregulate, you kill business and our commerce comes to a grinding halt.

So I think that things like not allowing anonymous shell corporations, I think that basic regulation of commodities and an accounting of how—for example, why, for a certain amount of time, Colombia was exporting more gold than it produced. Those should raise red flags. That is not rocket science. That is sort of basic due diligence on your commodities and how they move. The fact that in several countries where gold move extensively, you have free trade zones built into the airports, so you can fly gold in, walk it to the free trade zone without ever declaring it, and reship it to another country without it ever transiting in any formal way. That is the most basic loopholes that you can begin to close. I think if you—

Mr. FOSTER. So how rapidly will people—let's say you close those loopholes. Then you have Bitcoin or things like that, and there will be billions of dollars flowing immediately. Are we—

Mr. FARAH. I think the key is to raise the cost of illicit transactions to the point where they are no longer quite so lucrative and quite so easy, and over time, you build up, as we have done with some success in some ways with drug trafficking money, where you began enough regulations that it is no longer that easy, that cheap, and that—and with absolute impunity. You raise the cost over time. And I think, as I think many of my colleagues addressed, that these are rapidly adaptive groups, that you have to be able to think rapidly and ahead of the curve, which is something that bureaucracy is not very good at, but if you raise the cost over time, you diminish the impact of illicit behavior.

Mr. FOSTER. Okay. And I guess my time has expired, but I thank everyone for their thoughtful participation in this, because it is a real decision our society is going to have to make. Thank you.

Chairman FITZPATRICK. The gentleman from Pennsylvania, Mr. Rothfus, is recognized for 5 minutes.

Mr. ROTHFUS. Thank you, Mr. Chairman. I thank the panel for being with us today to continue this serious conversation that we have been having about terror financing. I would like to direct my first question to Professor Gurule.

In your testimony, you discussed the importance of secondary sanctions, and you recommend that the United States both strengthen existing sanctions, and potentially impose new ones, like those in the Comprehensive Iran Sanctions Accountability and Divestment Act of 2010 aimed at the Islamic State. As you know, however, the Joint Comprehensive Plan of Action (JCPOA), commonly known as the Iran Nuclear Deal, actually lifted many secondary sanctions against Iran and created loopholes, for example, regarding the sale of commercial passenger aircraft, which Boeing is already seeking to exploit.

Do you think it was wise for the President to waive these sanctions as part of the JCPOA?

Mr. GURULE. Well, I think that perhaps it would have been better to have waited to decide to lift the sanctions, to determine whether or not Iran is in compliance with its obligations under the Joint Comprehensive Plan of Action. To lift those immediately after the agreement was signed perhaps is questionable.

Mr. ROTHFUS. There are two aspects in dealing with Iran: one is the nuclear; but the other is that it is the world's leading sponsor of terrorism. Wouldn't lifting these secondary sanctions weaken our efforts to combat the world's leading state sponsor of terrorism?

Mr. GURULE. Well, certainly. And let's keep in mind that I think it was the secondary sanctions that really put the squeeze on Iran, and I think forced them to the bargaining table and forced them to agree to make certain concessions with respect to developing their nuclear sector. And then to take kind of that principal leverage that was used against Iran to bring them to the bargaining table and then to lift that, again, raises some serious questions whether or not that was premature, whether or not we should have waited, permitted some time to determine whether or not Iran is going to live up to its obligations under the agreement.

Mr. ROTHFUS. In your testimony, you also recommend that the United States should develop a comprehensive counterterrorist financing strategy. My concern is that the President can't even articulate an actual strategy to combat the Islamic State militarily. It is really not surprising that the Administration has also failed to develop a strategy to counter the financing of such groups.

In your opinion, why hasn't the Administration done this work to develop a plan to cut down on terrorist financing?

Mr. GURULE. It is a good question that you raise. And one possible answer is that it isn't a priority of the Administration, despite public statements to the contrary, and it certainly goes to the question of the effectiveness of the current U.S. Government's counterterrorist financing efforts.

I worked at the Treasury Department. I know how committed those employees are, how hard they work to counter this effort, but I think that their efforts would be enhanced if it was done in a more thoughtful, forward-leaning, forward-thinking, comprehensive manner, in terms of targeting priorities, anticipating future methods of moving money for terrorists around the world, and then there are specific strategies that have been developed in coordination with other important government agencies to combat those threats. So I think the failure to have such a strategy has undermined our overall efforts.

Mr. ROTHFUS. Mr. Zarate, your testimony also talks about the need to develop this comprehensive strategy. Here we are more than 2 years—it is June 2016—since the Islamic State was dismissed by the President as the "JV team." Do you have any insights as to why we don't have this comprehensive strategy outlined yet from the Administration? Any insights?

Mr. ZARATE. Congressman, I think we were caught flat-footed, to be quite honest. I think our withdrawal in 2011 left us blind to what was happening in Iraq. We had established the Iraq Threat Finance Cell in 2006, precisely to look at the financial intelligence and information around how Al Qaeda and other terrorist groups in the insurgency were raising and moving money. That was dismantled, and I think we were caught flat-footed; we just didn't have eyes on the ground, we were no longer looking at it. So I think that is one of the reasons. And think we have been playing catch-up.

And to Professor Gurule's point, in order for sanctions, or secondary sanctions, or any type of tool to work, we have to have the intelligence, we have to understand how these financial infrastructures work. We have to understand who their moneymen are; we have to understand what brokers they are relying upon; we have to understand what the intersection is with the regional and global economy; how money service businesses are potentially implicated. All of that has to be done, and I think we are playing catch-up.

And to Professor Gurule's point, I think we have colleagues at the Treasury Department who are working assiduously and with enormous energy to try to get at this problem, but I think we are doing a lot of catch-up work.

Mr. ROTHFUS. I yield back.

Chairman FITZPATRICK. The gentleman from California, Mr. Sherman, is recognized.

Mr. SHERMAN. There is, obviously, division in any political organization, such as the Administration. It may explain why we are not going after certain targets. There are those in the Administration trying to do everything possible to reduce the economic power of Iran, and now the Administration is considering a $100 billion Boeing jet deal so that Iran will be able to efficiently airlift thugs to Damascus, where thousands of people will be killed as a direct result of that airlift capacity and where hundreds of thousands will be driven into exile as a result of that capacity. Perhaps the biggest terrorist financial transaction will be licensed by Treasury, that is to say, a $100 billion transaction for an airline available to the IRGC for its airlift capacity.

I should also point out that—and this is outside the scope of this task force—when we look at financial problems, it is not just our enemies; it is our so-called friends. If people want to say, why do we have ISIS? We have ISIS because we have Malaki. Why did one of the best equipped and most lavishly provisioned armies in the history of the Middle East not only fade into nothing, but give its weapons to ISIS on the way out, and then leave the money in the Mosul Bank? You have to look at Mr. Malaki and we have to wonder why we ever put him into power.

I want to focus with Mr. Zarate and Mr. Gurule on just how much evidence you need to put an entity on the terrorism list. I think the book, "Treasury's War," says there was once an 80/20 rule. If you are 80 percent sure, put them on. Now, I see an awful lot of IRGC entities that aren't on. And I wonder—you look at what the legal standard is, which is you can put them on unless the courts determine it is arbitrary and capricious. That basically means the law says you get to do almost anything you want to do. I don't know—I think it is incredibly rare that any entity has gone into a U.S. court and said, take us off the list, it is arbitrary and capricious to put us on. Some have appealed to the Administration, but never has the Administration, to my knowledge, been overruled by the court system. So basically, the Administration can do what they want.

Has the thinking in Treasury swung too far in the direction of we need more proof, more documents, more files, and more review before we put an entity on the list? Gentlemen?

Mr. ZARATE. Congressman, the standard is a reasonable basis to believe that the individual meets the criteria of the executive order, and so there has to be a body of evidence. And with the USA PATRIOT Act allowing for the use of intelligence and protecting that information, intelligence can also be used as part of the body of evidence. But you are right, that is the lowest standard in the legal context that you would allow, and the appellate review is obviously the most permissive under U.S. law.

I think three things are at play: one, there has been more reticence to avoid litigation, because there have been challenges, and I think there is a bit of resistance there; two, I think there has been a recalibration as to when to use targeted sanctions most effectively. Is it effective to put people on these lists if they don't have any financial connectivity, don't have any business interest; so a more strategic thinking around how you use the list and for what purposes—

Mr. SHERMAN. Are you saying that there are circumstances where it is pretty obvious they are a terrorist organization, but you just don't bother to put them on the list because they don't seem to have much of a bank account?

Mr. ZARATE. It is not necessarily terrorist organizations, but particular individuals, for example, who may be foot soldiers, for example, in Mosul who may not be transacting, may not be have any financial benefit. And, frankly, one of the concerns that the Treasury has to deal with is banks and financial institutions dealing with a laundry list, as Professor Gurule mentioned, over a thousand STGTs, and the STN list is even longer; so a desire not to clog the system with irrelevant names, or less strategic names. So I think that is a serious issue.

And the third is diplomatically, what makes sense. A lot of times, the U.S. Treasury and the State Department use the list in a diplomatic way to push action, for example, the Saudi government. And sometimes, listing an individual or entity makes sense, and sometimes having a quiet conversation to get the same effect and impact makes sense. And so I think there is some degree of that balance that takes place.

So those would be the three reasons I would give as to why you have seen the phenomenon you have described.

Mr. SHERMAN. Mr. Gurule, should we be listing entities more quickly, do you think?

Mr. GURULE. I think that, as you stated, the legal standard is incredibly low. And then on appeal, if a designation is challenged by the person who has been listed, again, it is a very deferential standard to the administrative agency, arbitrary or capricious. And I would say 99 times out of 100, the designee loses. There are very, very few cases in which the designation is overturned. So it shouldn't be for fear that, oh, we are going to lose this and it is going to be overturned by a Federal judge.

I guess my concern is listing individuals primarily kind of for symbolic value. Okay, now we have listed, we have publicized that this guy is a senior member of ISIS, now he has been out and now the world knows, and so that has some value, but if there are no assets in the United States to be blocked, if there is no evidence that U.S. persons are doing business with Abu Bakr al-Baghdadi,

it seems to me that the designation does not have much value in terms of the objective of curtailing funding. If that is ultimately what the objective is, then—

Mr. SHERMAN. Part of the objective is just to punish and name shame the individual, but I will agree, maybe you don't want to do privates, but a colonel or a general is worth putting on.

I just want to, for the record, indicate that this contract to sell wea-—planes, I was about to say weapons, because that is what they are also, is not $100 billion, but it is tens of billions of dollars. I yield back.

Chairman FITZPATRICK. Mr. Poliquin of Maine is recognized for 5 minutes.

Mr. POLIQUIN. Thank you, Mr. Chairman, very much. And I appreciate you bringing these distinguished witnesses before us, and all the great work that we have done in the past year on this issue.

In a very frightening way, I think we all saw in Orlando that for all kinds of reasons, terrorism has now reached our shores. And this is something a lot of folks have been very concerned about for a very long period of time, so many issues that we have already discussed today. Lacking a priority by this Administration to stay on offense has put us in a very difficult situation, in my opinion.

Ms. Realuyo, let me ask you this question: What impact, if any, would the defeat of ISIS have on a broader impact on interrupting money flows to terrorist organizations around the world who look to harm us?

Ms. REALUYO. We have to take a look at the fight against ISIL in a specific way. And you have seen various Administration officials actually tout the progress that is being made, if we categorize it as a campaign against ISIL in Iraq and Syria. So we have seen that militarily and financially. But what has happened is that the group has actually metastasized, and this is what the fear is, is that they are actually sending people who are—the foreign fighters, we are now up to 40,000 foreign fighters, according to the CIA, who have traveled to Syria to fight alongside ISIS, including over 200 Americans.

Now, the problem that we have is that return of the foreign fighters, and I know several of you serve on the Homeland Security Committee, where that is the concern that we have. Then the third batch that we are worried about is the fight in the Levant, then those who are returning to places like Brussels and Paris. And the third iteration, which sadly we have seen here in the United States, are those who are inspired.

I think the victims and the families of victims of any terror attack are not making this distinction between ISIL-directed and ISIL-inspired. I think a lot of us are kind of caught up with what was the categorization of, sadly, the attack in Orlando or San Bernardino. The effect is the same, right, if we think of terrorism defined as the act of violence against innocents for a political or ideological or religious cause.

What we are seeing, though, is that even if we were to defeat ISIL, which is very important, there are three phases of the campaign against ISIL. There is the physical, which is the military. There is the financial, which actually has done very well in the last year since I last appeared before you. They are down year on year,

about 30 percent. And as we know, they need money to actually pay the foreign fighters and then, more importantly, sustain its caliphate.

And then the psychological one is what I think is now really coming to the forefront of the average Americans. What does it take and how are these people inspired so far away in basements across the United States, or in the U.K., or in France, or in Brussels? This is the question that we have to ask.

What is important is that defeat of ISIL, because of its ability to propagandize, and then, more importantly, inspire and train, which is what we saw in the case of the European attacks, foreign fighters who will then return to their home countries to wage jihad against their local populations. So it is a very complex issue that really has metastasized in a way that not just the United States, but other countries across the world now are trying to grapple with, this idea of homegrown versus ISIS-directed, and then, more importantly, the fight that we see now on the ground, particularly in Iraq. In the last couple of days, we have seen the Iraqi forces take up arms, and are actually trying to clear and hold parts of Fallujah.

But the financial piece—and to address the other question: So in the White House strategy of November 2014, there were nine lines of effort, and line number five is disrupting ISIL's financing. When we take a look at grading—since I am a professor, we grade, right—the nine lines of effort, the military and the financial have actually—we have seen progress on both fronts, but as we have seen, these attacks don't take a lot of money.

So you have to really keep fighting the fight physically, financially, and more importantly, psychologically. And I know that there are other hearings on the Hill this week that are looking at this concept of countering violent extremism, both here in the United States and abroad.

Mr. POLIQUIN. Mr. Cassara—if I may, Mr. Chairman. If you could pick one thing, one thing only, what would be your primary issue to interrupt? What would have the greatest impact, based on all the hearings that we have had and all those that you have participated in, all the work that you have done in your career, the one thing that would have the greatest impact at interrupting money flows to terrorist organizations, what would that be?

Mr. CASSARA. The thing that I would like to see the most, and it impacts more than terror finance, I would like to see trade transparency. We talked about this in the previous hearing. I think it is doable. I think the time is right. I think it impacts terror finance; it impacts underground finance; and it impacts revenue streams for governments. I think the time has come to aim towards international trade transparency.

Mr. POLIQUIN. Mr. Zarate, same question to you, sir.

Mr. ZARATE. Without a doubt, disruption and dislodgement of terrorists' control of resources and territory that they use to develop diversified portfolios and war economies. Groups that occupy real territory in urban environments not only are able to tax, develop trade schemes, exploit the resources, but they also use those environments to serve as an economic shield.

We have been reluctant to be more aggressive in Mosul precisely because we have to worry about the day after, and we have to worry about the financial and other infrastructure of that city. The reality is ISIS has used that city to fund itself, and to use that as a hub, along with Raqqa and its control of other cities, to develop a war economy. That is why some estimates have them raising $2 billion, and even with our best efforts, they continue to raise hundreds of millions of dollars. And so, I would say, whether it is ISIS or Al Qaeda or the FARC or Hezbollah, their ability to actually leverage resources and territory is probably the most fundamental thing you can do to disrupt terrorist financing today.

Mr. POLIQUIN. Thank you very much.

Mr. Chairman, I appreciate it very much. I yield back my time.

Chairman FITZPATRICK. The gentleman from Arkansas, Mr. Hill, is recognized for 5 minutes.

Mr. HILL. Thank you, Mr. Chairman. And thank you and Congressman Lynch for your significant leadership, and I appreciate the ranking member and the chairman of the full Financial Services Committee in sponsoring this task force, because I think it has been so important, and I think it has been a demonstration really across the Congress of returning to something that was a tenet of mine some 30-plus years ago, which was a strong, consistent, bipartisan view on foreign policy matters. And I want to thank Mr. Lynch and Mr. Fitzpatrick for demonstrating that in this matter, and thank the staff for their hard work, since they also have other things to do here at the Financial Services Committee. And thanks to our panel for coming back and for your full participation over the last year.

I just can't help but react to some of the commentary. You know, I think the issue that terror finance has really not been on the radar screen of this Administration until more recently is due to what I think is an a la carte NSC process that has thwarted the best judgment of our professionals at the State Department and our professionals at the Department of Defense. And it is not my opinion, it is Leon Panetta's opinion, it is Bob Gates' opinion, it is the Joint Chiefs' opinion, and therefore, we have been behind the curve on so many of these issues, as my friend, Mr. Sherman, noted.

And one of those we have been behind the curve on is terror finance. If we had had a better process in working with the Iraqis, I don't think we would have seen the explosion of ISIS out of Syria into Iraq, and by not reacting, they got the terror network they have today. If we were doing today what—2 years ago or 3 years ago, they would not have the terror network that we are so concerned about. So since San Bernardino and Paris, I do commend the Administration for changing the rules of engagement, including terror finance targets as military targets. It is something I think we talked about in our very first hearing of this group.

Well, as everyone on the panel knows, I have a pet project in this terror finance arena, and so I would like to get some views on it. First, I commend the Treasury's draft on eliminating this foreign-owned, single-member LLC issue. I think that is a good catch, one I personally didn't know about, that they didn't even register to get

a taxpayer ID number, so I think that is an important catch and will have lasting benefits.

Mr. Zarate, as we have talked before and as we have had testimony on this panel, we have talked about this issue, though, of beneficial ownership, and the Treasury proposal, in my view, sort of misses the mark, because it is too broad, it is 24.9 percent or 25 percent, it is relying on the usual suspects, i.e., the banks to sort of police it and basically report it through a SAR process, which is good, or okay, but it is extremely cumbersome, paper-based, burdensome on small institutions, I think way after the fact, not very timely, and I don't think will be effective, and it will end up being a major new paper-shuffling exercise.

But as I have argued in here, I think the IRS data and sharing the IRS data, particularly now that we add single-member non-citizen-owned LLCs is the most robust way to have a single data source that is all digitized, and it is already in the possession of the Federal Government.

So how do we add properly in 26 U.S.C. 6103 the ability for FinCEN to have access to the ownership information you find on a K-1 for an LLC and maintain privacy rights and follow our normal procedures? I will start with you, Juan, if I might.

Mr. ZARATE. Congressman, thank you. And I know that you have been focused on this issue for some time. I think you have to create a particular carve-out for the IRS to be able to share this information. And to your point, the information doesn't do much good if it is locked up in an archive and isn't made available to those who actually have to regulate and look for problematic trends, individuals, and networks.

I would also say there has to be a way for the markets to actually understand with whom they are doing business, and so, there should be some sharing of the burden. I agree with you, the burden shouldn't always be on the banks to have to determine ultimate beneficial ownership, but that does then put the onus on corporate registration regimes and entities, including at the State level, to actually understand and to have available information about corporations and LLCs that are based in those jurisdictions.

So I don't disagree with you, but I think there has to be a very specific carve-out to protect privacy and civil liberties, but it has to be real time, and there has to be some market mechanism by which market actors can share information about who their customers are, because ultimately, we want banks, financial institutions, regulated bodies to understand who they are doing business with.

Mr. HILL. I will yield back, Mr. Chairman, and go another round if you have one. Thank you.

Chairman FITZPATRICK. The gentleman from Kentucky, Mr. Barr, is now recognized.

Mr. BARR. Thank you, Mr. Chairman, and Ranking Member Lynch. Thank you for your leadership on this task force over the last year. This has been an important exercise in determining how we can better disrupt and degrade terrorist organizations through the financial streams that seem to end up in terrorists' hands. And thank you to the panel for your insightful testimony.

I wanted to focus a little bit on this Orlando attack, because the FBI has said to us in the aftermath of this tragedy that these are the kinds of attacks that are the most difficult to disrupt, the most difficult to detect, a lone-wolf scenario, a self-radicalized individual for whom normal intelligence gathering efforts are incapable of disrupting these kinds of lone wolf attacks.

So outside of the Bank Secrecy Act, or referencing the Bank Secrecy Act, is there anything that Federal law enforcement can do to identify financial transactions of individuals who are on watch lists that could maybe detect, before a tragedy like this, individuals who might engage in this kind of activity? Does anyone want to weigh in on that?

Ms. REALUYO. I think, sadly, the Orlando attack shows that people did see something and say something, well beyond the financial piece. So from what we know that has been disclosed through the reporting and open sources, he obviously transferred the deed for a very small value. Someone had to actually do that transaction. It is not a banking transaction, but there were probably lawyers involved.

The other thing as well, our system, because of this $10,000 threshold, we are always looking at the nature of the transaction as opposed to these kind of what I call institutionalized levels.

So the other thing I study is transactional organized crime, and, sadly, we have seen human trafficking as a scourge that is really dealing with the migration patterns through the Americas, around the world. A lot of those transactions are below that $10,000 threshold. But we also need to see and figure out, and that is what I wrote my testimony on, is how can you actually have the public who do see something, say something, know how to approach law enforcement or the government, whether they work at a bank or another financial institution, or some sort of interaction where they can actually take their complaints and, more importantly, their suspicions in a safe way to those who could prevent the next Orlando or San Bernardino.

We saw this too. I had the privilege of going and working with the L.A. Joint Terrorism Task Force the day after the San Bernardino attacks, and it was pretty interesting to see that after the attack, a lot of the neighbors were saying, well, we saw suspicious things taking place, but we didn't want to say something.

So I think it goes beyond just financial services, but if we can actually educate our public and, sadly, we also have a new generation. So my students at George Washington University who just graduated, they were children on 9/11. For them, it was a movie. We all know exactly where we were and, more importantly, we were inculcated in that culture of see something, say something, and we have to get the next generation to be just as aware that these people have this intent, irrespective of what the motivation is, and want to use violence against innocent people.

Mr. BARR. To follow up with any of the other witnesses, in the financial system, is there a blind spot? Is there something that we are not doing in our financial system that we should be doing to help identify suspicious financial activity that might tip Federal law enforcement to weapon purchases, things like that?

Mr. GURULE. I think it is difficult, because, again, the lone-wolf terror attack does not involve a lot of money. These are financed with a few thousand dollars at most. I can't imagine that the Orlando shooting cost Mateen more than that. And so I think it is very difficult to identify any financial transaction that would alert or raise some red flag, and then cause law enforcement to react. But I am concerned about people who have knowledge of someone who is going to commit a terrorist attack, such as the wife and other associates of Omar Mateen, and there is no legal obligation to disclose that information to the police.

It is interesting, however, that if you are a schoolteacher, you have to disclose information regarding a child who has been physically abused, or you believe has been sexually abused. If you are a nurse or a doctor, you have to disclose that to the police, but if you are a citizen and you have reason to believe that your boyfriend or close associate is going to launch a terror attack, you have no legal obligation to disclose that to anyone. You have not committed a crime by keeping that information to yourself.

