

House Foreign Affairs Committee

Sanctions and Financial Pressure: Major National Security Tools

HON. JUAN ZARATE

Chairman and Senior Counselor
FDD's Center on Sanctions and Illicit Finance

Chairman
Financial Integrity Network

Washington, DC
January 10, 2018

Chairman Royce, Ranking Member Engel, and distinguished members of the U.S. House of Representatives Committee on Foreign Affairs, I am honored to be with you today to discuss the role of sanctions and financial pressure in our national security. I want to thank Chairman Royce for his leadership of this Committee and years of diligent work on the Hill and in the foreign policy community. I am grateful for the sober work we did together on issues of national security. Your voice of reason, seriousness of purpose, and compassionate and strong vision for America's place in the world will be missed in Southern California, Congress, and in Washington.

I have been privileged to serve in the U.S. government – at the U.S. Justice Department, the Treasury Department, and at the National Security Council – spending much of my time developing the tools, strategies, and institutions of economic statecraft since September 11th. Among other developments in this period, the establishment of the Office of Terrorism and Financial Intelligence (TFI) at the U.S. Treasury signaled the U.S. government's recognition of the importance of Treasury's tools and suasion, financial intelligence, and financial pressure campaigns in our national security architecture.

Since leaving government in 2009, I have continued to work with think tanks, in academia, and in the consulting worlds to develop the understanding, strategies, and capacity in this space. The publication of my book, "Treasury's War: The Unleashing of a New Era of Financial Warfare," in 2013, was my attempt to explain the evolution and importance of financial and economic tools in our national security – and the critical nature of these issues for the international community in the years to come. Our founding of the Financial Integrity Network (FIN) almost four years ago signaled a desire to help clients meet heightened global expectations of financial integrity, to build the capacity and design new models to address the complexities of this environment, and to make the tools that protect the international financial system more effective. The establishment of the Center on Sanctions and Illicit Finance (CSIF) at the Foundation for Defense of Democracies (FDD) in November 2014, represented our commitment to create a think tank dedicated to developing the doctrines and strategies of national economic security, especially in the face of new challenges to U.S. power.

This background and ongoing work has afforded me insights and learning that I hope will be helpful to this Committee and Congress. Thank you again for the invitation to testify.

This is an important moment to take stock of the critical role that financial measures, including sanctions, play in our national security. These economic and financial tools of coercion have traditionally filled a gap in the national security toolkit between diplomacy and kinetic action. Over the past fifteen years, they have become the tools of first resort and even our central strategies in dealing with the hardest national security challenges facing our country.

Financial pressure campaigns have shaped our approaches to threats from nation states like Iran, North Korea, and Russia and non-state actors like terrorists, human rights violators, and malicious cyber actors; empowered the United States and the international community to address broad sets of transnational threats, like proliferation, transnational organized crime, sanctions evasion, and corruption; and enabled and complemented our diplomacy, law enforcement,



intelligence, and military efforts. These are measures aimed not just at rogue actors but are intended fundamentally to protect the integrity of the U.S. and international financial system.

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.

These tools can also be seen as convenient to use relative to other national security measures, serving as a clear statement of policy and allowing a public demonstration of the steps taken in response to crises or direct threats. There is a danger of overuse and a diminishment of their value and effectiveness if they are not deployed carefully and with clear strategic intent, especially given the burdens placed on the private sector to implement many of these measures.

As the United States and international community rely more heavily on these tools of economic statecraft, it is critical that we ensure their effectiveness, legitimacy, and preserve and strengthen the ability of the United States to use strategies of economic coercion against threats to U.S. national security. Congress plays a key role in this endeavor.

In recent years, Congress has taken an even more active role in the expansion and use of sanctions and financial measures in U.S. policy, as seen in key pieces of legislation over time like Title III of the USA PATRIOT Act in 2001, the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 (CISADA), the Hizballah International Financing Prevention Act of 2015 (HIFPA), and the Global Magnitsky Human Rights Accountability Act of 2016. This Committee has played a major role in this work. How Congress steers the evolution of the use of financial and economic measures, working together with the Administration, will be critical to the credibility of U.S. efforts and the sustainability of these tools and strategies.

