Congressional Testimony

The Honorable Juan C. Zarate
Chairman and Senior Counselor
FDD's Center on Sanctions and Illicit Finance

Chairman and Co-Founder
Financial Integrity Network

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
Task Force to Investigate Terrorism Financing

The Next Terrorist Financiers: Stopping Them Before They Start

June 23, 2016

Center on Sanctions & Illicit Finance
FOUNDATION FOR DEFENSE OF DEMOCRACIES

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 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 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.

- 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 cyberattacks 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 Hezbollah, 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.

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 it 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 and 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 kidnapping 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, it raided the Central Bank facility and stole over $600 million. In Sirte, Libya, it 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-Qaeda and Taliban 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.

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 mujahedeen, 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 Taliban, as evidenced in the travel from Iran of Taliban leader Mullah Mansour before he was killed, according to press reports.

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 Hezbollah 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 Taliban in Afghanistan, and Lebanese Hezbollah. With Hezbollah, 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 Hezbollah's "Business Affairs Component" have exposed financial and trade nodes that the Hezbollah 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 Hezbollah was moving as part of its drug money laundering scheme globally. Overall, the U.S. government has designated Hezbollah 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.

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.

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.

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 depend 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 cyberattacks 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.

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 Hezbollah 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 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 organized 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 prioritize 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 globalized environment they helped shape but instead take full advantage of the innovation and international appeal of American and Western business and technology.

In the 21st 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.

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