And by the way, if you provide that person some money, let's say for benign purposes, or some other material support, that isn't even a crime. Under the Material Support statute dealing with lone-wolf terrorists, it is only a crime if you provide the material support knowing or intending that that support will be used to commit a violent crime. So if you provide it for a benign purpose, you haven't committed a crime, and you are not prosecutable.

And so one of the recommendations that I made is that I think that those particular statutes, 2339(a) and 2339(b), need to have a lower scienter like 2339(b) that says, if you knowingly provide material support to a foreign terrorist organization (FTO), regardless of your intent, that is a crime. And I think that we need to bring those two statutes in line with 2339(b), and I am not saying eliminate the knowing or intending, but make it a lesser crime if you have knowledge that the person is a terrorist, or about to commit a terrorist attack, and you provide that person material support.

Mr. BARR. Thank you.

Chairman FITZPATRICK. The gentleman's time has expired.

We are going to go to a second round of questions. And the gentleman from North Carolina, Mr. Pittenger, is recognized.

Mr. PITTENGER. Thank you so much, Mr. Chairman. I really appreciate your leadership on this important task force.

One reference to Mr. Poliquin's statement and inquiry dealt with the data, and your response, I believe, Juan, was that we have legislation that hopefully will get passed before we break, to collect data from Customs and Treasury and Commerce, bill of lading and other export-import data, and then assimilate that and then provide it to FinCEN and other departments, so Customs and others. So at least we are moving that direction on that.

Ms. Realuyo, I would like to ask you, and Mr. Farah, your thoughts in terms of the nexus between the criminal element and the terrorist. I know that you are getting ready to have a conference in that regard. And just speak to that issue, if you would.

Ms. REALUYO. Several years ago, Doug and I began taking a look at this convergence of terrorism and crime. Traditionally, terrorist groups have state sponsors, and there are still state sponsors that

do exist, in the case of Iran supporting Hezbollah, but what we have seen with contracting Al Qaeda core, which was basically funded by donors, as opposed to what we see now in terms of ISIL and its other affiliates, Boko Haram, Al Qaeda in the Islamic Maghreb, they are actually reliant on criminal activities to support and sustain themselves, and some groups have actually moved away from the terrorist aspirations and just become criminal groups.

What we are seeing, then, is an actual need now to combine those who are doing the law enforcement, military intelligence, information gathering, and then, more importantly, operations to counter crime and counter terrorism in a much more interdisciplinary and interagency way.

So the way we are looking at this is actually we refer to them now academically at the National Defense University as illicit networks, which will also include nuclear proliferators, as well as all of their facilitators. And this is what we are trying to do, is when you take a look at—and Doug can speak much more in depth about this, drug trafficking transactions are actually supporting terrorist groups, as we have seen through the Lebanese Canadian Bank, is that case was briefed to you all here before, but this question that we were limiting ourselves by having silos of excellence here in Washington, right? Those who did counterterrorism only looked at terrorist groups, and those who worked on crime or drug trafficking were very siloed.

What we are seeing now is that our adversaries who threaten sovereignty and, more importantly, our economic viability, are actually joining forces, if not becoming these hybrid groups, and that is the case when we take a look at things like the FARC, Hezbollah, Shining Path, and then, more importantly, the metastasis of ISIL, which is really an auto-financed group, it is something we hadn't really seen before, that has actually created its own territory across two countries.

I defer to Doug, who can go much more granularly into this convergence that we have actually seen on the ground.

Mr. FARAH. Thank you, Celina.

I think it was in the early days a few years back, there was a lot of resistance to the idea, because the idea was that terrorists didn't care about money and criminals didn't care about ideology or whatever was diving terrorists. And over time, it became abundantly clear, and I think in the early days, Juan and John and others were working on in the policy world and on the ground seeing exactly how, for example, Al Qaeda was able to use blood diamond flows controlled by Hezbollah in West Africa to move and hide their value. And as you see that I talked about today, gold and other things are available to them. And it doesn't matter anymore on the ground really what you belong to if you are—because so many groups are in the money-making business together. And I think that goes back to one of the points I was making in my testimony about states that allow this or protect transnational organized crime as instruments of policy.

So when you have Venezuela using the FARC, which is both a designated terrorist organization and a major drug trafficking organization, as an instrument of their foreign policy and allowing

them safe harbor and constructing in their country a safe space where Hezbollah can come, where multiple other terrorist organizations can come, learn how to benefit from the drug trafficking and exchange methodologies and thoughts, then you have an entirely different level of complicity and convergence in ways that are very, very hard to disentangle.

Mr. PITTENGER. Can I ask you a quick question? Do you have a concern with FARC, the agreement between FARC and Venezuela?

Mr. FARAH. Yes, sir, I do. I would say there is a potential, there is a template that other groups have followed that I think that the FARC is very well advised on and is likely to follow. I think the primary leader, or the designer of the template are both the FMLN in El Salvador and the FSLN in Nicaragua, where they learned that they could take control of the state. Hugo Chavez and Fidel Castro are not exempt from this as well. They also are the brains behind how to move into the process as a political force, get rid of all the moderates in that political force that you create, and go almost directly into illicit financing mechanisms to perpetuate yourself in power with the complete absence of accountability.

I think in my written testimony, I noted that, for example, Daniel Ortega has acknowledged that he gets about $500 million a year from Venezuela, supposedly from the sale of oil, which is not nearly that much, which is essentially his personal slush fund. It doesn't—it is 20 percent of the national budget that is not allocated in the national budget in any way and which there is no oversight.

In El Salvador, you have Alba Petroleos, which is generating, by their own accounts, $1 billion a year, which is 23 percent of the national budget, which does not go through any appropriations process, any oversight whatsoever, and is simply the slush fund of senior party leaders, who have deep ties to the FARC, which allows the FARC to move money out and launder it through their state structure.

So I think that is an enormous problem, which the FARC is going to take full advantage as they move forward, because I think at the end of the day, one, it comes down to one's assumptions. The FARC are genuinely interested in becoming—incorporating into the peace process and joining the democratic process, because that is what they believe, or is it an extension, is the peace process an extension of their political agenda to take power and hold it over a long period of time? I believe the latter.

Mr. PITTENGER. I thank each of you for your invaluable insight and assistance.

I yield back.

Chairman FITZPATRICK. The ranking member, Mr. Lynch, is now recognized.

Mr. LYNCH. Thank you again, Mr. Chairman.

Professor Realuyo, in your remarks, you identified those five or six points that you really got to focus. I want to talk about point four, which is enhancing our financial intelligence in some of these areas, and especially Iraq and Syria where that is going on.

We have a bill that I think has four Republican Members and four Democratic Members here, to establish basically a reward system that allows and enables the Secretary of the Treasury to prepare a reward system for intelligence coming out of that area. One

of our great difficulties is that we don't have boots on the ground in a lot of these spots. You are right, it is a very unique auto financing system, they have control of territory, and we don't have a whole lot of information coming out. So one of the thoughts was to, and not only in this case with ISIL, but with other—I think Mr. Cassara has described them as criminalized nation states, being able to get information through whistleblowers or people who will come forward.

Do you think that is a practical approach to try to incentivize some greater intelligence capacity within our partner states, and also with insurgencies that are going up against Bashar al-Assad and some of these other, more criminalized nation states?

Ms. REALUYO. What I think you are referring to is something we call Rewards for Justice, a type of model. And it actually worked in terms of the very beginning of our engagement in Iraq to find Saddam Hussein and his sons. And actually, those who helped identify and locate Saddam Hussein are now living in the United States as their reward for justice. So it is an interesting way to complement the types of things that we are doing on the financial front, but also internally, we still need to invest a lot more in terms of those who are within our U.S. Government on how to use and then, more importantly, validate that type of information that might be coming, because if it is just a question of, like, we call confidential informants that we use throughout law enforcement agencies, such as the DEA, we have to figure out a better way to do that.

So the question is, how do we enhance our own intelligence capabilities, whether they be in our military or across the greater and broader U.S. Government, on how to keep up with—and this is the thing, I think, most of us are quite concerned with. I know Juan and I have talked about it.

Financial innovation and financial technology is moving at an unprecedented pace, and unfortunately, a lot of the talent and those who can detect the backdoors to these very constructive technologies that help us, whether they be virtual currencies or mobile payments, we need to get that kind of brain trust into the U.S. Government to help us take a look at these new anomalies. And that is what we are looking at, more ways to proactively promote public-private partnerships, which has been embarked, by the way, in the area of cybersecurity, because the firms that we are working with really understand the cost of these cyber breaches, we should impart that into financial services and the broader sector with the same aplomb as we are doing in the cyber sector.

Mr. LYNCH. Great.

And, Mr. Zarate, you have had a good perspective inside Treasury. One of the frustrating parts for us on this committee is when we—we were in the Gulf recently, and we got—one of our Treasury attaches is trying to interface with the FIUs in those areas. We have one young agent there who is handling five different countries. So we are understaffed. And with the complications with money coming out of the Gulf going up to Iraq and Syria, it is a real problem.

We have a bipartisan amendment to try to push through some more money to FinCEN and parts of Treasury that would deal with

that, OTA and other departments. How critical is that to—as the professor pointed out, we are in a competition for this talent, and the folks who are really, really keen on some of the cutting-edge technology in the financial services area are being pulled away by big money, understandably, by the private firms, and that is why these partnerships are so important.

How critical is it to make sure that we get the resources to hire the people, and especially with—as Mr. Gurule has indicated, I forget how many money service businesses are out there, but just to get coverage on that, how important is it to pump more money into FinCEN and Treasury so that we plus-up our capacity within the government?

Mr. ZARATE. I think it is incredibly important. And I think you are right that we have been under-resourced in a whole range of areas in this domain for a good period of time. And I will tell you that what you saw out in the Gulf was actually leaps and bounds beyond what we had when I was there, when we were fighting for budget dollars just to put one attache out there. Now you have, I think, three in the Gulf region. But I think you are absolutely right. The international presence has to be deeper. The technical expertise has to be present, and you are right that the market itself is sucking the expertise out of the U.S. Government. I work a lot with the private sector now on the outside, and a lot of these major global banks look like Treasury alumni associations—

Mr. LYNCH. Yes.

Mr. ZARATE. —and all of the key global compliance officers are all Treasury alumni, and for good reason—

Mr. LYNCH. Yes.

Mr. ZARATE. —for good reason, but it does demonstrate that there is a real demand in the private sector and in the public domain.

A final point: I think we now realize, and this comes from the years of experience that is represented on this panel, that these issues are not just critical to financial regulation, but they are central to our national security. And we have underinvested in this domain, both in the context of our tools and resources, but also our long-term strategic thinking in this domain. If you look at this compared to our DOD dollars, and those are important, I am a huge fan of our kinetics and our military force and projection, but if you look at it in comparison, it is miniscule, when in many regards, this is a key asymmetric power for our country, and we need to be thinking strategically, we need to be adapting quickly, and we need to contend with the fact that our enemies are thinking pretty creatively around our controls and our power, and that starts, first and foremost, with the office we created, the Office of Terrorism and Financial Intelligence, they need to be resourced.

Mr. LYNCH. Thank you. I know I am over my time, and I appreciate the chairman's indulgence, but just to put a finer point on the talent cycle here, even here on our subcommittees and task forces, Treasury is hiring away our staff, because someone else is hiring away their staff. And so, I guess it is—

Mr. ZARATE. Robbing Peter to pay Paul.

Mr. LYNCH. There is just—we have to train a lot more people on the things we are working on, but I am preaching to the choir here. As a group, you have been tremendous on this stuff.

I yield back.

Chairman FITZPATRICK. The gentleman from Arkansas, Mr. Hill, is recognized.

Mr. HILL. Thank you, Mr. Chairman. Just before I switch subjects, if I could return back to this issue of beneficial ownership and just continue my visit here on that.

So I understand the States and State incorporation laws, and there is a lot to be done there, and I am for any innovative suggestions on that. But still, regardless of that, whether I incorporate in Delaware or I incorporate in Arkansas, if I have an LLC, and it is domestic, I have a taxpayer ID number. And every year I file a balance sheet and K-1s for all those investors, at every percentage, not 25 percent, but at .9999 percent.

Therefore, I think it is a superior support with also a legal basis that it has to be accurate or you violated Federal law. Whereas, the statutes on, do I fill out my LLC information form with the Secretary of State, I am not sure how imposing that is.

So I would like other members of the panel to kind of react to Mr. Zarate's and my little colloquy we have had. Any other thoughts on this subject?

Mr. GURULE. I would add simply that, again, it seems to me that it is a critical component of know-your-customer. Know-your-customer has been a fundamental principle guiding transparency with financial institutions through the Bank Secrecy Act for decades.

Mr. HILL. Right.

Mr. GURULE. And I think that it is really part and parcel of that. I don't think that the principle of know-your-customer is being fully implemented if we don't know who the beneficial owner is of the particular company that is the customer of the bank. We have a CIP program that again requires—regulations require a customer to identify itself, and his name and address basically. And I don't think that goes far enough.

And so I think to fully implement the requirement of KYC to fully understand who you are doing business with, we need that information. And I don't think that it is an unreasonable request to impose on banks.

Mr. HILL. Fair enough. And I don't—I can understand that point of view. And people already have that Gramm-Leach-Bliley obligation. It is a legal obligation they have. They have an obligation to file an SAR when they see something that merits that. So those are already in place. In other words, they should know their beneficial owners, particularly in a credit situation. I would argue they know them all intimately because of the guaranty process to get that credit facility put in place.

But I am up here at a macro level saying, if I was trying to collect big data and I wanted it in a consistent format, and use some discovery techniques that are consistent with the Fourth Amendment, all this talk about whether the banks have it digitized or it is in paper in their files and all is, you know, a more—it is less robust than an IRS solution if I were looking for the needle in the haystack. So that is my comment on that.

Anybody else want to go there? Probably not. Good. I have worn you out.

So let me, if I could, switch to—well, let me do one thing before I switch to Section 314. How about the idea of a utility format for this data repository at the state level? We have automated secretaries of state, we have paper-based, we have robust Internet accessibility. I would still argue it is not timely and it is not impressive. But we can automate it.

So what about a utility-type structure? Mr. Zarate, do you want to start with that, and then others, to tackle this beneficial ownership issue?

Mr. ZARATE. Congressman, I think the utility model is incredibly important to pursue, not just in the context of ultimate beneficial ownership information (UBO), but more broadly to provide a new model for how the anti-money laundering system itself works.

I think we will talk about 314 in a second, but the reality is the current system is very much stovepiped institution by institution, transaction by transaction. We are now moving into an age when not only can we deal with big data, but we have potential use of AI technologies, the ability to collect data and analyze it in ways that are helpful not only to look at the past but also even predictive ways. And there are ways of collectivizing the risk and looking at vulnerabilities across sectors, as opposed to just one institution at a time.

And so to your point, I think a utility for purposes of State registry of corporations and ultimate beneficial ownership, is a great idea because people need access to that information, be they a bank or a car dealer or another regulated entity. But more broadly, and I think a big idea that stems from this, is we need to think aggressively about how we use new technologies to actually make this system more effective, to use the data we have. We have a lot of data. And it is part of what this task force has been looking at. And to use that technology to actually protect privacy and civil liberties, while also making the information more valuable on a real-time basis.

So we have talked a lot about this over the years, but there is now an opportunity, given the technology, to create a sense of a utility not just around particular data points, but around the entire system itself.

Mr. HILL. Thank you.

Mr. Chairman, may I have—would you yield me a minute?

I just want to touch on 314 about this issue of collaboration, Professor Realuyo, you mentioned—do you anticipate that the best approach to that is another center like our center in Pittsburgh on cyber or do you view it as just statutory protections that allow collaboration when it is needed? What do you think the best way to achieve collaboration is from our point of view as legislators, where there needs to be a framework, some sort of a legislative framework change made?

Ms. REALUYO. I have my lawyers here. But the real problem, and more importantly, we have been working on at our agency on counterterrorism and countercrime issues. You have to—on top of having actual requirements for information sharing and mechanisms for really timely information sharing, because we see now

that our adversaries are moving in milliseconds. And if you are aware of an app called WhatsApp that the rest of the world is using, you can really send instructions quite quickly. And we are only catching up in terms of this piece.

You have to create this culture of sharing. And I think it has taken—for example, the military, for jointness, it has taken decades for them to actually become what they call purple. So we need to incite, and more importantly, when we are looking inside the tragedies like Orlando and San Bernadino, highlight the fact that we are not sharing at light speed, even though our adversaries are operating at light speed, and then use legislation that compels and create mechanisms.

So you have to have the actual legal framework, and then within the legal framework, have the institutions who have—led by people with political will to actually enforce that legislation, and then have these actual mechanisms that can incorporate real-time data and information, and then pass it along to those in law enforcement or in the intelligence or military to actually act upon it.

We have greatly improved in the last 15 years since the tragic attacks of September 11th, but we have to see how these different facets help us to achieve the mission of countering terrorist financing.

Mr. HILL. Would any other panel members like to comment on that?

Mr. ZARATE. I can weigh in and defend Celina, if you like, sir. A couple of things—I think the Pittsburgh Center is an important model because it creates a discipline around the information sharing that is more than just sharing one piece of data at a time. It is about looking at trends, looking at particular cases.

In the U.K., they are experimenting with a model called JMLIT, which is a joint money laundering task force that is actually combining the private sector and the public sector in a more aggressive way. So I think more aggressive information-sharing models work.

One thing to keep in mind—and I know this task force has traveled a lot and has great influence when you meet with counterparts. One of the restraints internationally, though, is in laws around the world that prevent the sharing of customer data and information, even within a global institution. So a major global bank, let's say based in the United States, can't necessarily see on a real-time basis information about a customer or a transaction that happens in Malaysia or that happens in Turkey, in part because there are restrictions as to how that data can flow outside the borders of that country.

In a global enterprise, when we are asking institutions to manage their risk and where we want real-time information sharing, that is a 19th Century model for how we manage risk. And I think we have to take that up not only internally, but also with our counterparts around the world.

Mr. HILL. Thank you, Mr. Chairman. I yield my time back.

Chairman FITZPATRICK. The gentleman from Arkansas, Mr. Hill, has yielded back. And with that, the time for all questions has expired.

I also want to again thank our witnesses for their testimony, not just today, but for your willingness to appear before this task force

on multiple occasions and for providing your expertise even between hearings.

One of the things we tried to do with this task force was recognize the body of sort of your life's work, what you do each and every day, which is think about and work to protect our country, the citizens, the economy, and bring that focus back here to the House Committee on Financial Services.

And one of the other goals I had for the task force was to make sure that, as we look back at the work between the members of the task force and between parties, that there would be no light between us, since we are all singularly focused on the goal of chasing down terror finance, cutting it off, and keeping our country safe. And that occurred largely as a result of the work of Ranking Member Stephen Lynch, who has been really an incredible partner throughout this process. And I want to thank Mr. Lynch for his work.

And the work that we have going forward, we have a series of bills that are going to be coming out here.

And finally, I think the witnesses would all recognize that the work we do is supported by a lot of staff back in the office. They are the ones who keep the wheels turning. And Joe Pinder—when this idea was first brought to the Committee on Financial Services and presented to Mr. Pinder, not only did Joe immediately embrace the idea of going forward with this task force, he had already in his mind been thinking about this for some time; this is something he has a special interest in, and he has brought an incredible expertise to this.

And so, Joe, I want to thank you for what you do, what you have have done for the task force, what you do for our committee, and have done for our country.

But the members of the task force have committed a lot of time and effort over the course of the last year. I see French Hill is still here at the very end. And French has never missed a meeting, and has been an incredible resource with his background both in the Administration and now as a Member of Congress, as well as in the financial services sector. He is laser-focused on the issues, not just the ones he talked about here today, but the ones he has been talking to us about for the last more than 12, probably 18, months as we went through this work.

So with that, I just want to again thank the witnesses for what you have done for us. We are going to keep in touch. When the report comes out, that will be a result of staff work. There is a series of bills that will be introduced very shortly. And as those bills are introduced, it is our commitment to the witnesses to keep you engaged with us as we ask for your support. We believe these bills are as bipartisan as the work of this task force has been, and we hope to see them on the Floor soon and hopefully over to the Senate after they pass the House of Representatives.

The Chair notes that some Members may have additional questions for this panel, which they may wish to submit in writing. Without objection, the hearing record will remain open for 5 legislative days for Members to submit written questions to these witnesses and to place their responses in the record. Also, without ob-

jection, Members will have 5 legislative days to submit extraneous materials to the Chair for inclusion in the record.

With that, and without objection, this hearing is adjourned. Thank you very much.

[Whereupon, at 12:20 p.m., the hearing was adjourned.]

A P P E N D I X

June 23, 2016

John A. Cassara

Written Statement for the Hearing On

"The Next Terrorist Financiers: Stopping Them before They Start"

Before the

Task Force to Investigate Terrorism Financing

Of the House Financial Services Committee

June 23, 2016 at 10:00 A.M.

Chairman Fitzpatrick, Ranking Member Lynch and members of the Task Force to Investigate Terrorism Financing, thank you for the opportunity to testify today. It is an honor for me to be here.

On February 3, 2016, I was similarly honored to appear before this Task Force to testify on a topic of great concern – trade based money laundering and value transfer.[i]

I am pleased to note that as a result of the referenced hearing, there has been additional focus on trade-based money laundering (TBML) and its links to terror finance. I am also heartened that the Task Force has explored some of the recommendations in my testimony.

The focus of today's hearing is to summarize findings but also identify emerging terrorism financing threats so that we can act to mitigate coming dangers. So this morning, I would like to shift my focus away from TBML and take this opportunity to discuss another topic that I have also been concerned about for many years. It is already dramatically transforming financial services in areas of the world in which our adversaries operate.

• • • • • • • • • •

Exponential Growth

In 2008, I wrote an essay published by the Department of State titled "Mobile Payments – a Growing Threat."[ii] Eight years later, the threat has materialized.

Mobile payments is actually an umbrella term that covers diverse high-tech money transfer systems such as digital precious metals, Internet payment services, prepaid calling cards, and M-payments (i.e., money and e-value transfer via the use of cell phones).

(Note: I am limiting my remarks to mobile network operators where transactions are generally processed over the operators' wireless network/s. I will not address mobile payment services offered by financial institutions or the mobile payment service provider model where the provider offers mobile payment capabilities to its service users which may include merchants.)