This is especially important as the targets of U.S. measures adapt to pressure, the financial and economic environment globally grows more interdependent and complicated, competitors or adversaries seek to displace or undermine U.S. dominance and the U.S. dollar in the international financial system, and as new technologies enable economic and financial relationships between illicit actors.

Ultimately, the United States has a deep interest in preserving and deepening its ability to protect the integrity of the financial system and marshal economic and financial measures to address national and international security concerns.

Core Principles for the Use of Financial and Economic Measures

There are fundamental principles that should drive any serious use of sanctions, financial measures, or the deployment of an economic pressure campaign. These principles should inform the design, choreography, and strategy deployed before launching any type of sanction or form of economic coercion.



1. *Strategy Matters.* To be effective, an attempt to use sanctions or financial measures of any sort must nest within a coherent strategy and cannot stand alone. Too often, sanctions have been seen as either the only retreat for action to address a thorny national security issue, or as a silver bullet that can bend behavior and alter a threat landscape on its own. For any financial pressure campaign to work, it must be in service of an understood strategy and complemented by other tools of statecraft, power, and coercion. These tools can be used to deny access to the global financial and commercial system and disrupt the capabilities of actors in achieving their goals – be it preventing the development of weapons of mass destruction in the case of Iran and North Korea, deterrence against continued aggression as in the case of Russia, or disruption of broad global reach for terrorist groups.

Ultimately, these are measures that enable the United States and the international community to make it harder, costlier, and riskier for illicit actors and rogue states to raise and move money globally. In maximalist form, these tools can affect the budget, bottom line, and decision-making of the targeted regimes or networks. The strategy of economic coercion must then be crafted to achieve the defined goal.

2. *Coercive Tools in Concert.* The sanctions and economic toolkit must be seen as part of a broader set of coercive tools that are more effective when deployed in concert to shape the environment. In the case of North Korea, interdiction of suspect North Korean shipping, arrests of those involved in North Korean illicit financial activity, broad-based information campaigns to weaken the regime's control of the information environment, and an aggressive focus on the regime's human rights abuses are all complementary and functional parts of any campaign to isolate the North Korean economy and affect the regime's decision-making. These are also tools that should target, impact, and deter those who do business or finance the regime's activities. Sanctions must be seen as part of a broader effort to disrupt the target's ability to resource its ambitions and access the key elements of the financial and commercial system.
3. *Constant, Consistent Pressure and Enforcement.* For a financial pressure campaign to work, it must be applied and enforced constantly to identify and isolate the targeted behavior. Often, U.S. and international sanctions and pressure have suffered from applying an escalatory model based simply on reactions to provocations and violations of existing sanctions. Such sanctions have been perceived as important primarily in aid of diplomacy. Although that is a critical use of these tools, in order to be effective, they must be seen as their own form of pressure, coercion, and disruption that complements our diplomacy. As in the case of North Korea and Russia, some sanctions have been dictated more by the provocations of the regime as opposed to what an effective financial and economic pressure campaign should look like. Any use of sanctions must be part of a broader campaign to sensitize the international community and markets to exclude rogue actors involved with sanctioned parties from the legitimate financial and commercial system. This includes targeting sanctions evasion as its own threat and source of illicit finance worthy of focused enforcement attention. Like weeding a garden, such work has to be consistent and constant, to shape market and governments' behavior.



4. *Conduct-Based Focus.* A successful, sustainable campaign against rogue regimes and dangerous networks that enlists key allies and stakeholders should focus intently on conduct-based sanctions and measures that target the illicit, dangerous, and suspicious activities that violate international norms and principles and put the financial system at risk. A fundamental vulnerability for North Korea is that it is not only developing nuclear weapons capabilities in violation of international sanctions, but it is a criminal state. It is engaged in proliferation, massive human rights abuses, money laundering, corruption, sanctions evasion, counterfeiting, smuggling, drug trafficking, and other nefarious and suspect activities. A clear vulnerability for Iran is that the regime is corrupt, engaged in nefarious and illegal activities (from support to terror to cyber intrusions), and the Islamic Revolutionary Guard Corps controls – overtly and with a hidden hand -- many of the key sectors and elements of the economy.

Illicit or inherently suspect activities are interwoven into how many sanctioned parties do business – and try to avoid sanctions -- and should be isolated by the international community – governments and the private sector alike – regardless of the diplomatic posture. Such activities are the subject of sanctions, criminal laws, and financial regulations. At a time of heightened concern over transparency and accountability in the financial system, there should be no objection to doing so, especially in major economies and legitimate financial centers. As long as sanctions and related efforts to target illicit networks and their supporting financial and commercial infrastructure remain focused on the activities that violate accepted international norms and principles, they will prove more effective and be amplified by the actions of the private sector and actors concerned about real and reputational risk.

5. *Creativity and Flexibility in Application.* The use of sanctions and financial measures must be tailored to the desired strategies and targets, and we must remain open and flexible to new approaches in the application of these tools. The same playbook that has been used successfully for prior campaigns may not be the right approach for the next or a different campaign. A maximalist approach of full financial and economic isolation at once – especially at the outset of a financial and economic pressure campaign -- may not be the most effective way of using these tools. In some cases the mere threat of the use of sanctions, as with secondary sanctions or the potential application of Section 311 of the Patriot Act, can affect behavior and meet desired U.S. goals. In other cases, a phased constriction campaign, addressing specific vulnerabilities, risks, and threats over time, may be most helpful to deter actors or to ensure the longevity and effectiveness of any measures imposed. In addition, there may be a need for more creativity in the use of other kinds of sanctions, regulations, or financial measures – as with the targeting of specific types or categories of transactions or the phased unwinding of sanctions or regulations. The use of the Sectoral Sanctions List in the Russia context, the restrictions on types of debt and equity sanctioned under that program, and the application of Section 311 against “bad banks” for a range of illicit financial activity are good examples of this type of creativity.



6. *Protecting the Integrity of the Financial System in Practice.* A core pillar of the current environment is the idea that the anti-money laundering/countering the financing of terrorism (AML/CFT) system and related measures are designed to protect the integrity of the financial system. This is a preventative model that over time has required greater transparency, accountability, and traceability within the financial system. Though imperfect in many ways, the effectiveness of the AML/CFT regime underlies the ability to use sanctions and other financial and economic measures to exclude rogue actors from the financial system. If sanctions screening is to work, banks and other regulated financial institutions must know their customer and understand ownership and control interests for entities using their facilities to transact around the world. These tools of financial exclusion must be balanced with demands and utility of financial inclusion. All of this requires Congress and the Administration to recognize that the tools of financial and economic coercion are highly dependent on the effectiveness of the AML/CFT regime and the integrity of the financial system. These disciplines are often treated as separate endeavors or even industries. In practice, they are two sides of the same coin with sanctions and AML/CFT blending ever more neatly in the age of conduct-based sanctions and the growing use of financial regulations like Section 311, which have the effect of sanctions.

7. *International Norm Setting, Cooperation, and Legitimacy.* The United States has the ability to impact globally with its financial and economic might -- the size and attractiveness of the U.S. economy, the role of the dollar as the chief reserve and trading currency, and the historic credibility and importance of U.S. authorities. This gives global reach to even unilateral U.S. measures. But the authority to sanction or exclude actors from the U.S. and global financial system should be used wisely, when possible in concert with other countries and institutions like the United Nations, and with a clear understanding with the private sector of the regulatory expectations. They should also be used while understanding and tending to the legal foundation of these measures along with serious concerns for privacy and civil liberties.

The long-term legitimacy of any action is dependent on whether financial and economic measures are taken in furtherance and in support of accepted international norms and can be supported by facts. The strength of our campaign to pressure Iran revolved around the isolation of suspect Iranian actors and the key sectors because of underlying prohibited or nefarious behavior in violation of international norms and sanctions – along with our ability to demonstrate to governments and private sector actors the real risks that Iran presented to the financial system. Prohibitions on support to terrorism, proliferation of weapons of mass destruction, money laundering, financial criminality, and corruption are all norms and requirements understood by legitimate actors in the public and private domains. Basing economic campaigns less on political decisions and diplomatic predilections and more on underlying conduct that affects both international security and the integrity of the financial system helps support the legitimacy of these actions. Continuing to set these norms, in cooperation with the major players in the global system and in organizations like the Financial Action Task Force, is essential to our effective use of these tools.