The growth of access to cellular devices is breathtaking. In 1990, there were approximately 11 million mobile phones worldwide.[iii] In 2016, the number of mobile lines in service has surpassed the global population![iv] By 2010, more people will have mobile phones than electricity and running water.[v]

The GSMA, an organization that represents the global mobile industry, estimates that there are now approximately 411 million mobile money accounts in the world. The total was increased by almost a third in 2015. There are approximately 270 mobile money services operating in 93 countries. More than one billion mobile money transactions were processed in December, 2015.[vi]

We should cheer these developments. The G-20 included "financial inclusion" on its priority agenda to help over two billion adults around the world who have limited access to financial institutions. [vii] As an example, only an estimated four percent of Mauritanian adults have bank accounts.[viii]

I know many of Task Force members are international travelers. Many of you have traveled extensively in the developing world. Undoubtedly, you have observed how easy access to M-payments via the ubiquitous cell phone is transforming lives by providing a much needed link to contemporary financial services at a reasonable price. Users are not required to have a bank account or credit card. Countries without modern financial and communications infrastructure are able to "leapfrog" directly into cutting edge networks.

For example, in Tanzania only 12 percent of the population is engaged in the formal financial sector. Mobile banking services fill the gap and, as a result, are

expanding rapidly. The Central Bank of Tanzania estimates that the equivalent of $650 million is transferred each month through mobile transfers. [ix]

In Kenya, using 2013 data, an astounding 43 percent of Kenya's GDP flowed through M-Pesa, the country's leading mobile money service provider.[x] Twenty-three million Kenyans use M-Pesa or 90% of the adult population. There over 100,000 M-Pesa agents in Kenya.[xi]

How it Works

The following is a very simple summary of how money moves via cell phone.

1. The subscriber/user gives cash to an M-payment outlet. Sometimes these are nothing more than a small "mom and pop" kiosk or a convenience store in a rural village or city street. The user pays a small fee generally based on the amount of money involved.
2. The M-payment center transfers the money electronically through the phone company to the receiver's cell phone.
3. The recipient receives a text message informing him/her that the transfer to his "electronic-wallet" is complete.
4. The recipient uses the credits.

M-payments allow the purchase of products, services, payment of bills, the transfer of money person to person (P2P), the facilitation of micro payments for low value repetitive goods such as mass transit, the settlement of utility bills, payment of taxes, school fees, health, and many other services. Salaries and government benefits can be credited to cellular devices. M-payments have empowered small business creation. Remittances from migrant workers are sent home via the use of cell phones.

Unfortunately, this wonderful development in financial services is also going to have dangerous side effects that I believe deserve the attention of this Task Force.

Money Laundering and Terror Finance Dangers

I spent a career traveling the world investigating financial crimes such as fraud, money laundering and terrorist finance. I firmly believe that unless we move quickly to engineer new forms of data collection and analytic tools in M-payment systems and also put in place regulatory and enforcement countermeasures we will pay a very heavy price. In fact, there are signs that the abuse of the mobile payment industry by criminal elements is already happening.

I would like to reference the three distinct stages of money laundering and explain how M-payments are used in all three.

The first stage of money laundering is **"placement"** of illicit cash into a financial institution. There are many ways this occurs. One of the most prevalent methods both in the United States and around the world is "structuring," sometimes also known as "smurfing." For example, a professional money launderer takes a large amount of drug dollars and divides it into small amounts. He gives the small sums of money to "runners" or "smurfs" to deposit. The transactions are done in ways that attempt to avoid government mandated financial transparency reporting requirements. Financial transparency equates to financial intelligence. To put things in context, in the United States approximately 17 million pieces of financial intelligence are forwarded to the Treasury's Financial Crimes Enforcement Network (FinCEN) every year. Financial intelligence helps analysts and law enforcement officers follow the money trail. Most countries have similar types of financial transparency countermeasures.

With M-payments criminals now have a new way to "place" the proceeds of crime into financial networks. For example, a professional money launderer recruits a number of runners and gives them the proceeds of criminal activity. Small street sales of drugs, stolen property, or even suspect charitable or terror financing contributions can be laundered in this manner. The runners then go to M-payment establishments and use the illicit funds to load up their cell phones with money or "e-value" under the maximum threshold level. At the end of the day, the runner will be directed to forward the mobile money credit to master accounts controlled by the money launderer. This technique has been labeled by the Asian Development Bank as "digital smurfing." In contrast to money laundering where cash is placed into traditional financial institutions and sometimes money service businesses (MSBs), these structured M-payment placements are not transparent. With few exceptions, financial intelligence is not generated. And practically speaking, as I describe below, digital smurfing in most countries of concern is immune to law enforcement counter measures.

The second stage of money laundering is **"layering."** Once the illicit funds are "placed" into a financial institution, the objective is to layer the dirty money by multiple transfers and transactions thereby confusing the paper trail and adding multiple levels of venue and jurisdiction. Layering makes it very difficult for criminal investigators to "follow the money."

With M-payments, layering will be taken to new levels. In most jurisdictions, mobile value can be transferred from account to account and then directed to a

financial institution or MSB either in the host country or perhaps wired to another country or even an offshore haven. Mobile value can even be credited to an on-line account or perhaps used to purchase virtual currencies in cyberspace. A myriad of formal and informal money transfer systems such as hawala can also be added to the equation to further frustrate criminal investigators trying to follow the money trail. M-payments can also be used in hawala networks as a 21st century means of settling accounts between brokers. In short, layering schemes are only limited by the criminal's imagination.

The third stage of money laundering is defined as **"integration."** Once the dirty money is placed and layered, fronts for a criminal organization integrate the laundered money back into the economy. They might buy luxury vehicles, palatial homes, invest in shopping centers, the stock markets, and commercial enterprises of all sorts.

For example, the daughter of one of the worst kleptocrats in Africa has a net worth of billions of dollars. The country concerned has tremendous natural resources. The money controlled by the kleptocrat's family could be described as "fruits of corruption." In order to help "integrate" or legitimize the laundered ill-gotten gains, the kelptocrat's daughter has invested in cell phone carriers and M-payment providers in multiple countries.

In another example cited by the U.S. Department of State, in the West African country of Cote d'Ivoire funds are already being laundered via these M-payment techniques. In Uganda, also according to State Department reporting, "a significant portion of financial transactions . . . take place in the form of 'mobile money' payments and transfers, which could be abused by individuals and entities engaged in money laundering, terrorist financing, or other forms of financial crime. . . While the AMLA (financial intelligence unit/FIU) requires financial institutions to conduct comprehensive customer due diligence, it does not put the same requirements on mobile money transfers."[xii]

While sub-Sahara Africa is the region where mobile money is most widely spread, South Asia, the Caribbean, Latin America, and the Middle East are also rapidly expanding mobile financial services. Per industry sources, the following are a few examples of some of the most successful examples of M-payments; the Philippines, Bangladesh, Pakistan, and Afghanistan.[xiii] Some of these countries already boast millions of M-payment users.

Unfortunately, these same countries also face terror finance challenges and likewise have extremely weak anti-money laundering/counter-terrorist finance (AML/CFT) enforcement. In all of the above examples, due diligence practiced by

mandated reporting entities such as banks, money service businesses (MSBs), and designated non-financial businesses and professions is generally very weak. The FIUs are challenged - if not ineffectual - and law enforcement and prosecutors are hampered by a lack of expertise and capacity. To put things in perspective, in 2015 the Philippines had 0 convictions for money laundering; Bangladesh had 1 conviction; Pakistan had 0 convictions, and in 2014 (the last year statistics are available) Afghanistan reported only 4 money laundering convictions.

Realistically, there are no current tools to help law enforcement and intelligence officers identify and untangle suspicious M-payments in these and other countries where our adversaries operate. And as far as I am aware, none are on the horizon.

My point is that some skeptics might claim that there are few current cases linking mobile payments with money laundering and terror finance. I am convinced that currently there are many incidents and they will increase rapidly in the coming years. Cases are simply not recognized because the necessary technical infrastructures are not in place to trigger "red-flags." Moreover, there is a lack of understanding of the new M-payment threat and a corresponding lack of financial crimes investigative capacity in most of the countries concerned. There has been a rush by entrepreneurs and mobile payment carriers to develop the technology and deliver services while for the most part ignoring countermeasures that could be engineered into the systems to help thwart money laundering and terror financing.

Some countries are being careful. For example, M-payments in Lesotho are flourishing. So the Central Bank of Lesotho mandated that mobile money systems such Ecocash and M-Pesa must adhere to the Lesotho Money Laundering and Proceeds of Crime Act. The Central Bank issued guidance that was developed to conform to "international best practices and standards." M-payment providers are mandated to follow AML/CFT compliance programs. All transactions must be local and the amounts transferred have daily and monthly limits. In order to transfer higher amounts, know-your-customer (KYC) rules apply and subscribers are required to present their passport and proof of their sources of income. The system also has unusual behavior triggers which can lead to a suspicious transaction report (STR) being filed with the financial intelligence unit (FIU).[xiv]

The Lesotho model will help mitigate the digital smurfing risk. It will work for them because the size of the customer base is manageable. Lesotho has a population of two million. The real challenge will be to implement M-payment AML/CFT safeguards for large user communities.

For example, there are more mobile phones in Brazil than people, with approximately 275 million subscribers in a population of approximately 200

million – or approximately 100 times the population of Lesotho. Brazil is the fourth largest mobile market in the world. Yet despite the extensive mobile device penetration, mobile payments have been relatively slow to catch on. That will change soon.[xv]

Action Taken by the United States

So what is the United States government doing? The short answer is not much. Eight years ago when I first wrote about "the growing threat of M-payments," the idea of money laundering and terror finance via cell phones was mostly theoretical. In the interim, Treasury's Financial Crimes Enforcement Network (FinCEN) was given the mandate to sort out the myriad of legal, regulatory, and enforcement issues. Little was done.

U.S. regulators did make clear that existing financial services regulations apply to mobile banking and mobile payments providers. FinCEN announced "that the acceptance and transmission of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another person or location, by any means, constitutes money transmission" and is . . . "subject to relevant FinCEN regulations for AML/CFT purposes, either as part of the requirements on banks applying to all of their products and services, or as part of the requirements on money transmitters, a subset of regulated "money services businesses." [xvi] As such, mobile banking and mobile payment providers are required to register with FinCEN, be licensed in most of the states where they operate, and follow traditional financial intelligence reporting norms.

However, it gets complicated. According to the government's own data, FinCEN's MSB registration program has not been successful.[xvii] The diversity and accessibility of the MSB sector presents challenges for regulation and oversight.[xviii] Moreover, many of the businesses involved in the transfer of money through mobile devices aren't financial institutions. Some argue that companies involved in mobile payment systems that don't meet the established definition of providing banking services aren't subject to anti-money laundering enforcement scrutiny, regulation, or even consumer protection laws. Undoubtedly, more years will go by while industry pushes back against the requirements.

In addition, there doesn't seem to be a sense of urgency to deal with these issues. While the use of M-payments will continue to grow, we have a social-economic culture that includes very well-established electronic payments systems with numerous existing options to meet consumer needs outside of mobile. Moreover,

some observers in the U.S. have voiced concerns about M-payment interoperability, security, availability, consumer protection, etc.

Yet in most jurisdictions overseas, these concerns do not dominate discussion. As noted, many countries are hampered by weak anti-money laundering controls, enforcement, lack of capacity and expertise, corruption, and the lack of political will to seriously confront money laundering. M-payments are thriving in these same areas and I believe they represent clear and present money laundering and terror finance dangers that will accelerate globally in the very near future for the simple reason that criminal networks always gravitate towards the weak link.

What Should be Done?

Similar to my earlier testimony on TBML, I am somewhat optimistic about engineering AML/CFT safeguards into M-payments. As with TBML, M-payments generate big data. Advanced analytics can be applied. For example, current fraud frameworks and security intelligence platforms are agile and can be adapted to various architectures and use cases. They are currently being used by both global banks and telecom companies for financial crime detection, public security and regulatory purposes. Technology enables identity management capabilities and risk scoring using rules, predictive models, anomaly detection, as well as link and association analysis. In short, "red-flags" can be engineered into M-payment systems that could automatically trigger alerts, suspend suspect transactions, and generate the filing of financial intelligence reports with the host country's FIU.

The worldwide growth of mobile money services does necessitate banking and telecom regulators to work together to allow mobile platforms to work. This type of cooperation is challenging. And while there will be some costs for the M-payment industry, I believe M-payment providers should welcome robust anti-fraud and AML/CFT safeguards because they cannot afford being labeled as facilitating financial crime.

Overseas, ready markets already exist for M-payment AML/CFT safeguards. I encourage U.S. data and analytics innovators to get involved. If government does not wish to take the lead, I would like to see industry or a neutral and well-respected organization or think-tank convene an open forum where concerned law enforcement representatives, regulators, representatives from mobile carriers, and big data and analytics companies can discuss both the challenges and the opportunities of engineering AML/CFT countermeasures into M-Payment systems. Perhaps an analytic solution could be developed and shared with interested mobile operating platforms and host country FIUs in the developing world. The safeguards could be made available in ways similar to the Egmont Group's "secure

web" communications network and the United Nations Office on Drugs and Crime (UNODC) standard software system "GoAML" which is made available to FIUs around the world.

In addition, I believe that applicable law enforcement and intelligence agencies should heighten their awareness and reporting on the growing threat of M-payments.

As this Task Force understands, it's much easier and less expensive to take pro-active steps in the early stages of new financial threats rather than to wait and play "catch-up." We should not wait and react to a crisis if we can identify one in the making.

I appreciate the opportunity to appear before you today and I'm happy to answer any questions you may have.

---

[i] John Cassara, Testimony: "Trading with the Enemy: Trade-Based Money Laundering is the Growth Industry in Terror Finance;" available online at: http://democrats.financialservices.house.gov/uploadedfiles/02.03.2016_john_a._cassara_testimony.pdf

[ii] 2008 International Narcotics Control Strategy Report (INCSR) Volume II on Money Laundering, U.S. Department of State; available online at: http://www.state.gov/j/inl/rls/nrcrpt/2008/vol2/html/101346.htm

[iii] "Electronic Finance: A New Approach to Financial Sector Development?" World Bank Discussion Paper 431

[iv] David Runde, "M-Pesa and the Rise of the Global Mobile Money Market," August 12, 2015, *Forbes;* available online: http://www.forbes.com/sites/danielrunde/2015/08/12/m-pesa-and-the-rise-of-the-global-mobile-money-market/#663d74f723f5

[v] Roger Cheng, "By 2020, More People will Own a Phone than have Electricity," February 3, 2016, CNET; available online: http://www.cnet.com/news/by-2020-more-people-will-own-a-phone-than-have-electricity/

[vi] Daniel Thomas, "Vodaphone Rings Up Record Growth on Mobile Money Platform," *Financial Times*, April 24, 2016; available onlinehttps://next.ft.com/content/0242219e-087f-11e6-b6d3-746f8e9cdd33:

[vii] "Advancing Financial Inclusion to Improve the Lives of the Poor," *CGAP*, available online at: http://www.cgap.org/topics/financial-inclusion

[viii] 2014 International Narcotics Strategy Report (INCSR) Volume II on Money Laundering, U.S. Department of State; see entry under Mauritania

[ix] 2016 State Department International Narcotics Control Strategy Report (INCSR), Volume II on Money Laundering; available online at: http://www.state.gov/documents/organization/258726.pdf

[x] Runde
[xi] "The Future of Money," *60 Minutes*, November 22, 2015; available online via YouTube: https://www.youtube.com/watch?v=AHIgQttKajc&list=PL55ohbFcgaDMbY-iVxzP6cpJPDVMfDpV3
[xii] 2016 INCSR
[xiii] Runde
[xiv] John Cassara, "Out of Africa – AML Compliance for Mobile Payments," June 12, 2015, *Mobile Payments Today;* available online: http://www.mobilepaymentstoday.com/articles/out-of-africa-aml-compliance-for-mobile-payments/
[xv] Bethan Cowper, "Brazil is the Country to Watch for Mobile Payments," *Banking* 2015; available online at: http://www.paymentssource.com/news/paythink/brazil-is-the-country-to-watch-for-mobile-payments-3019867-1.html
[xvi] For more information, see "The Future of Money: Where do Mobile Payments Fit in the Current Regulatory Structure?": Hearing Before the Subcommittee on Financial Institutions and Consumer Credit, 112th Cong. (2012) (statement of James H. Freis, Jr., Director, Fin. Crimes Enforcement Network, U.S. Dept. of Treasury), available online at: http://financialservices.house.gov/uploadedfiles/james_freis_testimony.pdf
[xvii] 2007 National Money Laundering Strategy Report; available at: http://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/nmls.pdf
[xviii] Ibid

Testimony of Douglas Farah

President, IBI Consultants LLC
Senior Visiting Fellow National Defense University Center for Complex Operations
Senior Non-Resident Associate, Americas Program, CSIS

Before the Task Force to Investigate Terrorism Financing
House Committee on Financial Services

The Next Terrorist Financiers: Stopping Them Before They Start

June 23, 2016

Rayburn House Office Building Room 2128

Chairman Fitzpatrick, Ranking Member Lynch, and members of the Task Force:

Thank you for the opportunity to testify on the important issue of the changing nature of terrorist financing. I want to state clearly that I speak only for IBI Consultants and myself at this hearing, and not on behalf of either the National Defense University or CSIS.

I have been asked to address new mechanisms that terrorists are using to finance their activities, hide and move the value of their resources, and generate income. I would like to address several issues that I think are important, and that are often carried out in conjunction with transnational criminal organizations (TCOs).

A Historic Overview and the Rise of "Criminalized States"

In my three decades of focusing on transnational crime and 15 years working extensively on threat finance issues, I have found that there is very little new under the sun. Some new domains, such as cyber, have emerged and offer different alternatives but most of the money moves through the same general structures that they have for many years. These include trade based money laundering; the use of commodities such as diamonds, emeralds, and gold; bulk cash shipments; and informal money transfer systems.

The use of gold and precious stones by terrorist groups and TCOs has been widely documented but little understood. In 2002, I wrote a front-page investigation in the *Washington Post* on how al Qaeda and the Taliban used gold for financial transactions and how the organizations shipped millions of dollars in gold from Afghanistan and elsewhere to Dubai immediately following 9/11. It was one of the key financial lifelines that allowed the organizations to survive. [1]

In 2004 I wrote a book on how al Qaeda, Hezbollah and other terrorist groups, as well as multiple criminal syndicates used West Africa's "blood diamond" trade to move and store millions of dollars of value.[2] My colleague here today, John Casara, was one of the first in the U.S. government to try to focus on gold issues and has written extensively and compellingly on the issue.

Those terrorist organizations used these methodologies for the same reason Colombia's Revolutionary Armed Forces of Colombia (*Fuerzas Armadas Revolucionarias de Colombia* – FARC), Hezbollah and other terrorist groups use them today – because it is easy, low risk and largely unregulated. Dubai remains the center of the world gold and diamond trade and virtually every major gold bullion firm under investigation or convicted in the use of gold for terrorist financiers has a significant presence in that Emirate.

What has changed in recent years is the volume of the streams of illicit money flows in which terrorists and allied TCOs can hide their money movements. There are many factors at play in the rapid expansion of these flows, but I would like to start by reiterating a

---

[1] Douglas Farah, "Al Qaeda's Road Paved with Gold: Secret Shipments Traced Through Lax System in United Arab Emirates," The Washington Post, February 17, 2002, p. A01.

[2] Douglas Farah, Blood From Stones: The Secret Financial Network of Terror, Broadway Books, New York, 2004.

concept or a construct that I shared with this task force when I testified before you in May 2015: criminalized states and the hybrid criminal/terrorist structures they support.

By criminalized state I mean states where the senior leadership is aware of and involved – either actively or through passive acquiescence – on behalf of the state, in transnational criminal organizations (TCOs), where TCOs are used as an instrument of statecraft, and where levers of state power are incorporated into the operational structure of one or more TCOs.[3] In these states the government, relying on revenues from illicit activities to survive, often facilitate the overlapping activities with different terrorist organizations.

The existence of these criminalized states in Latin America, Africa, and parts of the former Soviet Union is a primary factor that facilitates terrorist and TCO financial movements, today, and one that has allowed for a significant increase in these activities. The fact that these illicit flows are embedded within state structures is also one of the key factors in making it difficult to halt such financial flows or to punish those engaged in such illicit activities.

This emerging combination of threats comprises a hybrid of criminal-terrorist and state- and non-state franchises, combining multiple nations acting in concert, and traditional TCOs and terrorist groups acting as proxies for the nation-states that sponsor them. No longer is the state/non-state dichotomy viable in tackling these problems, just as the TCO/terrorism divide is increasingly disappearing.[4]

In the Western Hemisphere, it is the involvement of numerous states led by Venezuela in an ongoing criminal enterprise that make disrupting and dismantling the financial networks so difficult. The government of Nicolás Maduro, along with the governments of Evo Morales in Bolivia, Rafael Correa in Ecuador, Daniel Ortega in Nicaragua and Salvador Sánchez Ceren in El Salvador, view the Revolutionary Armed Forces of Colombia (*Fuerzas Armadas Revolucionarias de Colombia* – FARC), a designated terrorist organization by the United States and Europe,[5] as well as a major cocaine trafficking organization, as a strategic ally.

This same bloc of countries, grouped under the umbrella of the Bolivarian Alliance for the Peoples of Our America (*Alianza Bolivariana Para los Pueblos de Nuestro America* – ALBA), has actively helped Hezbollah, the Spanish separatist ETA organization and other designated terrorist entities to establish a significant presence in Latin America. Hezbollah, in turn is a proxy for the nation of Iran and has access to the financial structures discussed

---

[3] This definition is drawn from my study of transnational organized crime in Latin America. For a full discussion see: Douglas Farah, *Transnational Organized Crime, Terrorism, and Criminalized States in Latin America: An Emerging Tier-One National Security Priority* (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, August 2012), accessed at: http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1117

[4] Douglas Farah, *Transnational Organized Crime, Terrorism, and Criminalized States in Latin America: An Emerging Tier-One National Security Priority,* op cit.

[5] "FARC Terrorist Indicted for 2003 Grenade Attack on Americans in Colombia," Department of Justice Press Release, September 7, 2004. accessed at: http://www.usdoj.gov/opa/pr/2004/September/04_crm_599.htm and: Official Journal of the European Union, Council Decision of Dec. 21, 2005, accessed at: http://europa.eu.int/eurlex/lex/LexUriServ/site/en/oj/2005/l_340/l_34020051223en00640066.pdf

below because their own state sponsor –Iran – protects them and Iran's Latin American allies in ALBA.

In my previous testimony, I discussed the vast flows of inexplicable resources that wash through the ALBA government financial structures. Both presidents Ortega in Nicaragua and Sánchez Cerén in El Salvador are former leaders of revolutionary movements in their home countries and have deep historic and abiding ties to both the FARC and the Chávez/Maduro criminal structure.