Urgency Attached to Effective Action

Ensuring the effective application and use of these measures is critical given the importance and complexity of these measures and the national security strategies affected. With the broadening and deepening of the application of sanctions to more conflicts, targets and types, and transnational conduct of concern – to include corruption, malicious cyber activity, and human rights violations – sustaining application with sufficient resources and policy attention becomes all the more important.

There is real urgency attached to this work. In the case of North Korea, there must be an all-out campaign to leverage financial information, sanctions, interdictions, and related financial measures to squeeze the regime's finances and access to capital. More importantly, these measures should be used to attempt to alter the dynamics with China by putting fundamental Chinese interests at risk – without needing to threaten China directly -- so they use their leverage to affect Pyongyang's decision-making.

This includes sanctioning entities – regardless of nationality or type – assisting North Korea to evade sanctions or engage in illicit or suspect financial or commercial activity; committing to a permanent and aggressive multi-national maritime interdiction campaign to address proliferation concerns, building off the Proliferation Security Initiative; deploying a multi-layered missile defense strategy that guards against missiles that can hit U.S. interests, allies, and U.S. territories, States, and the mainland; pursuing an aggressive anti-corruption/kleptocracy initiative to prosecute those profiting illegally or in violation of sanctions from dealings with Pyongyang and recovering any leadership-related assets; uncovering and designating those financially facilitating or profiting from human rights violations, cyber incursions, or proliferation activity. Other measures tied to monitoring of oil, coal, guest workers, and other trade proscribed under the current United Nations sanctions could tighten scrutiny and provide other avenues for enforcement actions. Under these conditions, it should be incredibly uncomfortable and fundamentally threatening for any country or entity to do business with Pyongyang.

With Iran, measures to isolate and pressure the Revolutionary Guard and the regime leadership – by spotlighting human rights abuses, corruption, support to terrorists and militant proxies, and the progress of their ballistic missile program in violation of UN sanctions – can be undertaken right away, regardless of one's view of the Joint Comprehensive Plan of Action (JCPOA) and would be consistent with that agreement's allowance for the application of non-nuclear sanctions.

With Russia, the United States must maintain escalatory dominance along with its European allies in the use of sanctions and economic statecraft – focusing ever more attention on Russia's continued aggression in Ukraine, Putin's corruption, support for Assad's regime in Syria and related human rights abuses, and malicious cyber activity. In the face of Russian use of its own economic and energy tools – along with its attempts to displace the U.S. dollar in the international financial system – the United States must maintain this pressure as a weapon of coercion, while being sensitive to European dependencies. Even if this does not roll back Russia's hold on Crimea, such measures should be used to deter further Russia aggression – in the physical and virtual worlds – against the United States and our allies.



In Venezuela, the use of sanctions to isolate the regime further by highlighting human rights abuses and corruption as the economy implodes and the regime descends further into dictatorship has to be handled with humanitarian designs squarely in mind to support the people.

With global terrorist organizations, continuing to apply financial pressure on the key dependencies and chokepoints for their financial infrastructure in the formal and informal system will be critical. This is especially the case for those terrorist groups, like Hizballah, which have a global, criminal footprint and a broad commercial and financial support mechanism.

And with transnational issues like proliferation finance, transnational organized crime, cyber hacking, and kleptocracy, where global financial networks support both illicit financial dealings and dangerous activity threatening to the United States, there is urgency to attacking the financial underpinnings that allow these networks to profit, connect dangerous actors, and undermine global security and governance.

There are many more programs and areas of focus, but in all of these campaigns, there is a need to ensure that the United States and its allies understand and can undermine the financial vulnerabilities of dangerous actors in the international system. Given the stakes, ensuring effectiveness of this system is all the more important now.

Improvement in Application of Sanctions and Financial Measures

There are certain overarching themes and issues that deserve focus if these financial measures are to remain effective and are to amplify the reach and sustainability of U.S. influence. These are arenas for improvement that apply to any and all uses of sanctions and financial measures.