Ortega has publicly acknowledged receiving some $500 million dollars a year that flow directly to him and his family members, reportedly from the sale of subsidized Venezuelan oil through the state run company Albanisa. However, little such oil actually exists. Yet the money flowing through the Albanisa structure is equivalent to about 20 percent of the nation's annual budget, but is completely unregulated and unaccounted for.

In El Salvador, the governing Farabundo Marti National Liberation Front (FMLN) controls ALBA Petróleos, which is 60 percent owned by PDVSA, the Venezuelan state oil company. Sánchez Cerén is a member of the ALBA leadership, as is Ortega.

According to public statements of FMLN leaders such as José Luis Merino, ALBA Petróleos began with $1 million from PDVSA in 2007 and by the end 2013 had revenues of $862 million, with no explanation for the massive growth.[6] Merino, who is a senior ALBA Petróleos advisor, publicly stated that he knew that "many people are nervous because ALBA Petróleos was born six or seven years ago with $1 million and now has $400 million. Let me correct myself, $800 million, and we are trying to change the lives of Salvadorans."[7] The following year ALBA Petróleos leaders said the company generated $1 billion in revenues. Yet there is no legal economic activity to undergird anything close to that amount of revenue.

This represents about 23 percent of the national budget. However, like Albanisa, the revenues do not flow into the national treasury, are not allocated through the normal budgetary process and are subject to no oversight. They are directly controlled by party elites, with no accountability. Investigations in El Salvador show that the ALBA Petróleos structure has moved at least $291 million through eight shell companies to offshore safety in Panama.[8]

The Growing Importance of Gold in TCO and Terrorist Structures

Within the context of these vast, economically irrational money flows already moving through criminalized states, the growing amount of unusual mining and exporting of minerals, particularly gold in Latin America must be viewed with concern.

The relatively high price of gold, coupled with the ease of movement, ease of placement and sale, and a striking lack of control over the movement of the commodity make it particularly

---

[6] These figures are taken from ALBA Petróleos official financial filings.

[7] "José Luis Merino defiende a Alba Petróleos por ataques de ANEP," Verdad Digital, October 31, 2013.

[8] Efren Lemus, "Alba tiene ocho offshore en Panamá y así reduce impuesto en El Salvador," El Faro, April 11, 2016, accessed at: http://www.elfaro.net/es/201604/el_salvador/18388/Alba-tiene-ocho-offshore-en-Panam%C3%A1-y-as%C3%AD-reduce-impuestos-en-El-Salvador.htm

attractive to both criminal and terrorist groups. The fact that gold movements are not required to be reported as financial transactions mean that almost-pure ore can be moved with great ease and little risk, and converted to cash almost immediately and again at little risk.

It is even easier if state institutions, rather than trying to find and halt the illicit movements of gold are complicit in that movement across borders. U.S. and European law enforcement investigations have documented multiple cases of Venezuelan government officials, in addition to aiding and abetting the flow of FARC-produced cocaine to the United States and Europe, moving gold illegally through the free trade zones of Curacao, Panama and elsewhere.

As one recent study noted, "There are two broad characteristics of gold and the gold market which make it enticing to criminal groups. The first is the nature and size of the market itself, which is highly reliant on cash as the method of exchange. The second is the anonymity generated from the properties of gold, which make tracking its origins very difficult to do. These factors make gold highly attractive to criminal syndicates wishing to hide, move or invest their illicit proceeds."[9]

Due to the almost complete lack of risk, moving gold is increasingly becoming a preferred method of payment for other illicit products, such as cocaine. And in some cases, illegal mining is replacing cocaine trafficking as the primary illicit commodity moved to the international market.[10]

"Today criminal mining moves more resources to illegal groups, the guerrillas and mafias, than narco-trafficking," said Colombian President Juan Manuel Santos last year. He estimated the revenue from illegal gold mining to be more than $2 billion.[11]

According to one study, while it takes six months to grow coca and process a kilo of cocaine, along with significant technical skills, low-cost and low-skill gold mining in the Colombian jungle can yield 2 kilos a month. In addition, "a kilogram of cocaine can sell for about 5 million pesos ($2,570) in the Colombian jungle while a kilogram of gold can fetch 19 times that, or similar to global market prices....The precious metal is also relatively easy to legalize while cocaine remains banned. As soon as it's excavated and away from the mine it's legal."[12]

As the inter governmental Financial Action Task Force (FATF) noted in its 2015 report title "Money Laundering/terrorist financing: Risks and vulnerabilities associated with gold,"

---

[9] Financial Action Task Force, "Money laundering/terrorist financing: risks and vulnerabilities associated with gold," July 2015, accessed at: http://www.fatf-gafi.org/media/fatf/documents/reports/ML-TF-risks-vulnerabilities-associated-with-gold.pdf

[10] "Minería illegal desplaza a la coca en ocho regions," El Tiempo (Colombia), September 12, 2012, accessed at: http://www.eltiempo.com/archivo/documento/CMS-12214227

[11] "Minería supera al narcotráfico en ingresos: Santos," CM& Noticias, August 11, 2015, accessed at: http://www.cmi.com.co/mineria-supera-al-narcotrafico-en-ingresos-santos

[12] Cecilia Jamasmie, "Illegal gold profits for rebels in Colombia five times larger than cocaine," Mining.com, June 24, 2013, accessed at: http://www.mining.com/illegal-gold-mining-profits-for-rebels-in-colombia-five-times-larger-than-cocaine-68592/

Gold is an extremely attractive vehicle for laundering money. It provides a mechanism for organised crime groups to convert illicit cash into a stable, anonymous, transformable and easily exchangeable asset to realise or reinvest the profits of their criminal activities.

The gold market is a target for criminal activity because it is highly lucrative. Understanding the various stages of the gold market continuum, and the types of predicate offending that can occur in each stage, is critical in identifying money laundering and terrorist financing risks emanating from this industry. [13]

Because of the ease of using gold, where many large gold smelting and refining companies act as banks as well as commodity brokers, when the formal financial system comes under pressure, this is an easy, low risk and cost free alternative.

When the U.S. government's inter-agency investigation successfully took action against the Lebanese Canadian Bank (LCB) in 2011, designating the bank both a "primary money laundering concern" and primary financial vehicle for Hezbollah, the bank collapsed.[14] This left multiple important stakeholders with the need to find alternative financial service providers and ways to both launder and move cash value. Recent U.S. and European law enforcement investigations show that many of those providing financial services to Hezbollah and TCOs through LCB are now moving resources through a web of gold companies based in Dubai.

This new rush to gold has brought noticeable distortions to the gold market, though few steps have been taken to examine them. Those using gold often disguise the origin of the gold so as to avoid scrutiny in the country of origin. Thus Peruvian gold purchasers may move the gold out of Medellín, Colombia, and show the origin as Colombian, a situation that led to a time recently when Colombia on paper was exporting more gold than it actually produced.

Because the FARC and its allies in Venezuela want to disguise the origin of their gold after it is mined, they often move it through Guyana, Suriname, Nicaragua and/or Ecuador to avoid detection of gold entering the market from places where such movements would arouse suspicions of TCO and terrorist connections.

A joint investigation by *Ojo Público*, a consortium of news outlets in South America, into gold mining found that:

Through a travel to mining centers in Peru, Bolivia, Ecuador and Colombia, accessing to judicial and police documents on illegal trafficking of metal and analyzing the exportation of gold from South America, ***OjoPúblico*** *identified the major financiers of the gold fever that has devastated large parts of South America in recent years—a group of companies from the US, Switzerland, Italy and the United Arab Emirates, associated or linked to the London Bullion Market Association (LBMA), the union that sets the international price of gold and that gathers the major traders of this asset in the world.*

---

[13] Financial Action Task Force, op. cit.

[14] U.S. Department of Treasury, "Treasury Identifies Lebanese Canadian Bank Sal as a 'Primary Money Laundering Concern," Press release, February 10, 2011, accessed at: https://www.treasury.gov/press-center/press-releases/Pages/tg1057.aspx

These companies -Metalor Technologies and MKS Finance, from Switzerland; Northern Texas Refinery (NTR Metals) and Republic Metals Corporation (RMC), from the US; Italpreziosi from Italy and Kaloti group from the emirate of Dubai-, are also suspected of buying hundreds of tons of illegal gold from south American exporting firms managed by illegal mining operators linked to money laundering, organized crime and cross-border smuggling of metal. The judicial authorities of Peru have targeted these companies (which also acquire gold in Medellin, La Paz and Guayaquil) because of the 25 criminal cases opened after the confiscation of one ton of metal in Callao between 2013 and 2014, and because of other processes of money laundering from illegal mining."[15]

The same consortium later found that many of the companies it had traced in its original investigations had set up an offshore financial structure in the British Virgin Islands (BVI) under the guidance of the Mossak Fonseca law firm based in Panama but with offices operating in Lima, Peru and elsewhere.[16]

The case of Goldex, where the company was accused by Colombian officials of laundering billions of dollars for the FARC and other criminal organizations, shows the template of how illicit gold moves and is used for laundering.

Colombian prosecutors handling the case say the company moved some 47 tons of gold, valued at $1.4 billion, over a six-year period prior to the arrest of its leader. Goldex records showed a host of anomalous and illegal activities that were carried out but are seldom investigated or prosecuted. In this case, however, prosecutor Luz Angela Bahamon concluded that "it is not possible to come to any conclusion except that all of the gold and all of this income they were trying to justify was of illegal origins and came from illegal organizations that needed to create a structure to launder their profits." [17]

The conclusions were based on a series of irregularities that are common in the illicit gold trade and across the world of commodities. As one report noted about the Goldex case:

At the indictment hearing in January this year, the prosecutor described how Goldex sourced its gold from a network of ephemeral supply companies whose life cycle rarely exceeded three years. The companies financed millions of dollars of gold purchases with just thousands in capital and conducted hundreds of transactions in a single day without having a single contract employee, Goldex company records show. Their offices could be found in the most unexpected locations, such as scrapyards or a family home in a village in the state of La Guajira, where the owner swears there has been no gold trading in the 50 years since her great-grandfather built the house.

---

[15] Óscar Castilla C., Nelly Luna Amancio y Fabiola Torres López, "Dirty Gold: Chasing the Trace of the London Bullion Market," OjoPúblico,, June 9, 2015, accessed at: http://ojo-publico.com/dirty-gold-chasing-the-trace-of-the-london-bullion-market/

[16] Óscar Castilla C., "Panama Papers: Las Islas Vírgenes de la Minería Ilegal," OjoPúblico, April 15, 2016, accessed at: http://panamapapers.ojo-publico.com/articulo/las-islas-virgenes-de-la-minerial-ilegal/

[17] James Bargent and Michael Norby, "Blood gold: From conflict zones in Colombia to jewelry stores in the US," Al Jazeera America, November 18, 2015, accessed at: http://america.aljazeera.com/articles/2015/11/18/blood-gold-colombia.html

Purchase records show that the gold these companies supplied to Goldex was bought from thousands of dead people and people who never existed. Yet more of the precious metal was registered as having come from people who told prosecutors they had never been involved in the gold trade, in some cases because they had been living on the streets for years.[18]

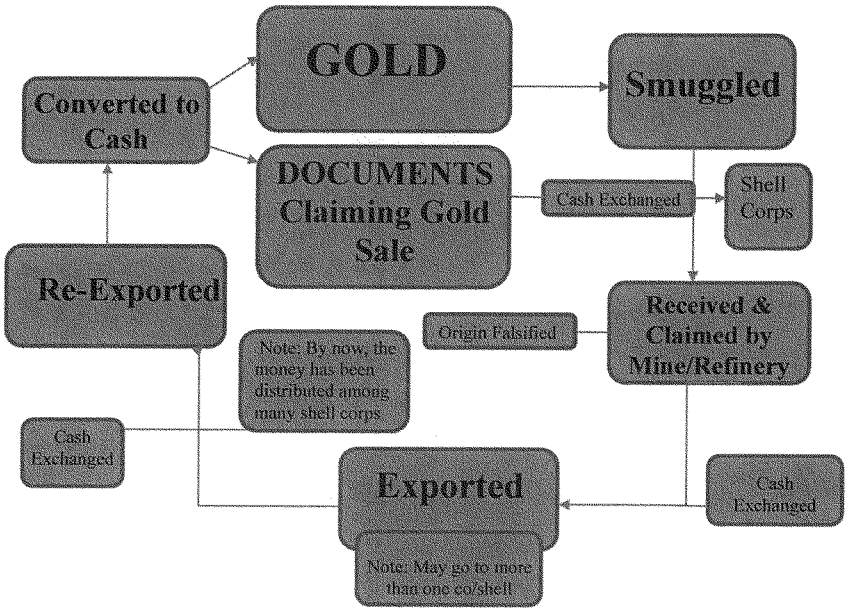

Figure 1: Illicit Financing/Money Laundering with Gold. Created by Liana Reyes-Reardon, IBI Consultants

The Vital Roll of Offshore Havens

The massive leak of the internal documents of the Panamanian law firm Mossack Fonseca, now known as the Panama Papers, gives an unsettling view of just how easy it is to use law firms in certain jurisdictions to incorporate entities where the real owners are never

[18] Bargent and Norby, op cit.

disclosed, and then use those entities to move massive sums of money to offshore havens where the anonymity is preserved.[19]

While privacy issues are real and valid, the current structure represents one of the most glaring weaknesses in the financial structures that are used by a host of illicit actors, including terrorists and TCOs. It is easy but dangerous to forget that al Qaeda and Hamas used extensive offshore structures in the Bahamas to move money around the globe for terrorist groups, including al Qaeda, prior to and following the attacks of 9/11.[20]

This opaque world overlaps with the vast unregulated world of gold and other commodity movements, and both intersect in the growing number of "criminal state" jurisdictions. This amounts to a perfect storm for terrorist financiers and TCOs to hide and move cash and cash value across the world in ways that are virtually untraceable.

As it stands now, law firms in Panama, Delaware, and multiple other jurisdictions inside and outside the United States can establish a company with bearer shares and that company can then open bank accounts in jurisdictions that pride themselves on bank secrecy. There is no requirement that the real owner(s) of the company or account ever be known.

With those structures in place, large gold refineries acting as banks can then wire the value of gold deposited in their offices to those anonymous companies for deposit in hidden bank accounts.

All of this makes the work of law enforcement difficult if not impossible in tracing financial flows, even when the official strongly suspects the involvement of terrorists TCOs. While this secretive and opaque financial architecture exists, there is very little need for terrorist groups and TCOs to invent a host of new ways to move money and finance their activities. The current system, with its multiple vulnerabilities outside the regulated world where we focus most of our attention, works just fine.

Conclusions

I want to thank the Task Force to Investigate Terrorism Financing for the effort it has put forth to better understand the serious issues associated with this topic, and for the light it

---

[19] International Consortium of Investigative Journalists, " Giant Leak of Offshore Financial Records Exposes Global Array of Crime and Corruption," ICIJ, April 3, 2016, accessed at: https://panamapapers.icij.org/20160403-panama-papers-global-overview.html

[20] In Congressional testimony on February 12, 2002, Assistant Treasury Secretary Juan Zarate the services provided by Bank al Taqwa based in the Bahamas, noting that: "There is some evidence to indicate that those who support terrorist groups use shell banks and companies and perhaps correspondent accounts to collect and move money. On November 7, 2001, the Treasury Department listed Bank al-Taqwa, a Bahamian-based shell bank, as a terrorist financing source. In 1997, it was reported that the $60 million collected annually for Hamas was moved to accounts with Bank Al Taqwa. As of October 2000, Bank Al Taqwa appeared to be providing a clandestine line of credit to a close associate of bin Laden and as of late September 2001, bin Laden and his al-Qaida organization received financial assistance from the chairman of that bank." See: Treasury Deputy Assistant Secretary Juan Zarate, "Testimony Before the House Financial Subcommittee," U.S. Department of Treasury, February 12, 2002, accessed at: https://www.treasury.gov/press-center/press-releases/Pages/po1009.aspx

has shed on the financial structures that enable and facilitate the financing of terrorism. While the formal instruments for moving money are understood and regulated, the growing use of commodities and the ease of using anonymous offshore structures remain significant gaps that are easily exploited and seldom examined.

Part of the growing use of gold and other commodities is due to the measureable success the Treasury Department and some of the region's nascent Financial Intelligence Units have had in moving against the formal banking sector. For example, the joint Treasury/DEA case in Honduras late last year against the Rosenthal clan that shut down Banco Continental for its alleged involvement in drug trafficking and money laundering[21] was an important signal in the region that law enforcement was willing to tackle politically powerful families and their financial institutions.

But little attention is being paid to the multiple anomalies that are blooming across the region. These include: a major diamond polishing center in a region with few diamonds to justify its existence; a gold refinery with capacity to refine four times the annual output of the host country; hosts of gold buying companies with few resources that grow, spread and disappear almost as quickly as mushrooms; small banks operating in marginal jurisdictions that show highly unusual rates of growth in their financial deposits and other activities; and government-sponsored mega projects that claim to spends hundreds of millions of dollars but in reality exist only on paper as a vehicle for laundering money.

Irrational economic behavior on a large scale shrouded in opaque or non-existent reporting is almost always indicative of significant TCO and/or terrorist activities. These behaviors are multiplying, particularly in criminalized states, across the globe. This creates the river that allows the funding of terrorism to grow more difficult to detect and disrupt.

Thank you.

---

[21] Steven Dudley, "US Releases Indictment Against Honduran Behemoth," InSight Crime, October 7, 2015, accessed at: http://www.insightcrime.org/news-analysis/us-releases-indictment-against-honduras-elite

Written Testimony of
Jimmy Gurulé*
Professor of Law
Notre Dame Law School

Before the
Task Force to Investigate Terrorism Financing
June 23, 2016

Chairman Fitzpatrick, Ranking Member Lynch, and other distinguished members of the 114th Congress' Task Force to Investigate Terrorism Financing:

Permit me to begin by thanking you for inviting me here to testify on the important and timely topic of "The Next Terrorist Financiers: Stopping Them Before They Start."

As we approach the fifteen-year anniversary of the 9/11 terrorist attacks that tragically took the lives of almost 3,000 innocent civilians, it is imperative that the U.S. government continue to evaluate and enhance the effectiveness of such counter-terrorism measures as curtailing terror financing in order to protect national security and save innocent lives.

The government's counter-terrorism strategy must be proactive, not reactive, anticipating how, when, and where ISIS, al Qaeda, and the next major terrorist organization will attack the United States and kill Americans. The terrorist attack that recently took place in Orlando, Florida, where forty-nine innocent people were killed and over fifty others were seriously injured, as well as the mass shooting that occurred on December 2, 2015 in San Bernardino, California, leaving fourteen dead and twenty-two others seriously wounded, serve as stark reminders of what is at stake in this undertaking.

Depriving terrorists of funding is central to an effective counter-terrorism strategy. "Terrorists seldom kill for money, but they always need money to kill."[1] And while Omar Mateen, the person responsible for the largest mass shooting in the nation's history, and Syed Rizwan Farook and Tashfeen Malik, the San Bernardino shooters, did not need much money to finance their terrorist attacks, the Islamic State, the terrorist organization that inspired their hatred of Americans, requires substantial financial resources to pursue its goal of establishing a Caliphate State.

At the super-structure or organizational level, the Islamic State needs money to recruit and train terrorist fighters, and to pay their salaries. The terror group also needs funding to purchase vehicles, weapons, ammunition, and explosives. Moreover, the Islamic State has exploited social

---

* Professor Gurulé served as Treasury Under Secretary for Enforcement from 2001 to 2003.

[1] Terry Davis, Sec'y Gen. of the Council of Europe, Speech at the First Joint Plenary Meeting of MONEYVAL with the Financial Action Task Force (Feb. 21, 2007), http://www.coe.int/t/dghl/monitoring/moneyval/Activities/Speech/Terry%20DavisJPlen.pdf.

media—most notoriously Twitter—to send its propaganda across the globe in order to recruit and radicalize people vulnerable to its message.

A recent report published by the Brookings Institution states:

> By virtue of its large number of supporters and highly organized tactics, ISIS has been able to exert an outsized impact on how the world perceives it, by disseminating images of graphic violence (including the beheading of Western journalists and aid workers and more recently, the immolation of a Jordanian pilot), while using social media to attract new recruits and inspire lone actor attacks.[2]

The Brookings Institution reports that between September 2014 and December 2014, the number of Twitter accounts used by supporters of the Islamic State is conservatively estimated to be at 46,000.[3] In short, the Islamic State needs money to sustain its global social media campaign and finance other terrorist-related activities.

(A) Increasing the Use of Secondary Sanctions

Shortly after the 9/11 terrorist attacks, President George W. Bush signed Executive Order 13224 (E.O. 13224), invoking his congressional grant of authority under the International Emergency Economic Powers Act.[4] E.O. 13224 declared a national emergency with respect to "grave acts of terrorism and threats of terrorism committed by foreign terrorists, including the terrorist attacks ... committed on September 11, 2001 ... and the continuing and immediate threat of further acts on United States nationals or the United States."[5]

Initially, the Executive Order designated twelve individuals and fifteen entities as "Specially Designated Global Terrorists" (SDGTs) and identified them in the Annex to the order. To date, the number of SDGTs has grown exponentially, to approximately 1,000 individuals and entities.[6] Throughout, E.O. 13224 has been the centerpiece of the government's counter-terrorist financing efforts.[7]

E.O. 13224 authorizes the Secretary of the Treasury, in consultation with the U.S. Secretary of State and Attorney General, to designate additional persons and entities as an SDGT and block

---

[2] J.M. Berger & Jonathon Morgan, *The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter*, CTR. FOR MIDDLE E. POL'Y AT BROOKINGS, no. 20 (Brookings Project on U.S. Rel. with the Islamic World), Mar. 2015, at 2.

[3] *Id.*

[4] International Emergency Economic Powers Act (IEEPA), Title II of Pub. L. No. 95-223, 91 Stat. 1626 (codified at 50 U.S.C. § 1701, et seq. (2012)).

[5] Exec. Order No. 13224, 3 C.F.R. § 786 (2001), *reprinted as amended in* 50 U.S.C. § 1701 note (Supp. IV 2004) [hereinafter E.O. 13224].

[6] *See* Dep't of Treasury, OFAC, Terrorist Assets Report, 2014, Annual Report to the Congress on Assets in the United States, 23d, at 6, https://www.treasury.gov/resource-center/sanctions/Programs/Documents/tar2014.pdf.

[7] The discussion herein of E.O. 13224 is taken in large part from GEOFFREY CORN ET AL., NATIONAL SECURITY LAW: PRINCIPLES AND POLICY 402–04 (2015).

the assests located in the United States of such persons or entities who (1) "act for or on behalf of" or are "owned or controlled by" SDGTs, (2) "assist in, sponsor, or provide financial, material, or technological support for" SDGTs, or (3) are "otherwise associated with" SDGTs.[8] Further, E.O. 13224 authorizes the Secretary of State, in consultation with the Secretary of the Treasury and the Attorney General, to designate as SDGTs persons determined "to have committed, or to pose a significant risk of committing, acts of terrorism that threaten the security of United States nationals or the national security, foreign policy, or economy of the United States."[9]

E.O. 13224 has been an effective tool in curtailing funding to al Qaeda, which largely relies on support from external donors or corrupt charities sympathetic to their cause and having assets within the United States. Such individuals and entities have been designated as SDGTs, which requires their assets located in the United States to be blocked and prohibits all U.S. persons from conducting financial transactions with such designated parties.

The Islamic State poses a different terrorist financing challenge. Unlike al Qaeda, the Islamic State is primarily self-funded, obtaining the vast majority of its revenue from (1) oil and gas sales, (2) extortion and taxation, (3) kidnapping-for ransom, (4) looting banks, (5) selling stolen antiquities, and (6) human trafficking—that is, selling young girls and women as sex slaves.[10] The Islamic State's annual budget is an estimated $2 billion.[11] Further, despite recent military airstrikes aimed at destroying the infrastructure that allows the Islamic State to pump Syrian oil, and the fact that global oil prices have fallen, the terror group continues to generate as much as $200 to $500 million a year from its oil exports.[12]

E.O. 13224 has proven less effective in depriving the terrorist organization of funding. Assistant Secretary for Terrorist Financing Daniel Glaser stated, "[t]hey derive so much of their resources internally, that more traditional counterterror finance tools we would apply, say in the case of Al Qaeda, to cut off a terror organization from its income sources are not applicable in this case."[13] As such, targeting Abu Bakr al-Baghdadi, the leader of the Islamic State, for designation under E.O. 13224 has limited practical value and only symbolic significance. He has no assets located in the United States subject to blocking, and there is no evidence that any U.S. persons are doing business with him.

---

[8] E.O. 13224, *supra* note 5, at § 1(c)–(d)(i)–(ii).
[9] *Id.* at sec. 1(b).
[10] David S. Cohen, Treasury Under Sec'y for Terrorism and Fin. Intelligence, Remarks at the Carnegie Endowment for Int'l Peace, "Attacking ISIL's Financial Foundation" (Oct. 23, 2014), http://www.treasury.gov/press-center/press-releases/Pages/j;2672.aspx.
[11] *See* Jose Pagliery, *Inside the $2 Billion ISIS War Machine*, CNN (Dec. 11, 2015, 9:09 PM), http://money.cnn.com/2015/12/06/news/isis-funding/.
[12] *See id.; see also* Patrick Wintour, *Oil Revenue Collapse Means ISIS Reliant on Gulf Funds, Inquiry Hears,* THE GUARDIAN (Mar. 8, 2016, 12:15 AM), http://gu.com/p/4hctg/sbl (claiming that military attacks on oil infrastructure, falling global oil prices, and the low quality of Syrian oil have reduced annual oil revenues to $200 million); Hamza Hendawi & Qassim Abdul-Zahra, *ISIS is Making up to $50 Million a Month from Oil Sales,* BUSINESS INSIDER (Oct. 23, 2015, 2:46 AM), http://www.businessinsider.com/isis-making-50-million-a-month-from-oil-sales-2015-10.
[13] Mathew Rosenberg, Nicholas Kulish & Steven Lee Myers, *Predatory Islamic State Wrings Money from Those It Rules*, N.Y. TIMES (Nov. 29, 2015), http://nyti.ms/1Op4fja.

The government must adapt to the terrorist-financing challenges posed by the Islamic State. A good model is the economic sanctions regime imposed on Iran, which heavily relied on secondary sanctions. "Ordinarily, when the United States imposes economic sanctions, it imposes primary sanctions only—to restrict its own companies and citizens (or other people who are in the United States) from doing business with a rogue regime, terrorist group, or other international pariah."[14] Secondary sanctions "involve additional economic restrictions designed to inhibit non-U.S. citizens and companies abroad from doing business with a target of primary U.S. sanctions."[15]

Congress should consider enacting legislation against the Islamic State similar to the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 (CISADA), which imposed important secondary sanctions on foreign entities doing business with Iran.[16] The CISADA was intended to force foreign firms to choose between participating in the U.S. commercial market or entering into energy-related transactions with Iran. The CISADA greatly expanded the scope of prohibited activities to include efforts by foreign companies to (1) sell, lease, or provide to Iran any goods, services, technology, information or support that would allow Iran to maintain or expand it petroleum refineries and (2) to supply refined petroleum products to Iran.[17]

The CISADA sanctions any activities that "directly and significantly" assist Iran in either developing its oil refining capacity or obtaining refined petroleum.[18] Moreover, the prohibited transactions under the Act either must be done knowingly or involve circumstances in which the party "should have known, of the conduct, circumstances, or the result."[19] By inserting the negligence standard, which extends liability to parties who "should have known," the CISADA significantly expanded corporate liability beyond the existing Iran Sanctions Act of 1996 (ISA), under which parent corporations were liable only for approving or facilitating prohibited transactions.[20]

The CISADA requires the President to impose at least three different economic sanctions on foreign companies found in violation of the Act, and the statute added three new sanctions to the previous six authorized under the ISA.[21] These include: (1) prohibitions on foreign exchange

---

[14] Jeffrey A Meyer, *Second Thoughts on Secondary Sanctions*, 30 U. PA. J. INT'L L. 905, 905 (2014).
[15] *Id.*
[16] Comprehensive Iran Sanctions, Accountability, and Divestment Act (CISADA) of 2010, Pub. L. No 111-195, 124 Stat. 1312 (codified at 22 U.S.C. § 8501 note (2012)). The Iran and Libya Sanctions Act of 1996 (renamed the Iran Sanctions Act of 1996) is Pub. L. 104–172, 110 Stat. 1541, as amended by Pub. L. No. 111-195, § 102, 124 Stat. 1312, 1317–28 is referred to in para. (10) of the CISADA, which is set out as a note under section 1701 of title 50, War and National Defense. *Accord* CORN ET AL., *supra* note 7, at 387–88 (discussing the scope of the CISADA).
[17] *See id.* § 102.
[18] *Id.*
[19] *Id. See also* OFAC Iranian Financial Sanctions Regulations, 31 C.F.R. pt. 561 (2010) (implementing subsections 104(c) and (d) and other related provisions of CISADA).
[20] *See* U.S. Dep't of State, Additional Information for the Iran and Libya Sanctions Act, 61 Fed. Reg. 66067, 66068 (Dec. 16, 1996).
[21] *See* CISADA § 102(b).

transactions subject to United States' jurisdiction; (2) prohibitions on transfers of credit or payment between, by, through, or to financial institutions that are subject to the United States' jurisdiction; and (3) prohibitions on transacting or exercising any right, power, or privilege with respect to property subject to the jurisdiction of the United States.[22]

Legislation similar to CISADA should be enacted to impose sanctions on those foreign companies contributing to the development of the Islamic State's oil sector. As previously noted, U.S. military airstrikes have seriously damaged the Islamic State's oil infrastructure in territories it controls in Syria. However, the Islamic State should be prevented from repairing and rebuilding these damaged oil refineries with the assistance of foreign firms. To this end, secondary sanctions could be statutorily imposed on any foreign entities selling parts or providing technical support or services to assist the Islamic State in prohibited repair.

E.O. 13224 has limited application to foreign companies doing business with the Islamic State. Under section 2(a) of E.O. 13224, U.S. persons are prohibited from dealing in property blocked under the order and from providing funds, goods or services to SDGTs.[23] The sanctions available under E.O. 13224 would therefore only apply if the foreign firm providing assistance to the Islamic State was designated as an SDGT and had property in the United States subject to blocking. In such a case, U.S. persons would be prohibited from doing business with the designated foreign company. However, it is unclear whether a foreign firm assisting the Islamic State could be so designated under E.O. 13224. While assisting the Islamic State in rebuilding its oil infrastructure might plausibly constitute providing services "in support of[] such acts of terrorism" in violation of section 1(d)(i) of the Executive Order, this argument is highly tenuous.

Finally, the Islamic State itself has been designated an SDGT pursuant to E.O. 13224. Therefore, U.S. persons are prohibited from dealing with the terrorist organization. However, the executive order does not prohibit foreign firms and individuals from conducting business with the Islamic State.

The legislation I am proposing that Congress enact would allow for secondary sanctions beyond what is currently permitted under E.O. 13224. Regardless of whether a foreign firm held property within the United States or had been designated an SDGT, the entity would be subject to

---

[22] *Id.* § 102(b)(2). Prior to the CISADA, the President could choose from among six sanctions to impose on foreign entities:

(1) denial of Export-Import Bank assistance for exports;
(2) denial of export licenses or other specific requests under U.S. export control;
(3) denial of loans exceeding $10 million from U.S. financial institutions in any twelve month period;
(4) prohibition on sanctioned financial institutions from designation as a primary dealer in U.S. debt or as a repository for U.S. government funds;
(5) ban on procurement contracts with the U.S. government; and
(6) case-by-case imposition of import restrictions.

Iran and Libya Sanctions Act of 1996, Pub. L. No. 104-172, § 6, 110 Stat. 1541, 1545 (codified at 50 U.S.C. § 1701 note (2012)).

[23] E.O. 13224, *supra* note 5, at § 2(a).

a wide array of economic sanctions similar to those imposed against foreign businesses assisting Iran in developing its oil-refining capacity. Further, a CISADA-type of legislation would provide the President with a more nuanced set of punitive measures for combating those foreign enterprises that aid and do business with the Islamic State.

(B) Prosecuting Terrorist Financiers under the Material Support Statutes

The Department of Justice has a dismal record of prosecuting financiers of terrorism. Since September 11, 2001, there has been only one major terrorist financing prosecution. In November 2008, a federal jury convicted five leaders of the Holy Land Foundation for Relief and Development (HLFRD) for providing material support to Hamas, a designated foreign terrorist organization (FTO).[24] The HLFRD was a charity incorporated in the United States by the five criminal defendants and was used to raise money for Hamas. There have been no major prosecutions of individuals responsible for raising money for al Qaeda or affiliated terrorist organizations. Further, the provision of the *United States Code*, 18 U.S.C. § 2339C, which expressly prohibits raising and providing funds to terrorists, has rarely been used.

Individuals who raise money for foreign terrorist organizations or provide funding to such groups should be prosecuted under the material support statutes: 18 U.S.C. §§ 2339A, 2339B, and 2339C. Moreover, individuals providing financial support to "lone wolf" terrorists should also be punished.

Section 2339B prohibits the provision of material support or resources, including financial resources, to an FTO.[25] To prove a violation of § 2339B, the defendant must have knowledge that the organization is a designated FTO or has engaged or engages in acts of terrorism.[26] The

---

[24] *See* Press Release, Dep't of Justice, Federal Judge Hands Down Sentences in the Holy Land Foundation Case (May 27, 2009), https://www.justice.gov/opa/pr/federal-judge-hands-downs-sentences-holy-land-foundation-case.

[25] 18 U.S.C. § 2339B (2012). For purposes of § 2339B, a "foreign terrorist organization" is an organization designated as a terrorist organization under section 219 of the Immigration and Nationality Act, which is codified under section 1189 of title 8, Aliens and Nationality. Section 219 authorizes the Secretary of State to designate a group as a "foreign terrorist organization" if the group meets certain criteria:

> (A) the organization is a foreign organization;
> (B) the organization engages in terrorist activity (as defined in section 1182(a)(3)(B) of this title) or terrorism (as defined in section 2656f(d)(2) of title 22) [sic], or retains the capacity and intent to engage in terrorist activity or terrorism; and
> (C) the terrorist activity or terrorism of the organization threatens the security of United States nationals or the national security of the United States.

8 U.S.C. § 1189(a)(1) (2012).

[26] Section 2339B provides:

> To violate this paragraph, a person must have knowledge that the organization is a designated terrorist organization (as defined in subsection (g)(6), that the organization has engaged or engages in terrorist activity (as defined in section 212(a)(3)(B) of the Immigration and Nationality Act), or that the organization has engaged or engages in terrorism (as defined in section 140(d)(2) of the Foreign Relations Authorization Act, Fiscal Years 1988 and 1989).

18 U.S.C. § 2339B(a)(1).

government is not required to prove that the defendant intended to further the FTO's terrorist activities. That prohibition is based on a finding that FTOs "are so tainted by their conduct that any contribution to such an organization facilitates that conduct."[27] However, § 2339B is limited to the provision of material support or resources to an FTO, and does not apply where the recipient is a lone wolf terrorist.

Section 2339C makes it a crime to "provide or collect" funds with the intention that the funds be used, or with the knowledge that such funds are to be used, to commit one of the terrorism-related crimes enumerated in the statute. Section 2339C is broader in scope than § 2339B, as it is not limited to raising or providing funds to an FTO. However, § 2339C requires proof of a heightened scienter not required under § 2339B. The government must prove that the defendant had knowledge or acted with the intent that the funds be used to commit a violent crime. The statute does not prohibit providing funds to a lone wolf terrorist if the funds were provided for a benign purpose.

To better stop terrorist financiers, Congress should amend § 2339C to prohibit the provision or collection of funds with knowledge that the recipient has engaged in acts of terrorism or intends to commit a terrorist act in the future. Individuals should not be permitted to knowingly provide financial resources to persons they know have engaged or intend to engage in acts of terrorism. Providing funds with knowledge that the recipient has engaged or engages in terrorist acts should be a separate offense under the statute. Ultimately, § 2339C should be amended to require proof of the same scienter requirement needed to support a conviction under § 2339B.

(C) Justice Against State Sponsors of Terrorism Act

Civil tort actions that seek large monetary damages provide an invaluable supplement to criminal enforcement actions and economic sanctions intended to deter and punish acts of terrorism. Private lawsuits brought by the victims of international terrorism can have a deterrent effect against corrupt charities, donors, financial institutions, foreign states, and front organizations that provide financial support and other services to terrorist organizations.[28]

On May 17, 2016, the U.S. Senate unanimously passed the Justice Against Sponsors of Terrorism Act (JASTA) in an effort to strengthen civil terrorism causes of action.[29] This proposed legislation ensures that those who aid and abet terrorist attacks on U.S. soil are held accountable for their conduct, even if such offenders are foreign sovereigns or their instrumentalities. The JASTA does so through modest amendments to the Foreign Sovereign Immunities Act (FSIA) and the Anti-Terrorism Act (ATA), each of which recognizes this fundamental principle. The proposal

---

[27] Antiterrorism and Effective Death Penalty Act (AEDPA) of 1996, Pub. L. No. 104-132, § 301(a)(7), 110 Stat. 1214, 1247, note following 18 U.S.C. § 2339B (Findings and Purpose).

[28] *See* JIMMY GURULÉ, UNFUNDING TERROR: THE LEGAL RESPONSE TO THE FINANCING OF GLOBAL TERRORISM 324–69 (2008) (providing a comprehensive discussion of private causes of action with which to hold terrorist financiers accountable).

[29] Justice Against Sponsors of Terrorism Act, S. 2040, 114th Cong. (2015).

is a narrowly drawn statute that will deter international terrorism, guarantee the victims of terrorism have their day in court, and grant the executive new powers to resolve civil terrorism cases through diplomatic means.

The bill's new immunity exception, proposed to amend chapter 97 of Title 28 by inserting section 1605B, provides in part:

> A foreign state shall not be immune from the jurisdiction of the courts of the United States in any case in which money damages are sought against a foreign state for physical injury to person or property or death occurring in the United States and caused by (1) an act of international terrorism in the United States; and (2) a tortious act or acts of the foreign state, or of any official, employee, or ... agency, regardless where the tortious act or acts of the foreign state occurred.[30]

This provision ensures that U.S. courts will have jurisdiction over a tort involving an act of international terrorism committed by a foreign state on U.S. soil. The JASTA further provides that, where jurisdiction against a foreign state is satisfied, a U.S. national may bring a civil claim against a foreign state pursuant to the Anti-Terrorism Act.[31]

The Anti-Terrorism Act of 1992, codified at 18 U.S.C. § 2333, provides a private right of action to any U.S. national injured by reason of an act international terrorism. The federal courts are currently divided on whether the provision allows claims premised on a theory of aiding and abetting.[32] Generally, plaintiffs have a much easier burden of proof in a jurisdiction that permits § 2333 liability based on aiding and abetting. The disagreement as to the scope of the ATA could lead to inconsistent verdicts, depending on whether the plaintiff must prove that the defendant himself committed an act of international terrorism, or merely that he aided and abetted some other actor in doing so.

The JASTA removes this confusion by expressly recognizing a cause of action for aiding and abetting liability in the very narrow circumstance of international terrorism. It is important to note that the bill provides for aiding or conspiracy liability under the ATA only when the act of international terrorism was committed, planned, or authorized by a designated FTO. It does not apply to individuals who have no association with an FTO. Further, the proposed aiding and abetting liability provision requires prove of knowledge and substantial assistance.

---

[30] Justice Against Sponsors of Terrorism Act, S. 2040, 114th Cong., § 3(a) (as passed by Senate, May 17, 2016).
[31] The Antiterrorism Act of 1990—the short title to section 132 of the Military Construction Appropriations Act of 1990—was reenacted by the Federal Courts Administration Act (FCA) of 1992, Pub. L. No. 102-572, Title X, § 1003, 106 Stat. 4506. Section 1003(c), which appears as an 18 U.S.C. § 2331 note. Though the reenacted law was not designated as a short title, the collection of the FCA's "terrorism" provisions is colloquially referred to as the "Anti-Terrorism Act" of 1992. 18 U.S.C. § 2333 is the civil remedies provision of the Act, added Oct. 29, 1992, Pub. L. No. 102-572, Title X, § 1003(a)(4), 106 Stat. 4506, codified as amended.
[32] *See* Jimmy Gurulé, *Holding Banks Liable Under the Anti-Terrorism Act for Providing Financial Services to Terrorists: An Ineffective Legal Remedy in Need of Reform,* 41 NOTRE DAME J. LEGIS. 184, 206–09 (2015).

Finally, sponsors of the JASTA recognize that terror victims' demands for justice may complicate international diplomacy in certain circumstances. To address this concern, section 5 of JASTA gives the chief executive the power to intervene in any civil litigation against a foreign state alleging support for terrorism and then to obtain a stay of the proceedings while government-to-government discussions proceed. Ultimately, the JASTA will allow families victimized by terrorism to proceed in court against their attackers and enablers and hold them accountable for their actions. For all of the above reasons, this proposed legislation should be enacted into law.

(D) Developing a National Counter-Terrorist Financing Strategy

The threat of international terrorism is dynamic and constantly changing and evolving. The Department of State has designated over fifty foreign terrorist organizations that threaten U.S national security, and virtually every year new terrorist groups are added to the government's list.[33] Today, the terrorism threat confronting the United States is radically different from the threat posed by al Qaeda in 2001. However, the one thing that remains constant is that terrorists need money to terrorize. At the same time, terrorists have diverse sources of funding. To effectively prevent terrorists from plotting attacks against the United States and killing Americans at home and abroad, the U.S. government must stem the flow of funds to terrorist organizations.

To accomplish this critical objective, the United States should develop a comprehensive counter-terrorist financing (CTF) strategy. No such strategy exists today. The government's CTF strategy must be proactive, not merely reactive, focusing not merely on funding methods currently used by terrorist organizations, but also responding to emerging methods and techniques to collect and transfer funds internationally to support terrorist activities.

The CTF should address how the Islamic State's ill-gotten funds from its various illicit activities are transferred globally to finance its terrorist activities. The strategy should include a plan to curtail terrorist funds derived from each of these revenue sources. Furthermore, the CTF strategy should seek to address how other terrorist organizations are raising money, and what methods they are using to move money globally.

Finally, the CTF strategy needs to be adaptive. As the United States successfully disrupts the flow of funds to terrorists from one source, for example, transactions through financial institutions, the CTF strategy must consider new and alternative methods of money transfer that the terrorists will likely use next. The government's strategy must adjust accordingly and set forth a new plan that curtails the flow of funds to terrorists from this different origin. It is imperative that the U.S. government develop a comprehensive CTF strategy along these lines to more effectively respond to the diverse and innovative methods used to finance global terrorism and disrupt its efforts.

---

[33] As of June 2, 2016, the number was at fifty-eight, to be exact. *See* U.S. Dep't of State, Bureau of Counterterrorism and Countering Violent Extremism, Country Reports on Terrorism 2015, at 349–50, http://www.state.gov/documents/organization/258249.pdf.

Statement of

Celina B. Realuyo*
Professor of Practice
William J. Perry Center for Hemispheric Defense Studies
at National Defense University

on

"Communicating, Cooperating and Collaborating through Public-Private Partnerships to Counter the Financing of Terrorism and Crime"

at a Hearing Entitled

"The Next Terrorist Financiers: Stopping Them Before They Start"

Before the Task Force to Investigate Terrorism Financing,
Committee on Financial Services,
U.S. House of Representatives

June 23, 2016

* The views expressed in this testimony are my own and do not necessarily reflect the views of the William J. Perry Center for Hemispheric Defense Studies, National Defense University, or the Department of Defense.

Thank you Chairman Fitzpatrick, Vice Chairman Pittenger, Ranking Member Lynch, and members of the Task Force to Investigate Terrorism Financing for the opportunity to appear before this committee today to testify on U.S. efforts to combat the financing of terrorism and money laundering that threaten U.S. national security interests at home and abroad. Today we face a broad spectrum of security threats such as global terrorism, transnational organized crime, economic crises, cyber attacks, extreme natural disasters and revisionist states that have made national security more challenging than ever before. The complexity of these security threats, particularly from illicit networks, such as terrorists, criminals and proliferators, requires a multi-disciplinary approach to comprehend and counter them effectively.

The convergence of these illicit networks and the magnitude, velocity and violence associated with their illegal activities are overwhelming governments and threatening state sovereignty and our economy. Governments can no longer guarantee the security, prosperity, rule of law and governance that their people expect and deserve. Often, average citizens who "see something and say something" are the first to recognize anomalies and identify threats; they know their industries, workplaces and communities best. For these reasons, governments need to actively identify and engage partners in the private and civic sectors to better detect, dismantle and deter the bad actors that undermine our security, economy and society. By fostering more robust partnerships among the public, private and civic sectors of society, together, we can better counter the convergence of illicit networks in the U.S. and overseas.

Money serves as the lifeblood for any activity, licit or illicit; financing is the most critical of enablers for terrorism, crime and corruption. In the post-9/11 world, we have witnessed how "following the money trail" has enhanced our efforts to counter the threats around the world. Since international financial flows are not controlled or managed by governments, public-private partnerships with the many facets of the financial services industry are essential in combating threats to the international banking system, such as terrorist financing, money laundering, political corruption and cybercrime. Governments

no longer enjoy a monopoly on national security or the use of force as they did in the past; therefore, they need to adopt a "whole of society" approach to understand and address the evolving threats to our security and prosperity in this globalized world. In the 21st century, all sectors need to communicate, cooperate and collaborate (C^3) through public private partnerships (P^3) to counter the convergence of illicit networks and safeguard national security.

U.S. and Coalition Efforts to Counter the Islamic State in Syria and the Levant (ISIL)

Before elaborating on the importance of public-private sector collaborations to counter threat finance and protect the international financial system, let me provide a contextual update on U.S. and Coalition efforts to counter the financing of ISIL. ISIL is the most prominent example of the terror-crime convergence threatening Iraq, Syria and beyond. "Following the money trail" of ISIL has been instrumental in our understanding and planning for the detection, disruption and dismantling of ISIL and its support networks. The methodical use of the financial instrument of national power, through financial intelligence gathering and targeting key leadership and their critical assets, has degraded ISIL's revenue-generating abilities and its capacity to fund and sustain its criminalized caliphate.

As articulated by the White House, the U.S. has built a global coalition of over 60 partner nations with the goal of degrading and ultimately defeating ISIL. In November 2014, President Obama set forth a comprehensive strategy featuring nine lines of collective effort to counter ISIL:

1. Supporting Effective Governance in Iraq
2. Denying ISIL Safe-Haven
3. Building Partner Capacity
4. Enhancing Intelligence Collection on ISIL
5. Disrupting ISIL's Finances
6. Exposing ISIL's True Nature

7. Disrupting the Flow of Foreign Fighters
8. Protecting the Homeland
9. Humanitarian Support[1]

Since I last appeared before this committee in May 2015, we have witnessed progress on the military and financial fronts of the fight against ISIL. According to the State Department 2015 Country Reports on Terrorism, ISIL remains the greatest threat globally, maintaining a formidable force in Iraq and Syria, including a large number of foreign terrorist fighters. That said, ISIL's capacity and territorial control in Iraq and Syria reached a high point in spring 2015, but began to erode over the second half of the year. For example, at the end of 2015, 40 percent of the territory that ISIL controlled at the beginning of that year had been liberated. In Syria, local forces expelled ISIL fighters from several key cities along the routes connecting the two ISIL strongholds of Raqqa and Mosul, and reclaimed about 11 percent of the territory ISIL once controlled. These losses demonstrated the power of coordinated government action to mobilize against and confront terrorism.[2]

The loss of territory ISIL governs and controls in Iraq and Syria in 2015 also resulted in diminished funds available to it. ISIL relies heavily on extortion and the levying of "taxes" on local populations under its control, as well as oil smuggling, kidnap for ransom, looting, antiquities theft and smuggling, foreign donations and human trafficking. Coalition airstrikes targeted ISIL's energy infrastructure – modular refineries, petroleum storage tanks and crude oil collection points – as well as many millions that were literally stored in bulk cash storage sites. These airstrikes have significantly degraded ISIL's ability to generate revenue. The U.S. led this international effort,

---

[1] The White House, FACT SHEET: The Administration's Strategy to Counter the Islamic State of Iraq and the Levant (ISIL) and the Updated FY 2015 Overseas Contingency Operations Request, November 7, 2014, https://www.whitehouse.gov/the-press-office/2014/11/07/fact-sheet-administration-s-strategy-counter-islamic-state-iraq-and-leva

[2] U.S. State Department Country Reports on Terrorism 2015, Strategic Assessment, http://www.state.gov/j/ct/rls/crt/2015/257513.htm

including through the UN, to confront ISIL's oil smuggling and its antiquities dealing, delivering additional blows to its financial infrastructure.[3]

More recently, appearing before the Senate Armed Services Committee on April 28, 2016, Secretary of Defense Carter described the headway that the Coalition has made to counter ISIL on the military front through "Operation Inherent Resolve."[4] The United States has spent $6.4 billion on counter-IS military operations since August 8, 2014, with an average daily cost of $11.5 million.[5] Secretary Carter said: "We've seen results in targeting ISIL's leaders and finances. We're systematically eliminating ISIL's "cabinet," having taken out its so-called ministers of war and finance. We captured one of the principals of ISIL's chemical warfare enterprise, removed external plotters from the battlefield, and most recently took out the ISIL emir for southern Mosul, weakening ISIL's ranks there. And our attacks on ISIL's economic infrastructure – from oil wells and trucks to cash storage to ISIL's financial leaders – is putting a stranglehold on ISIL's ability to pay its fighters, undermining its ability to govern, and making it harder to attract new recruits.[6]

ISIL is on its heels in Iraq and Syria as the Iraqi armed forces seek to retake control of Fallujah and Mosul, key ISIL strongholds. The Fallujah offensive, which began May 22, follows a series of ISIL defeats in western Anbar province, a longtime Sunni Muslim stronghold and a bastion of support for anti-government militants since the U.S.-led invasion of Iraq in 2003. Iraqi government forces, backed by training, advice and air support from a U.S.-led international coalition, retook Ramadi in December 2015 and Hit four months later. After Fallujah, the northern city of Mosul is the last major

---

[3] *Ibid.*
[4] U.S. Department of Defense Operation Inherent Resolve website, http://www.defense.gov/home/features/2014/0814_iraq/
[5] U.S. Department of Defense, "Operation Inherent Resolve: Targeted Operations against ISIL Terrorists," http://www.defense.gov/News/Special-Reports/0814_Inherent-Resolve
[6] Secretary of Defense Testimony, Statement on Counter-ISIL Operations and U.S. Military Strategy in the Middle East before the Senate Armed Services Committee, As Delivered by Secretary of Defense Ash Carter, Washington, D.C., April 28, 2016 Secretary of Defense Ash Carter Testimony, http://www.defense.gov/News/Speeches/Speech-View/Article/744936/statement-on-counter-isil-operations-and-us-military-strategy-in-the-middle-eas

urban area in Iraq controlled by Islamic State that promises to be a fierce battle against the group.[7]

ISIL - An Adaptive Adversary

While the momentum of the counter-ISIL offensive by the Coalition looks promising on the military and financial fronts, ISIL is proving to be a very adaptive adversary and is expanding its reach well beyond Iraq and Syria. ISIL has a diversified spectrum of criminal and revenue-generating activities that provides it the flexibility to respond to Coalition attacks on its financial infrastructure. Terrorism experts Jean-Charles Brisard and Damien Martinez, in a May 2016 report at the Center for the Analysis of Terrorism, stated "despite the constant airstrikes on its oil infrastructure, ISIL still has a $2 billion empire; and it's making up lost revenue by squeezing the population under its control through raising taxes. ISIL's military defeat is not imminent. As things stand, ISIL economic collapse remains some way off in the mid-term."[8]

The report posits that ISIL made $2.4 billion in 2015, a $500 million drop from the center's revenue estimate the previous year. The main reason ISIL is still making billions is taxes. ISIL's extortion of the people trapped inside its territory in Iraq and Syria has skyrocketed from $360 million in 2014 to $800 million in 2015, according to researchers. According to the U.S. Treasury Department, the Coalition's effort to disrupt the ISIL's economy is working. "We are seeing progress... since late-2015, ISIL's production of oil has declined by about 30%. Their ability to generate revenue has been reduced by at least that much," Treasury said.[9] As oil revenues have declined, ISIL is becoming more reliant on extortion and taxation in the territories that it still occupies. Therefore, re-establishing control of those territories is essential to defeating ISIL militarily, financially, and psychologically.

---

[7] Ghassan Adnan and Asa Fitch, "Iraqi Counterterrorism Forces Enter Fallujah," *Wall Street Journal*, June 8, 2016, http://www.wsj.com/articles/iraqi-counterterrorism-forces-enter-fallujah-1465389277

[8] Jose Pagliery, "ISIS Makes Up for Lost Oil Cash with Rising Taxes and Fees," May 31, 2016, CNN.com, http://money.cnn.com/2016/05/31/news/isis-oil-taxes/

[9] *Ibid.*

ISIL's Influence Beyond Syria and Iraq

ISIL's claim to be a caliphate has raised concerns that its ambitions stretch well beyond Syria and Iraq. The tragic terrorist attacks in Paris on November 13, 2015 and the claimed downing of a Russian plane over the Sinai just weeks earlier demonstrate that ISIL's aspirations are global in nature. ISIL is thinking beyond the Middle East—and, increasingly, it is demonstrating capabilities to act beyond the region as well. Militant groups in Egypt, Nigeria, Pakistan, Afghanistan, Indonesia and the Philippines have taken up the ISIL's trappings and sworn allegiance to its leader, al-Baghdadi. According to the Heritage Foundation, in just two years—from fall 2013 to fall 2015—ISIS established a presence in at least 19 countries.[10]

Libya represents ISIL's new caliphate. According to the State Department, ISIL's branch in Libya was estimated to have up to 5,000 terrorist fighters. The group has seized territory that spans more than 150 miles of Mediterranean coastline between the cities of Tripoli and Benghazi. It also conducted attacks in Libya's oil crescent and in Sabratha, near the border with Tunisia. However, ISIL also suffered losses in Libya in confrontations with militia groups, in particular in the eastern Libyan city of Darnah.[11] The U.S. and its European allies are increasingly concerned about ISIL's expansion in North Africa, have intensified pressure on Libya's divided governments and factions to reconcile, and signaled they are considering expanding military operations there.[12]

The conflicts in Syria and Iraq have attracted foreign fighters by the thousands. Middle Eastern and Western intelligence agencies have raised concern that their citizens who have joined the fighting in Iraq and Syria will become radicalized and then use their

---

[10] Lisa Curtis, Luke Coffey, David Inserra, Daniel Kochis, Walter Lohman, Joshua Meservey, James Phillips and Robin Simcox, *Combatting the ISIS Foreign Fighter Pipeline: A Global Approach*, The Heritage Foundation, January 2016, http://www.heritage.org/research/reports/2016/01/combatting-the-isis-foreign-fighter-pipeline-a-global-approach

[11] U.S. State Department Country Reports on Terrorism 2015, Strategic Assessment, http://www.state.gov/j/ct/rls/crt/2015/257513.htm

[12] Zachary Laub, Online Writer/Editor, and Jonathan Masters, Deputy Editor, *CFR Backgrounder, The Islamic State*, Council on Foreign Relations, March 22, 2016, http://www.cfr.org/iraq/islamic-state/p14811

passports to carry out attacks in their home countries. Unfortunately, we have seen this to be the case in recent terror attacks in Paris and Brussels. U.S. Director of National Intelligence James Clapper estimated in February 2015 that more than thirteen thousand foreign fighters joined Sunni Arab antigovernment extremist groups, including the Islamic State, in Syria, and that more than 3,400 of more than twenty thousand foreign Sunni militants hailed from Western countries. (Estimates of the group's total forces range from around thirty thousand to more than a hundred thousand.)[13]

The influence of ISIL has reached U.S. homeland. In July 2015, FBI Director Comey estimated that upwards of 200 Americans have traveled or attempted to travel to Syria to fight alongside ISIL.[14] In addition to recruiting foreign fighters, ISIL has inspired homegrown terrorists responsible for the deadly December 2015 San Bernardino and more recently the June 12, 2016 Orlando attacks. Just days before the Orlando attack, FBI Director James Comey eerily spoke about the three prongs to the ISIL threat: the recruitment to travel, the recruitment to violence in place, and then what you saw a preview of in Brussels and in Paris — hardened fighters coming out, looking to kill people. Comey reiterated that the FBI has close to 1,000 open cases nationwide involving people at various stages of ISIL recruitment.[15] The Orlando attack at the Pulse nightclub left 49 dead and 53 wounded, representing the deadliest mass shooting in U.S. history. Omar Mateen, a self-radicalized 29-year old U.S. citizen of Afghan descent, who pledged allegiance to ISIL on a 911 call during the attack, perpetrated the terrorist act, according to the initial FBI investigation.[16]

The contemporary threat posed by ISIL to global security has been empowered by a dangerous convergence of terrorism and crime that generates significant income for the

[13] Zachary Laub, Online Writer/Editor, and Jonathan Masters, Deputy Editor, *CFR Backgrounder, The Islamic State*, Council on Foreign Relations, March 22, 2016, http://www.cfr.org/iraq/islamic-state/p14811
[14] Julian Hattem, "FBI: More than 200 Americans have tried to fight for ISIS, *The Hill*, July 8, 2015, http://thehill.com/policy/national-security/247256-more-than-200-americans-tried-to-fight-for-isis-fbi-says
[15] Associated Press, "FBI Director: No Decrease In Number Of US ISIS Cases," Minnesota CBS Local News, June 7, 2016, http://minnesota.cbslocal.com/2016/06/07/fbi-isis/
[16] Ralph Ellis, Ashley Fantz, Faith Karimi and Eliott C. McLaughlin, "Orlando shooting: 49 killed, shooter pledged ISIS allegiance," CNN.com, June 13, 2016, http://www.cnn.com/2016/06/12/us/orlando-nightclub-shooting/

group. The systematic practice of "taxation," oil smuggling, kidnapping for ransom, human trafficking, and antiquities looting across the territory it occupies provide vital resources for the group's military, financial, recruitment, and propaganda campaigns. Continued supply and demand for illicit goods and services, and ISIL control of the supply chains in these criminal markets, provide it with an ideal operating environment its illicit activities that now expands beyond Iraq and Syria. Neutralizing this synergy requires a global coalition that encompassing the public, private and civic sectors on a transnational level. While raising awareness of ISIL's brutal crimes like sexual slavery and antiquities trafficking can reduce demand, the most effective manner to counter it remains the military, financial, and ideological defeat of the ISIL and a reinstatement of control of the occupied territories in Iraq and Syria and beyond.[17]

Public-Private Sector Collaboration to Safeguard the International Financial System

Since the 1970's, the U.S. government recognized the need to work with the private sector to pursue financial crimes like fraud, tax evasion, and money laundering. Under the Bank Secrecy Act of 1970, or BSA for short, U.S. financial institutions are required to assist U.S. government agencies to detect and prevent money laundering. Specifically, the BSA requires banks to keep records of cash purchases, file reports of cash transactions exceeding $10,000, and report suspicious activity that might indicate money laundering, tax evasion, or other criminal activities.[18] Financial institutions are required to know their clients (and their clients' clients), monitor their transactions for anomalies, and report concerns to the authorities.

In the U.S., FinCEN (the Financial Crimes Enforcement Network) serves as the country's financial intelligence unit (FIU), collecting and analyzing suspicious transaction reports; FinCEN has counterparts globally, providing the opportunity for global cooperation. Once it came to light that Al Qaeda used the formal banking system to finance the 9/11 attacks, banks and other financial institutions, concerned with

[17] Celina B. Realuyo, "The ISIS Convergence," *American Foreign Policy Council Defense Dossier*, March 2016, HTTP://WWW.AFPC.ORG/FILES/DEFENSE_DOSSIER_MARCH_ISSUE_16.PDF
[18] U.S. Bank Secrecy Act, FinCEN website, http://www.fincen.gov/statutes_regs/bsa/

reputational risk, realized they had a new and vital task -- to detect and report possible cases of terrorist financing. Now bankers needed to understand and identify how terrorist groups raise, move, store, and use money and what vulnerabilities exist in banking system to prevent future cases of terrorist financing. Not only did the modes and rules change, but so did the forward-leaning posture of the industry which became more motivated to interact and share information with the government and fellow financial institutions.

U.S. Counterterrorism Financing and Anti-Money Laundering Efforts

The U.S. law enforcement and intelligence community works closely with officials at various financial institutions, many of whom have been vetted and hold an active security clearance, to investigate and prosecute specific cases of terrorist financing and money laundering. Increasingly, bank officials are former law enforcement agents or bank regulators. The financial sector has invested billions in human, technological, and financial resources to enhance their AML/CTF (anti-money laundering/counterterrorist financing) compliance capabilities. While these relationships between the public and private sectors have been quite productive, particularly in detecting Iranian sanctions violations, some financial institutions have expressed frustration regarding the lack of information flow from the government on the impact this cooperation has had on actual cases. Not knowing the details about the value of these submissions makes it harder to be compliant and misses the opportunity to fine-tune a company's internal capacity to identify violations and suspicious activity. The private sector continually calls for better two-way communications and more information to justify and effectively direct the immense investment in AML/CTF programs to the board and shareholders who require proof that the money was well spent.

There are many examples of successful venues through which private industry and government work together. In 2010, the Financial Intelligence and Information Sharing Working Group (FIIS WG) was established following the completion of a public-private partnership pilot project under the auspices of the Office of the Director of

National Intelligence's Office of Private Sector Partnerships. The original project's content aside, both the analysts and the business people involved found that the shared communication about threat-finance typologies and red flags was productive. To keep the dialogue going, the participants started a free-standing group which organically blossomed due to the information-sharing gaps in this area. While the group has no affiliation with the government, the FIIS WG is intended to provide experts in the financial services industry and the U.S. government with a forum to informally discuss relevant topics, including protection of critical financial infrastructure, prevention of fraud, and counterterrorist financing and money laundering.

FIIS WG meetings and the relationships formed at those events facilitate information flow and bridge cultural gaps between government and industry. The FIIS WG eventually found a home with the American Security Project, (a non-partisan public policy & research organization in Washington, D.C.) Its members include hundreds of representatives of both public and private sector entities, including regulatory, intelligence, defense, and law enforcement agencies, financial institutions, think tanks, consultancies, and academia.[19] The FIIS WG has become a peer-to-peer community of practice and useful forum to exchange knowledge and experience about red flags, trends, emerging financial technologies, new payment systems, virtual currencies, alternative value systems, and the threats and vulnerabilities that accompany them.

Besides the banks themselves, several trade associations and nongovernmental organizations have become actively involved in raising awareness, training, and educating the financial industry on the threats to the international financial system from financial crimes. One such example is ACAMS, the Association of Certified Anti-Money Laundering Specialists. It is the largest international membership organization dedicated to enhancing the knowledge, skills and expertise in AML/CTF (anti-money laundering and countering terrorist financing) and financial crime detection and prevention. Members represent various financial institutions, regulatory bodies, law enforcement

[19] American Security Project Threat Finance and Financial Intelligence website, http://www.americansecurityproject.org/asymmetric-operations/threat-finance-and-financial-intelligence/

agencies and industry sectors. ACAMS circulates and discusses the latest trends and case studies in money laundering and terrorist financing through seminars, forums, international conferences, and local chapters.[20] The participation of senior U.S. government officials from the Departments of Treasury, Justice, and Homeland Security, the bank regulators, and law enforcement agencies, responsible for combating terrorist financing and money laundering, at ACAMS events demonstrates the active outreach conducted by the U.S. government to promote public-private partnerships.

Countering Emerging Threats to the Financial Sector

Another example of cross-sector collaboration to protect the international financial system is the Financial Services Information Sharing and Analysis Center (FS-ISAC.) It serves as the global financial industry's "go-to" resource for cyber and physical threat intelligence analysis and sharing. FS-ISAC is unique in that it was created by and for members in 1999 to prepare for Y2K and operates as a member-owned nonprofit entity. It was established by the financial services sector in response to the 1998 Presidential Directive 63, (later updated by the 2003 Homeland Security Presidential Directive 7) that mandated that the public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect the U.S. critical infrastructure, of which the financial sector is a vital component.[21]

In response to emerging global threats in cyberspace to the financial sector, FS-ISAC's board extended its charter in 2013 to share information among financial services firms around the world. Constantly gathering reliable and timely information from financial services providers, commercial security firms, federal/national, state and local government agencies, law enforcement and other trusted resources, the FS-ISAC can quickly disseminate physical and cyber threat alerts and other critical information to other organizations. This information includes analysis and recommended solutions from leading industry experts.

[20] ACAMS Mission website, http://www.acams.org/join-acams/#tabbed-nav=what-is-acams
[21] Financial Services Information Sharing and Analysis Center website, https://www.fsisac.com/about

The Center's Critical Infrastructure Notification System (CINS) allows the FS-ISAC to send security alerts to multiple recipients around the globe near-simultaneously, while providing for user authentication and delivery confirmation. The system also provides an anonymous information sharing capability across the entire financial services industry; this protects members' proprietary information and client confidentiality. When they receive a submission, industry experts verify and analyze the threat and identify any recommended solutions before alerting FS-ISAC members. This procedure assures that member firms receive the latest tried-and-true procedures and best practices for guarding against known and emerging security threats.[22] Peer-to-peer collaboration brokered by formal organizations like FS-ISAC, combined with notifications to the appropriate government officials in the U.S. and elsewhere, is an example of timely and effective mechanisms to detect, address, and prevent threats to the financial system in the traditional and cyber domains.

International Cooperation and Public-Private Partnerships

Unilateral, individual country efforts are not enough to counter terrorist financing and money laundering. Our international financial system is far more interconnected and interdependent than ever before. International cooperation between the public and private sectors is therefore paramount. The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the ministers of its 34 member jurisdictions. The FATF sets standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. It serves as a "policy-making body" working to generate the necessary political will to bring about national legislative and regulatory reforms to protect in the global financial system. The FATF has developed a series of recommendations that are recognized as the international standard

[22] *Ibid.*

for combating of money laundering and the financing of terrorism and proliferation of weapons of mass destruction.[23]

The FATF values private sector expertise and operational knowledge, as essential resources to evaluate the application of the AML/CFT requirements to business practices, and to encourage the practical adoption of the standards. The private sector can serve as a helpful sounding board to "test" or assess the potential impact of measures under consideration, or brainstorm on possible technical solutions in a specific field affecting the financial industry. It is also an important way to learn about market developments and access new information regarding emerging threats and vulnerabilities to the global financial system.[24] The FATF Private Sector Consultative Forum is the formal means to reach out to and cooperate with private sector stakeholders. It holds open consultations with interested stakeholders and sets up working groups to examine specific issues including financial innovations like mobile payments, virtual currencies, store of value cards that could be vulnerable to money laundering or terrorist financing.[25] These examples of domestic and international public-private partnership have strengthened the international financial system to detect and deter terrorist financing, money laundering and other financial crimes. According to declassified intelligence reports, groups like Al Qaeda and the Mexican drug cartels decided to refrain from using the formal banking sector due to the enhanced compliance and monitoring measures adopted by the private sector.

Strengthening U.S. Capabilities and Promoting Public-Private Sector Collaboration to Combat Terrorism, Crime and Corruption

The U.S. and its allies have increased their efforts to detect the financing of terrorism and crime, levied economic sanctions, and raised awareness among the private

[23] FATF website, http://www.fatf-gafi.org/about/
[24] FATF Recommendations 2012, "Public and private sector partnership in fighting financial crime," http://www.fatf-gafi.org/documents/documents/publicandprivatesectorpartnershipinfightingfinancialcrime.html
[25] FATF "G8 Public-Private Sector Dialogue on anti-money laundering and countering the financing of terrorism (AML/CFT)," http://www.fatf-gafi.org/publications/fatfgeneral/documents/ppsdsept13.html

and civic sectors about how bad actors can exploit the international financial system to fund their networks and deadly operations. These endeavors to leverage the financial instrument of national power against terrorism, crime and corruption are laudable but could be further expanded at the national, regional and international levels with the following measures:

1. Integrate the financial instrument of national power more deliberately into future U.S. strategies to counter emerging transnational threats;
2. Strengthen U.S. and international financial intelligence and information-sharing mechanisms to more effectively combat terrorism, crime and corruption;
3. Dedicate more financial, human and technological resources to government agencies, responsible for investigating, prosecuting and countering terrorist financing, money laundering and other financial crimes. The 2017 fiscal year budget request for the Treasury Department for the Office of Terrorism and Financial Intelligence was only $117 million to curb terrorist financing, including ISIL financing, and to implement sanctions targeting Iran, North Korea, Syria, as well as $115 million for the Financial Crimes Enforcement Network.[26]
4. Set aside a percentage of forfeited assets and/or fines levied on financial institutions for sanctions evasion, money laundering and compliance infractions to fund domestic and international capacity building programs;
5. Retain and expand a vigorous designation and sanctions regime against state sponsors of terrorism, foreign terrorist organizations, transnational criminal organizations, foreign narcotics kingpins and specially designated nationals;
6. Promote public-private partnerships; raise awareness among bank and non-bank financial institutions of emerging trends in money laundering and terrorist financing to keep up with the unprecedented pace of technological change;
7. Empower the private and civic sectors to actively to detect and deter financial crimes and contribute to counter threat finance strategies and operations; and

[26] U.S. Department of Treasury FY2017 Budget in Brief Fact Sheet, https://www.treasury.gov/about/budget-performance/budget-in-brief/Documents/FY17FactSheet.pdf

8. Encourage more formal research and study of the illicit economy and anticipate how new financial innovations, services, technology, such as virtual currencies and block chain, could possibly be used and abused by terrorists and criminals to finance and facilitate their operations.

In conclusion, terrorists, criminals and their facilitators are presenting complex, asymmetrical threats to U.S. national security interests at home and abroad. The dangerous convergence of illicit networks challenges the sovereignty, security and prosperity of the nation state and must be actively addressed. These illicit networks require critical enablers, most importantly financing, to realize their destructive agendas of terrorism or crime. Stemming the flow of funding to groups, like ISIL, can significantly degrade their violent operations and impact. As these illicit networks adapt and evolve, we must constantly update our methods of detecting, disrupting, dismantling and deterring our adversaries with the financial instrument of national power. Only through proactive interagency, multi-sectorial and international strategies can we effectively counter terrorism, crime and corruption around the world.

Thank you, Mr. Chairman and committee members for your time and attention.

FINANCIAL INTEGRITY
NETWORK

The Honorable Juan C. Zarate
Chairman and Co-Founder
Financial Integrity Network

Chairman and Senior Counselor
Center on Sanctions and Illicit Finance

Former Deputy Assistant to the President and
Deputy National Security Advisor for Combatting Terrorism

Former Assistant Secretary of the Treasury
for Terrorist Financing and Financial Crimes

Testimony before the
House Financial Services Committee
The Task Force to Investigate Terrorism Financing

The Next Terrorist Financiers: Stopping Them Before They Start

June 23, 2016

Juan Zarate
Financial Integrity Network

June 23, 2016

Chairman Fitzpatrick, Ranking Member Lynch, Vice Chairman Pittenger, and distinguished members of the Task Force to Investigate Terrorism Financing. I am honored to testify before you to discuss the evolving challenges and threats from terrorist and illicit financing. I am especially pleased to be testifying with former colleagues and distinguished experts in this field.

Let me begin by commending this Task Force and the Committee for its diligent work and focus on terrorist financing over the past year. This Task Force has resurrected important policy conversations and oversight to ensure the effective application of U.S. tools, information, authorities, and strategies to tackle the challenges of terrorist financing and illicit financing. These are issues that affect our national security and the integrity and strength of the global financial system.

I was privileged to testify at the first hearing on April 22, 2015, and noted at the time that the work of the Committee would prove even more relevant as the terrorist threat evolved and America's enemies adapted to find ways to raise and move money for their causes. I also testified that there would be a need to tackle core issues of transparency and accountability in the global financial system to ensure that we could protect the U.S. financial system from abuse. Much of my testimony today builds on those prior reflections and recommendations.

Since the Task Force began its work, much has happened to underscore the need to focus on terrorist financing and illicit finance – and the importance of the strength, resilience, and integrity of the U.S. and international financial and commercial systems.

- Terrorist organizations and criminal networks have continued to leverage local and regional economies and the global commercial system to both profit and evade scrutiny, with the U.S. and other governments attempting to expose and disrupt significant illicit financial and trade networks and nodes from Panama to Afghanistan.
- Growing regional and proxy battles in the Middle East, South Asia, and Africa have increased the risk that terrorist and militant groups are taking advantage of crises, lack of governance, and fund flows to rejuvenate longstanding financial support from donors, charities, and state sponsors.
- Terrorist infiltration and control of urban environments, populations, and resources – in cities like Mosul, Sirte, and Raqqa -- have complicated how the U.S. government and our allies attempt to disrupt terrorist financing, putting a premium on dislodging terrorist organizations physically from key sites and sources of revenue.
- The application of U.S. law to exclude Hizballah from the Lebanese financial system has created enormous pressure in Lebanon, with Hizballah leadership speaking out against the closing of Hizballah-related bank accounts and a bomb exploding in front of Blom Bank in Beirut on June 12, 2016.
- The Panama Papers and tax-related leaks have raised important questions about the limits of financial transparency, accountability, and traceability and whether the current anti-money laundering/countering the financing of terrorism (AML/CFT) system is effective.
- Complications and burdens on the legitimate financial community in the application of sanctions and financial crime risk management have continued to abut against the public policy needs for financial inclusion.

Juan Zarate
Financial Integrity Network

June 23, 2016

- New technologies enabling the digital economy are providing enormous opportunities for financial access and innovation, but illicit actors are finding ways to leverage tools like digital currency to create illicit bazaars via the Internet and access capital without scrutiny, as seen in the Silk Road and Liberty Reserve cases.
- Continued, significant cyber attacks by state and non-state actors on financial institutions and networks, to include the recent heist affecting the Bangladeshi Central Bank and others via the SWIFT bank-messaging network, have tested the trust in the international financial system and continued to demonstrate that the financial sector remains at the heart of the cyber storm.

These are just some examples and recent developments that continue to illuminate and complicate the terrorist and illicit financing landscape. Billions of dollars in illicit trade and money laundering continue to reach the hands of criminal and illicit actors. There is much work to be done to ensure the United States and our partners around the world are making it harder, costlier, and riskier for terrorist groups and illicit actors to raise and move money across and within borders.

Indeed, the terrorist threat and its underlying ideology have continued to metastasize, and the global threat of terrorism has adapted quickly. Terrorist organizations continue to adapt to the pressure placed on their global financial networks since 9/11 and have learned to raise and manage their own budgets by becoming for-profit organizations taking advantage of the economic resources and opportunities where they operate. Just as the problem of terrorism is more global and diversified today than ever before, the means and resources that networks and groups have to raise and move money have become more varied and localized.

Though under increasing pressure, the so-called Islamic State of Iraq and al-Sham (ISIS) has maintained its hold on key territory – even beyond the Syrian and Iraqi theaters -- and has erased or reshaped borders in the heart of the Middle East. Its finances in Iraq and Syria have been disrupted thanks to targeted air strikes on oil infrastructure and cash centers, but the group continues to raise millions of dollars in revenue and manages a diversified war economy as it attempts to govern and expand its reach.

To contain the global reach of terrorist groups and to thwart the manifestation of their ambitions, we must disrupt their financing and force them to make operational and strategic choices. After 9/11, the U.S. government understood that defending the country and undermining terrorism required deterring, disrupting, and dismantling terrorist funding sources and networks, as these are all essential to the broader counterterrorism mission. Whether it is Al Qaeda, ISIS, or Hizballah, the reality is that terrorist groups need money to operate their networks, logistics, maintain territory or influence, and to plan strategically against the United States and our allies.

Any terrorist group, illicit network, or rogue state seeking significant global reach and impact needs access to the financial and commercial system. Financial flows and budgets become even more important as groups like ISIS, Boko Haram, and al Shabaab attempt to govern and operate local economies.

Juan Zarate
Financial Integrity Network

Money is their enabler, but it's also their Achilles' heel. If you can cut off funding flows to rogue groups or states, you can restrict their ability to operate and govern, and force them to make choices—not only budget decisions, but also strategic choices.

Financial strategies are powerful tools that can constrict our enemies' current activities and their strategic reach. Yes, one suicide bombing may cost a terrorist organization less than $1,000, but if that organization cannot pay for all the sophisticated training it would like, cannot adequately maintain its international alliances, and cannot develop all the programs and operations it imagines, then its ultimate impact will be limited. In maximalist terms, we can alter the enemy's behavior by affecting its bottom line.

The Threat of Terrorist and Illicit Financing

This strategy to combat terrorist financing is not a silver bullet nor is it immune to the enemies' defenses. Terrorists and rogue actors have adapted to this kind of financial pressure.

Terrorist Financing in 2016

ISIS, al Qaeda, and their affiliates have had to adapt, and their affiliates have grown more independent and innovative in developing self-funding mechanisms while individual members and cells use local means to raise necessary funds. The future of terrorist financing parallels the more fractured and localized nature of al Qaeda itself and will present new challenges and opportunities for counterterrorism officials.

ISIS runs a war economy in territory it controls, with a diversified portfolio providing them income. Revenue from running oil operations in Iraq and Syria has been a major source of revenue for the group – as it has taken advantage of the black market in oil, old Iraqi oil smuggling routes, and developed mobile refineries and transport to transact with brokers and even the Assad regime in Syria. The U.S. and coalition airstrikes and pressure on the ground in Iraq have dislodged ISIS from some of its oil infrastructure, but it continues to hold facilities and fields in Syria. It will continue to seek control of oil installations and resources.

With its control of territory and the second largest city in Iraq, Mosul, ISIS is able to tax and extort the local population – raising taxes and fees as pressure mounts – control food supplies to ensure submission by local tribes and populations, engage in kidnap for ransom and other criminality, and trade illegally in antiquities from the historic sites it desecrates. It also had access to approximately ninety banks in the Iraqi territory it controls – which have been ordered cut off from transactions by the Central Bank of Iraq – but may also have maintain access to banks in Syria and continues to have access to currency exchange house and money service businesses in the territories it controls – from Libya to Iraq.

This access to urban environments, economies, and local financial institutions – even small money service businesses -- is different than the safe havens and terrorist financing risks of the past. Their ability to leverage financial institutions, even as they are cut off from cross-border transactions, presents real risks to the legitimate financial system. This makes sanctions and financial crime risk management all the more important now. The territories and economies

terrorists control have allowed them to use economic shields to avoid complete isolation and destruction, as U.S. and coalition forces have to be mindful of civil populations, infrastructure, and to contend with the "day after" effects of ISIS rule.

Fortunately, the pressure against ISIS is reducing its revenues. With less territory under its control, the loss of historic sites like Palmyra, fewer foreigners to kidnap and barter, and reduced access to revenue such as salaries sent into Mosul, its income sources have been hurt. This has forced ISIS to reduce pay to its fighters. Targeting of financiers has helped reduce financial leadership as well.

ISIS is resilient, and this model of financing is not new. For years, al Qaeda in Iraq (AQI) had siphoned oil, extorted and kidnapped for ransom, and robbed banks to raise money, especially as it came under pressure from the U.S. and Iraqi governments. The group attempted to rob the Central Bank of Iraq on June 13, 2010, and engaged in a July 2011 online funding appeal. Now, AQI's successor ISIS robs the coffers of the banks in cities it enters and controls. In Mosul, they raided the Central Bank facility and stole over $600 million. In Sirte, Libya, they stole over $4 million.

In addition, as ISIS continues to grow in prominence among violent Sunni extremists and demonstrates continuously that it is an effective fighting force against President Assad in Syria and his allies in Iran, as well as Shia enemies throughout the Middle East, the group is likely to obtain more funding from foreign donors, in particular from the Gulf, and through crowd-sourcing and other grassroots' fundraising.

The estimates of the ISIS' income and resources vary widely and change as the battlefield shifts, with reports from the Congressional Research Service, the United Nations Al Qaida and Taleban Monitoring Group, and the Financial Action Task Force providing fidelity regarding sources and means of funding. U.S. officials remind us that ISIS must expend resources in order to govern and maintain its momentum, as ISIS is losing ground financially.

ISIS' and al Qaeda's regional outposts also rely more heavily on diffuse and localized funding schemes, often relying on criminal activities such as extortion, kidnapping, and financial fraud that provide fruitful sources of funding. These activities, however, also expose networks and members to attention from local authorities and enforcement.

Al Qaeda in the Islamic Maghreb (AQIM) has mastered the kidnapping for ransom business, taking European hostages and ransoming them to the tune of tens of millions of dollars a year paid for by governments and insurance companies. This, along with AQIM involvement in drug smuggling through the Sahel into Southern Europe, has allowed AQIM to become a funding engine for the broader al Qaeda movement, with support in the past to Boko Haram in Nigeria and perhaps even other sympathetic groups emerging in North Africa. And the al Qaeda affiliate in Somalia, the al Shabaab movement, has created the most diversified and innovative funding, with a combination of taxes and checkpoint fees, diaspora remittances, and a charcoal trade-based money-laundering scheme to raise millions of dollars. This explains why the United Nations has imposed sanctions on charcoal exports from Somalia in an attempt to cut off an important revenue source for the al Shabaab moneymen.

Juan Zarate
Financial Integrity Network

June 23, 2016

Because al Qaeda is seeking alternative financial sources and efficient vehicles for moving money, it will continue to develop relationships and operations that tie its financing to the infrastructure and operations of other organizations. Today, al Qaeda in the Indian Subcontinent (AQIS) relies on donations from sympathizers and supporters in the Persian Gulf and Arab states while also increasingly collaborating and sharing resources with Pakistani based militant groups and leveraging its cells in cities like Karachi. For example, al Qaeda is known to share resources and secure funding from Lashkar e Taiba, Pakistan's largest and most capable terrorist organization. According to General Carter Ham, Boko Haram, al Shabaab, and al Qaeda have shared funds and traded explosives.

Although al Qaeda has been hurt financially, elements of the old funding networks that sustained the Afghan and Arab mujahideen, al Qaeda core, Islamists in Chechnya, AQI, and other elements of the AQ network still exist. Sympathizers, deep-pocket donors, and charities and other organizations can be used to funnel money to sympathetic causes.

These networks have been weakened over time, but they have also revitalized around specific causes important to Islamic extremists, of which the most important now is Syria. Syria is providing the most fertile ground for a resurrection of the old financing and recruitment networks – out of the Arabian Gulf, Iraq, and North Africa – as extremists help drive the fight against Assad in Damascus. With the need and call for humanitarian funding for refugees and those in desperate need, groups like ISIS or Jabhat al Nusra, al Qaeda's Syrian affiliate, can use charity to raise money – and develop their governance and social operations. Dangerously, these groups have learned that to survive in these environments and not be rejected by the populace, they have to fight while baking bread and mending wounds. External funding allows them to do this.

The deepening conflict between Sunni and Shia in countries throughout the Middle East and South Asia – along with the tumult stemming from the Arab Revolutions – is also providing an opportunity for these networks to be rejuvenated. Thus, galvanizing events, conflicts, or causes could help resurrect these established networks and means by which they have justified support for Islamist causes and moved money transnationally, often relying on front companies, traditional hawala, and cash couriers.

Authorities then must maintain scrutiny over these networks and financiers and ensure consistent oversight using existing measures to combat money laundering and terrorism financing. The U.S. government must also press its Gulf allies to prevent the financing of violent extremists groups – quietly and through targeted designations as the Treasury has with respect to terrorist financiers in Qatar and Kuwait. It must also find avenues of cooperation, as with the joint designation on April 7, 2015, of the Al Furqan Foundation Welfare Trust with the Kingdom of Saudi Arabia. Finally, the U.S. government must pressure Iran to stop the facilitation of financing for terrorist groups in and through its territory – including for al Qaeda and the Taleban, as evidenced in the travel from Iran of Taleban leader Mullah Mansour before he was killed, according to press reports.

Juan Zarate
Financial Integrity Network

June 23, 2016

The Blending of Illicit Financial Networks

Importantly, money allows seemingly disparate networks and groups to blend their operations and facilitate their activities. Money – and the potential for profit – grease relationships that would ordinarily never exist. This adaptive collaboration is seen already in the case of drug trafficking, where groups like Hizballah and AQIM have profited from the drug trade from South America through West Africa and the Sahel into Europe. In the past, al Qaeda and groups like Lashkar-e-Taiba (LeT) have benefited from alliances with Indian crime lord Dawood Ibrahim and his organized crime network. The overlaps between the criminal underworld, illicit financial activity, and terrorist operations and funding will continue to evolve as marriages of convenience emerge in common areas of operation. Focusing on key financial conduits, nodes, and networks that serve not just terrorists but transnational criminals will be critical for counterterrorism officials.

The grand global arms traffickers of this era, like Manzar al Kassar and Viktor Bout, have proven this rule. They were willing to service any group or regime willing to pay the right price – often selling arms to warring sides in the same conflict. This principle of opportunistic profit and operations is now implicating the interactions of networks of all ideological stripes. There is money to be made and logistical networks to be harnessed to achieve criminal and political goals.

This blend of purposes is seen most clearly in the conversion of terrorist groups into drug trafficking organizations – like the FARC in Colombia, the Taleban in Afghanistan, and Lebanese Hizballah. With Hizballah, the U.S. government continues to expose the connections between the group and international drug trafficking and money laundering. Recent actions by the DEA and Treasury to dismantle networks of Hizballah's "Business Affairs Component" have exposed financial and trade nodes that the Hizballah operates and led to arrests and enforcement actions around the world. Treasury's Section 311 action against Lebanese Canadian Bank (LCB) in 2011, exposed the hundreds of millions of dollars Hizballah was moving as part of its drug money laundering scheme globally. Overall, the U.S. government has designated Hizballah supporters in twenty countries around the world.

Ideology gives way to opportunity. The reason is money. America's enemies – drug trafficking cartels, organized crime groups, militant groups, and terrorists -- are funding each other, as a matter of convenience and opportunity.

These connections also tie groups together and allow them to work together more broadly. The DEA, the FBI, and the intelligence community have focused more and more attention on the nexus between drugs and terror – with terrorist groups assuming the role of drug trafficking organizations and drug trafficking organizations taking on the characteristics and violent methodologies of terrorist groups. The U.S. Attorney for the Southern District of New York has merged its international drug and foreign terrorism sections because of the intimate link between the two.

Crime can pay, making it an especially attractive avenue for fundraising for networks and groups with global ambitions. Where there is money to be made and moved, financial institutions will

be implicated. Banks and financial intermediaries will continue to weigh the balance between making significant amounts of money while doing business with suspect customers and the need to apply the most stringent financial controls and standards on money flowing through its systems. We have seen this over and over, with multinational banks targeted by regulatory authorities and investigators for taking chances with their efforts to evade sanctions and scrutiny.

Growing Sophistication & Illicit Financing Channels

Illicit financial networks continue to grow in sophistication and take advantage of the international financial system to profit and move money. Sophisticated organized crime groups and drug cartels use the same channels in the international financial and commercial systems to build their financial empires. Drugs, illicit goods, and money all flow, and facilitators and illicit money managers help devise ways to hide and layer transactions and evade scrutiny.

The Panama Papers leaks reveal how corporate vehicles formed by Mossack Fonseca were used by some, like Rami Maklouf (the cousin of Bashar al Assad), and the former Qaddafi regime, to evade sanctions and move and hide millions of dollars in wealth. The recent arrest of "King Midas," the chief money launderer for the Sinaloa cartel in Mexico revealed an intricate network of financial interests that allowed him to handle and hide nearly $4 billion over ten years for the organization, according to press accounts. Treasury actions – to include the Section 311 action against Banca Privada d'Andorra last year – have revealed intricate schemes run by third-party money launderers to move money for clients in Venezuela, Russia, and China. And FinCEN's recent Geographic Targeting Order for high-value real estate purchases in New York and Miami – especially through shell companies -- is an attempt to gather information about a real money laundering vulnerability in the United States.

In many cases, the old methodologies of money laundering and tax evasion are refreshed, with greater awareness of the controls in place through regulation and financial due diligence. Sanctions evasion blends seamlessly into other financial crimes like tax evasion and money laundering. Some money launderers have learned how to game banks' compliance systems and work around existing sanctions and financial crime controls.

New technologies and innovations in the storage and movement of money and value are reshaping the international financial landscape. This is especially the case in developing economies and communities without access to formal financial outlets, which are relying more heavily on mobile devices and mechanisms for storing and transferring money. The pace of growth of these systems in the developing world has been staggering. By 2009, the developing world accounted for three-quarters of the more than four billion mobile handsets in use. Prepaid cards, as an alternate way to store and transfer value, have gained momentum over the years as a replacement for standard currency transactions, with more innovation on the horizon. Crowd sourcing and fundraising facilitated by social media and the Internet – a problem anticipated by a Treasury Department reported issued in 2003 – are now a regular means by which terrorist groups raise and move money.

In addition, the development of online, alternative currencies and new mechanisms for virtual barter will further open the Internet for potential exploitation by illicit actors. The Liberty

Reserve and Silk Road networks demonstrated the rapid evolution of digital illicit marketplaces where all forms of illicit goods and activities – drugs, arms, and human trafficking – were blended and facilitated by digital currencies. The new economy has begun to implicate terrorist financing as well. On November 23, 2011, Philippines police arrested four for involvement in a $2 million remote toll scam that started in 2009. The cell gained access to AT&T customers and telephone operating systems to pass revenues to the suspects or their associates. The group hijacked telephone infrastructure and rerouted calls to collect funds and transfers from unwitting users. These funds were then sent on to support Jemaah Islamiyah, the Indonesian-based al Qaeda network, and Lashkar-e-Taiba.

Tracking the mass volumes of rapid and anonymous money flows around the world and getting in front of new technologies to allow for lawful and appropriate tracking will remain major challenges for law enforcement, intelligence, and regulatory officials, especially because groups and individuals are able to hide and layer their identities and ownership interests. Digital currencies – replacing the traditional use of currency and the traditional controls and chokepoints that are attached to international money flows – have emerged as efficient, yet potentially problematic ways to raise, move, or hide illicit capital.

In many cases, financial interests have served as the impetus for new ways to evade the financial pressure of the United States, new structures to profit from markets of opportunity, and new relationships to subvert the legitimate financial system. The enemy has learned to adapt against the tools and methods used to pressure it financially.

Emerging Challenges to Financial Integrity and Security

The international environment for financial integrity has matured rapidly. There are now clear international standards and heightened expectations for transparency and accountability, with the definition of financial crime expanding to include issues like tax evasion along with the broadened use of financial sanctions to address national security risks. The sanctions and anti-money laundering worlds have begun to blend with expectations that the financial and commercial communities take ownership of managing the real risks to their institutions. Jurisdictions too are now being judged by the effectiveness of their AML/CFT and sanctions systems. Though expectations are high, performance has fallen short and the global effort to protect the integrity of the financial system has proven imperfect and often ineffective.

The Panama Papers revealed systemic weaknesses that have been understood by experts for some time. The leaks have revealed to the public what was already known to many of us. There are corners of the international financial system – in some jurisdictions, certain institutions, and in specific sectors – that have not received the light of international scrutiny and attention. Corporate formation agents and facilitators have often operated under the cloak of bank secrecy or lack of regulation. Investment advisors have not been subjected previously to regulation or scrutiny. Some lawyers have acted as financial facilitators, planners, and conduits for illicit activity. The gatekeepers of significant financial activity have taken advantage of the opacity of corporate structures and often been exempted from anti-money laundering regulation.

Juan Zarate
Financial Integrity Network

This is why the Treasury's new Customer Due Diligence rule, requiring financial institutions to verify the ultimate beneficial owners of companies, is a critical and important step in creating greater transparency in the system. This is also why proposed legislation requiring companies to know and file information on their ultimate beneficial owners is a critical next step to ensure that U.S. companies are not being used by international criminals and sanctions evaders to hide or move illicit capital and investments.

Systemically, there are some additional worrying signs. In Europe, the legal structure and basis for the use of targeted sanctions against individuals and entities, based on United Nations designations, remains under enormous stress. The need to reconcile ex-ante due process for individuals with the preventative demands of asset freezes and designations continues to challenge the mechanism by which the European Union adopts and enforces targeted sanctions. Without a solid foundation and a sustainable system, the European Union and countries will remain reluctant to adopt aggressive measures to stop terrorist financing using these tools.

In addition, the ecosystem that allows for this form of financial warfare and isolation is resilient but fragile. The forced isolation of more and more actors – and the tendency of the private sector to decline doing business in at-risk sectors, jurisdictions, and with suspect actors – raises the possibility of reaching a tipping point where the effectiveness of these tools begins to diminish. This is especially the case when the use of financial sanctions and regulations are used to address more diverse range of diplomatic and political ills and concerns – like human smuggling, child labor, and human rights abuses.

With the threat of financial sanctions, public opprobrium, and the potential erosion of reputation for banking suspect actors, legitimate financial actors are exiting from problematic markets. This raises concerns that less credible or scrupulous financial actors will fill the vacuum. It further raises the concern that legitimate and credible financial institutions will abandon markets most in need of access to capital and an improved culture of compliance and embedding of global standards across the board. For authorities, this would entail a potential loss of visibility into certain financial activity.

We have seen this happening already – with banks stung by enforcement actions and painful, public settlements beginning to exit markets and business lines wholesale, money service businesses in North America struggling to find banking relationships with major banks, and embassies searching to maintain bank accounts in the United States and Switzerland.

An inherent and dynamic tension has emerged between the isolation of suspect behavior from the formal financial system and the incorporation of more of the world into the formal financial system. Going forward, the core principle of isolating and exiling actors from the legitimate financial system for policymakers needs to be balanced with the need to ensure that rogue actors can be captured and affected by the legitimate financial system.

More worrisome, our ability to use these powers could diminish as the economic landscape changes. Treasury's power ultimately stems from the ability of the United States to use its financial powers with global effect. This ability, in turn, derives from the centrality and stability of New York as a global financial center, the importance of the dollar as a reserve currency, and

the demonstration effects of any steps, regulatory or otherwise, taken by the United States in the broader international system.

If the U.S. economy loses its predominance, or the dollar sufficiently weakens, our ability to wage financial warfare against terrorists and America's enemies could wane. It is vital that policymakers and ordinary Americans understand what is at stake and how this new brand of financial warfare evolved. For it is only a matter of time until U.S. competitors use the lessons of the past decade to wage financial battles of their own—especially against the United States.

Opportunities Ahead

The need to combat terrorist financing is just as important today as it was after 9/11. We need to constrict the budgets of ISIS and al Qaeda and to cut the financial and resource links between the groups in order to contain their capabilities, reach, and ambitions. Congress, the Administration, and the private sector must work together in some key areas.

Sharpening Our Tools & Enlisting New Networks

The playbook designed over the past thirteen years is still sharp and can be wielded with effect against targeted actors and networks of concern. The continued reliance on these measures for tactical and strategic purposes by the U.S. government is a testament to their importance. The use of financial intelligence, tools and suasion, enforcement, and financial diplomacy can all be used aggressively to attack terrorist and illicit financing as it hits key chokepoints and the financial system. But the use of these tools must remain strategic, their implementation focused on effectiveness, and they must be reinforced with a strengthened and committed international system devoted to the protection of the international financial system and our collective security.

Indeed, one of the great strengths of the campaign to combat terrorist financing and illicit finance is that it is based on international norms and principles that are subscribed to by all the relevant banking centers and jurisdictions – and now well understood by the private sector. These standards, established by the Financial Action Task Force and reinforced by the World Bank, International Monetary Fund (IMF), the United Nations, and countries around the world, form the baseline for the integrity of a financial system that is intended to be transparent, accountable, and safe. This also means that the sanctions system that has formed the core of these campaigns must be driven by the United States but adopted more fully by the legitimate capitals of the world. They must be encouraged to take on the task of combating terrorist financing in their countries and globally – as we have seen recently in Kenya in the wake of al Shabaab attacks.

The blending of terror and criminality, along with the local means groups are using to raise and move money, expose them to local and regional disruption, even if they are not using the formal financial system. Thus, drug enforcement agents, customs officers, policemen, and tax authorities all become even more relevant in the world of illicit finance – as terrorist groups exploit the seams in the international system. This offers opportunities for the United States and other law enforcement agencies to partner in more creative ways, to amplify the intelligence, financial, and military cooperation that already may exist between countries. We have seen this

kind of partnership bear fruit in countries around the world, as authorities monitor cash couriers, financial crime, and fraud and corruption schemes.

Finally, we need to operationalize the type of financial and strategic suasion that has made the campaign against terrorist financing effective over the past decade. There are new partners in the international system who need to be enlisted as we combat new forms of terrorist financing.

For example, to combat the looting of antiquities for profit by ISIS, the United States should help empower and enlist a whole set of actors and networks already committed to the preservation of peoples, texts, and culture – including leading archaeologists, anthropologists, universities, heritage trusts, museums, libraries, and even activist celebrities. The Antiquities Coalition, UNESCO, and other organizations have already sounded the alarm, and the U.S. should leverage their insights, networks, and activism to stem the flow of funds to ISIS from this trade.

A new coalition should be galvanized to stop the funding of terror and conflict from the illicit wildlife trade – especially the decimation of elephants and rhinos in Africa for their valuable ivory. This trade, which will bring the extinction of some of the world's most magnificent animals, is exploited for profit by terrorist and militant actors, like al Shabaab, the Lord's Resistance Army, and the Janjaweed, along with drug trafficking organizations from South Asia and China. The United States could help galvanize and energize the international efforts to prevent these environment crimes and focus a strategy on disrupting the financial and commercial networks that enable this trade to flourish. This effort would combine the environmental activists with the national security community. In this manner, we could serve both our natural and national security, with a new set of allies in the international system.

The power to affect the budgets of America's enemies is an enormous power that needs to be tended carefully and wielded wisely. And America's enemies – especially nimble terrorist organizations -- will continue to find ways to work around the international pressure and strictures put upon them. This is why the campaign against terrorist financing is not a static venture but instead an ongoing and critical part of the changing terrorist and international security landscape. The U.S. government, led by the Treasury, must continue to innovate and find new ways and partners to make it harder, costlier, and riskier for terrorist groups around the world to raise and move money.

Targeted Unwinding

The United States has grown incredibly sophisticated in the use of sanctions and financial measures to drive strategies of financial exclusion. Yet, as the U.S. Treasury begins to unwind certain sanctions programs and delist individuals and entities from longstanding sanctions lists, the United States should consider how best to manage targeted unwinding measures to achieve our strategic goals. Unwinding can occur because a change of behavior has been achieved, political or diplomatic goals met, or as a tool of continued persuasion. There are good and important reasons to unwind sanctions, but the way in which sanctions are unwound can reinforce our strategic goals and reinforce the influence of our financial measures.

Juan Zarate
Financial Integrity Network

Blunt unwinding may give a rogue regime too much in a deal, could reinforce the regime's hold on power and resources available to it, and may not allow for the targeting of relief to build the private sector or alternates sources of power or influence. It also may not allow for steps – staged or targeted – that would force a regime to change its illicit financial behavior.

This is a challenge now with Iran, Cuba, and even Burma. These are not just risky countries because they are sanctioned regimes and countries. They are inherently suspect and present financial crimes risks because of the nature of their autocratic and corrupt economies, the opacity of their systems, and the use of the economy by the regimes for a range of dangerous or illicit activities.

A system of targeted unwinding could advance the strategic goal that an illicit regime or networks not misuse an economy and financial system to benefit terrorists, proxies, and accelerate its nefarious international ambitions and capabilities. It could also accelerate reforms that match international standards and expectations. If such a system could prove effective, it might spur responsible reform within a country as it tries to reintegrate into the global system. The United States should ensure that it is using its power of unwinding to full effect.

More Aggressive Information Sharing Systems

If the AML/CFT system is to work, there needs to be more a more aggressive and expansive information-sharing environment. In the first instance, this means taking advantage of public-private information sharing systems, like Section 314(a) of the USA PATRIOT Act, to focus collaboration on systemic and real vulnerabilities in key sectors. This moves beyond the classic Bank Secrecy Act system currently in place, but instead entails more targeted collaboration between regulated financial institutions, regulations, and law enforcement to target vulnerabilities and networks of concern. This happens episodically and is taking shape faster in places like the United Kingdom. There needs to be a more aggressive model of cooperation between regulated financial entities and authorities in the United States.

This also means allowing global financial institutions the ability to share suspect account and transactional information across borders within their institutions. Currently, privacy and data protection laws often impede an institution's ability to share data within its own network. Without this, a financial institution may not see the risks and vulnerabilities in its own system without costly or time-consuming work arounds. This is a 20th century model crashing against a 21st century economy and expectations. With illicit actors moving at the speed of the digital economy, these roadblocks to internal information sharing have to be overcome or removed.

Importantly, Section 314(b) of the Patriot Act must be expanded to allow financial institutions to share information within their respective sectors more consistently and rapidly. This requires that we begin to think about information sharing in the private sector as enabling the discovery of sector-wide vulnerabilities – like criminal networks that use multiple accounts at different institutions – as well as the effectiveness of our preventative measures against sector-wide risks. With the onset of new technologies that facilitate the collection of big data and predictive analysis, technology firms should help regulated industries create models that allow the private

sector to share and analyze data more rapidly and effectively, while sharing the burden and costs of compliance.

We need to begin to think differently about how information is shared, analyzed, and used to protect the integrity of the financial system and our national security.

Balancing Financial Exclusion and Inclusion by Sharing the Risk

Governments have been demanding regulated financial communities to serve as gatekeepers of the financial system, so as to ensure that systems and institutions are not misused by criminal or terrorist actors. Governments have equally been concerned that institutions, particularly major global banks, have exited from specific markets, business lines, and customers in reaction to perceived regulatory and real risk. The global banks have felt whipsawed by this dual message and pressure, while sectors such as money service businesses and certain communities have found themselves without banking services.

Where there is a need for financial services or international flows of funds, the international community should find a way of facilitating such flows. When those financial flows or transactions – as with remittances to and in conflict zones -- represent heightened and perhaps unmanageable sanctions and financial crime risk, then there needs to be a shared solution to create safe corridors or channels for such financial activity.

If such flows are important to unstable economies or remittance-dependent countries, then governments and international financial institutions, like the IMF and World Bank, need to devise ways to build comfort in the risks that can be taken by providing safe channels for flows or helping to validate ecosystems of financial transparency that meet acceptable international standards. No system is perfect, and in a risk-based AML/CFT model there is an acceptance of a certain degree of risk. Without some public sector or international assumption of risk, the private sector will avoid environments that present costly and unjustifiable risk. The twin goals of financial integrity and inclusion can be met with some creative collaboration.

Focusing on Effectiveness of the AML/CFT and Sanctions Systems

The United States should continue to focus its domestic and international efforts on the effective implementation of the AML/CFT system globally. This is not just about supporting the efforts of the Financial Action Task Force to assess jurisdictions – though that is critical. This is about ensuring that international norms, sanctions, and the heightened expectations in the international system are being met and reinforced.

The United States must remain committed to its own financial transparency. Our economy cannot be seen or used as a money-laundering conduit or haven for illicit actors of any stripe. We need the transparency envisioned in the recently published CDD rule and the proposed beneficial ownership legislation presently before the Congress. This will entail demanding similar transparency and regulation in jurisdictions around the world, including those emerging as major economies or out from under sanctions.

Juan Zarate
Financial Integrity Network

June 23, 2016

The United States must continue to enforce sanctions and its financial crimes and anti-corruption laws to ensure that financial security threats are being addressed. The United States has consistently been the driver in using its toolkit to expose terrorist and criminal networks, and its work to enforce anti-corruption laws has resulted in global impact, as seen in the FIFA corruption cases. The United States should not be shy in driving enforcement, as long as it is justified by the facts and clearly intended to meet the demands of the U.S. legal system and international norms. It should also ask the same of its partners, especially the enforcement of sanctions which is often left to the United States.

With the private sector, the United States should find ways of building the capacity of the financial sector to manage financial crimes and sanctions risk. This entails engaging key jurisdictions and working with partners to ensure financial institutions of various sizes and sophistication understand their obligations and how to meet them. American efforts to ensure the integrity of the financial system depends on its effective implementation globally.

Addressing the Convergence of Cyber and Financial Warfare

The frequency and sophistication of attacks on banks are increasing, with each attack representing a more dangerous intrusion and demonstration of systemic vulnerabilities. The recent attacks on the SWIFT system were a wake-up call for the international community that the systemic vulnerabilities are real. CitiBank alone reports ten million cyber attacks on its system a month. Banks are prime targets for sophisticated, organized cyber criminals. Banks hold not just money and customer accounts, but also collect and centralize sensitive customer data and some clients' intellectual property.

More importantly, banks have been pulled into a more serious and sustained cyber financial battle. Nation states and their proxies realize that banks serve as both key systemic actors important for the functioning of the global economy and as chief protagonists in the isolation of rogue regimes and actors from the financial system. Thus, the financial community finds itself drawn into combined financial and cyber battles – neither of which it controls. This has led cyber security experts in the banking community to admit openly, "We are at war."

Western banks and the financial system are now encountering the convergence between economic and cyber warfare. Major and minor state powers, along with super-empowered individuals and networks, can harness economic interdependence and cyber weapons to increase their global power status at the expense of their geopolitical rivals. The danger emerging is a coalition of actors – perhaps states using non-state proxies in cyber space -- launching financial and cyber assaults.

The need for urgent attention to this convergence within the financial community and among Washington policymakers is clear. The current level of interaction between stakeholders is not sufficient to address the growing threat from cyber financial attacks. There needs to be a more aggressive approach to private sector defense of its systems and public-private collaboration to defend critical financial systems.

Juan Zarate
Financial Integrity Network

June 23, 2016

This approach would borrow in part from the post 9/11 anti-money laundering and sanctions model to leverage financial suasion against rogue capital and actors as a way of protecting the financial system. The President's April 1, 2015 Executive Order allowing for the use of sanctions to address malicious cyber activity is an important cornerstone to this approach and related cyber financial deterrence. This would also entail a more aggressive "cyber privateering" model to empower and enlist the private sector to better defend its systems in coordination with the government.

We need to begin to address the convergence of cyber and financial warfare as the leading front in systemic vulnerabilities to the integrity and safety of the international financial system.

All of these measures will help maintain core elements of the U.S. toolkit and ensure we are able to drive the international agenda to isolate terrorist and rogue actors. It will also help build more integrity and security in the international financial system.

Strategic Impact of the Counter Terrorist Financing Mission

The strategies that resulted in this period after 9/11 focused squarely on protecting the broader international financial system and using financial tools to put pressure on legitimate financial institutions to reject dealings with terrorists, rogue and illicit financial actors. The use of this type of financial power and its focus on terrorist financing in particular have revealed some fundamental policy issues and paved the way for new ways of thinking about national security.

The focus on financial intelligence continues to reveal links and associations between America's enemies and networks – otherwise unseen through conventional intelligence. Financial trails don't lie, and they can reveal relationships of convenience and for profit, such as between al Qaeda and Iran or between groups like Hizballah and al Qaeda in the Islamic Maghreb and South American drug cartels. The "follow the money" doctrine and financial network analysis puts into relief both emerging threats and the enemies' vulnerabilities.

Treasury's designation process – which reveals openly and notoriously the underlying financial infrastructure of terrorist organizations and rogue groups – not only resulted in international financial isolation but also raises difficult and fundamental issues of national security import. For example, the question of how to deal with Gulf allies – such as Qatar and Kuwait – that have supported extremist causes and groups, especially in the wake of the Syrian crisis, often come through the designation process. In addition, new debates emerged and continue to be relevant, including how to treat organizations like the Muslim Brotherhood, with its leadership raising money and advocating the use of suicide bombers. The question of how to treat financial facilitation should continue to emerge difficult policy questions.

The targeting of financial facilitators also provided novel insights for a new type of deterrence. Though a terrorist trigger puller may not be deterrable in the last instant of an attack, others in the network and business cycle – like bankers and financiers -- could be deterred if they recognized that their resources and legitimacy were at risk. Such deterrence – whether public or quiet -- could affect the availability of capital and the ability of networks to execute significant plots and expand global networks. This insight also allowed us to think differently about how to

affect weapon of mass destruction (WMD)-terrorism by looking at the threat as a business cycle – from the source of nuclear material to the smugglers and facilitators to the end users. Deterrence then was not just aimed at suicide attackers but instead at all of those in the cycle who might touch on the proliferation and deployment of WMD. The focus on financial support to America's enemies will continue to present new opportunities to influence their activities.

In addition, it is in the context of financial warfare that the United States experienced its most consistent questions and tradeoffs about the use of cyber weapons to disrupt the enemy's financial resources. Concern over the effects on the financial system and confidence in the United States as the keeper of the modern capitalist system has constrained the use of such weapons. Ironically, this is the arena in which the United States financial system now faces its greatest vulnerability.

Importantly, using financial power and suasion to affect America's enemies and their budgets – well beyond U.S. borders – provided a form of asymmetric power that the United States could use against non-state networks exploiting the global system. In many ways, this was a strategic window into a new way to leverage power in the 21st century – which does not require kinetics and relies heavily on the influence and decisions of private sector actors. Devising and leveraging this new type of strategic suasion is a critical and new way of thinking about how to leverage American power as power dynamics devolve and shift globally.

A Comprehensive U.S. National Economic Strategy

The tools discussed and the strategies of financial exclusion need to be embedded in broader strategies of national and economic security. The United States and the international community have begun to wrestle with the complications of an interconnected global environment where economic power, access to resources, and cutting-edge technologies are redefining national power. The myriad vulnerabilities and opportunities in this shifting landscape require a new national economic security strategy.

Countries such as China and Russia are already playing a new geo-economic game, where economic power is leveraged aggressively for national advantage. In this vein, the United States should concentrate on sharpening its tools and reinforce the strength and resilience of a transparent international financial system, along with its partners. This should not just be a strategy of financial exclusion.

The United States should find ways to develop strategies of financial inclusion, using its economic influence, private investment, and commercial interests abroad to help allies, reinforce strategic interests, and complement the strategies of financial exclusion. Good behavior and allies around the world should be rewarded with investment and opportunities to work with the United States and our private sector, and U.S. economic tools should not be seen as simply confined to the quiver of economic sanctions.

Importantly, the United States should develop defensive economic strategies with our allies to counter the potential influence and pressure that countries like Russia and China may wield. International alliances should be recast to ensure key resource and supply redundancy, while

Juan Zarate
Financial Integrity Network

trade deals should create new opportunities for influence and economic advantage. The Trans-Pacific Partnership is a major step in the right direction. The United States should deploy new doctrines of deterrence like a "boomerang deterrent" making it patently unwise for countries to try to attack or weaken the U.S. given the entanglement of the international commercial and financial systems.

The U.S. government's approach to its economic vulnerabilities is also scattered – with strategies to protect supply chain security, combat transnational organised crime, secure the cyber domain, protect critical infrastructure, and promote U.S. private sector interests abroad to compete with state-owned enterprises. As the Venn diagram of economic and national security overlaps ever more exactly, the U.S. should craft a deliberate strategy that aligns economic strength with national security interests more explicitly and completely. It should also design this strategy with its allies squarely in mind.

The intelligence community should prioritise collection and analysis to focus on the global landscape through this lens. The Departments of Commerce, Energy, and Defense should sit down together – and then with the private sector – to determine how to maintain investments and access to strategic materials and capabilities critical to national security. Our homeland security enterprise should focus on protecting and building redundancies in the key infrastructure and digital systems essential for national survival. Law enforcement and regulators should have access to beneficial ownership information for suspect investments and companies formed in the United States.

The U.S. president should also review the traditional divide between the public and private sectors where cooperation is essential. We should view the relationship between government agencies – such as the Export-Import Bank, Overseas Private Investment Corporation (OPIC), and USAID – and businesses as core to the promotion of U.S. interests, creating alliances based not just on trade and development but also on shared economic vulnerabilities and opportunities. The White House needs to ensure that its national security and economic experts are sitting at the same table crafting and driving the strategy while consulting the private sector.

In doing this, the U.S. and Western liberal democracies must reaffirm their core principles. Western capitalist societies should not strive to be like either China or Russia, and analysts should not automatically overestimate the strength of such alternate systems and inadvertently create structures that move us towards a state authoritarian model. On the contrary, the United States should commit to remaining the vanguard of the global free trade, capitalist system, while preserving the independence of the private sector and promoting ethical American business practices. The United States and its allies should not retreat from the globalised environment they helped shape but instead take full advantage of the innovation and international appeal of American and Western business and technology.

In the twenty-first century, economic security underpins the nation's ability to project its power and influence. The United States must remain true to its values but start playing a new, deliberate game of geo-economics to ensure its continued security and strength.

Juan Zarate
Financial Integrity Network

June 23, 2016

Thank you again for the privilege of testifying. I would be happy to answer any questions and provide more detail as requested.