- *Targeted, Strategic Enforcement.* To be effective, sanctions and financial measures must be enforced. Simply designating or labeling an activity of concern alone cannot ensure the effective application of sanctions or an effective campaign. This is essential as the targets of financial measures and actions grow more sophisticated and adapt around the pressure. Enforcement of sanctions evasion, anti-money laundering, and other financial criminal provisions allows authorities leeway to apply the criminal law, in addition to issuing regulations or sanctions in the wake of financial measures. This enforcement should ideally be coordinated, along with the inter-agency, while respecting the independence of relevant law enforcement and regulatory agencies. This does not preclude the use of targeting task forces and policy coordination at the federal level to ensure attention and enforcement on high-priority sanctions regimes and issues, along with consistency of approach in line with the U.S. government's strategy. There should be a tendency and default toward more enforcement task forces tied to strategic national security campaigns.
- *Focus on Ownership and Control.* The U.S. and European sanctions regimes explicitly cover ownership and control interests subject to sanctions for those designated under relevant sanctions programs. Regulated institutions are required to determine ownership and control interests for purposes of sanctions compliance based on percentages of



ownership and indicators of control or management, which are not often clear in the private sector. Though there is some attention by authorities to tracking and mapping ownership and control interests for designated parties, more needs to be done proactively and as a matter of consistent practice to investigate, analyze, and publish information about entities owned and controlled by designated parties.

This effort can take advantage of three trends in the environment: (1) greater attention to ownership/control requirements and disclosures under international standards, the Fourth EU Money Laundering Directive, and greater Office of Foreign Asset Control (OFAC) and regulatory attention in the United States; (2) the sensitivity in the private sector, beyond just the banking community, to understanding ownership interests for purposes of addressing corruption concerns and risks; and (3) the growing attention and work by commercial entities, think tanks, and advocacy groups in using open source data to compile network maps and lists of sanctioned parties' ownership interests. Groups like C4ADS, the Enough Project, and FDD have published and shared the names and identifiers of companies owned by designated parties or facilitating sanctions evasion. Treasury, through OFAC, should focus programmatically on enforcing follow-on sanctions on initial individual and network designations and explore ways of taking advantage appropriately of the open-source research and capabilities produced that could enable OFAC's research, follow-on designations, and enforcement.

- *More Aggressive Information Sharing Systems.* To understand better the risks and vulnerabilities to the financial system along with the economic infrastructure of those targeted, there needs to be a much more aggressive information sharing model that seeks to collect more targeted financial data while also allowing the private sector to share data more aggressively.

If the AML/CFT and sanctions system is to work, there needs to be a more aggressive and expansive information-sharing environment. In the first instance, this entails using regulatory authorities, like Geographic Targeting Orders, OFAC subpoenas, and Section 311 actions targeting "classes of transaction" to gather more financial and commercial data tied to sanctioned parties, jurisdictions, and their ownership and control interests. This idea allows for the use of financial regulation and legitimate and lawful information gathering tools to understand historical and shifting financial patterns and relationships, while helping the private sector focus on areas of prioritized concern and risk identified by U.S. authorities.

This also 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, and instead entails more targeted collaboration between regulated financial institutions, regulations, and law enforcement to target vulnerabilities and networks of concern. This happens episodically, is being piloted in specific projects, and in general is taking shape faster abroad. 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 in certain countries impede an institution's ability to share data within its own network or enterprise. Without this data, a financial institution may not see the risks and vulnerabilities in its own system without costly or time-consuming workarounds. 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 analytics, 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. My partner, Chip Poncy, and I have written about moving toward a utility model for compliance risk management, which will save costs and manifest in different models as technology enables more effective data sharing, protection, and analysis.

- *Commitment to Reinforcing International Norms with Sanctions Campaigns.* 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 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 that are 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 illicit financing in their countries and globally.

In this regard, the United States has borne much of the burden (and often the blame) of enforcing sanctions intended to protect the financial system and the international community. It is Treasury's OFAC that produces the universal list of designated parties checked and screened against by all legitimate financial institutions in the world. There are no other jurisdictions that have a dedicated entity charged with enforcing sanctions, working with the private sector to provide guidance, or even defining how such authorities should be used on a consistent basis. This then lends itself to these tools being used internationally to settle political or diplomatic scores, instead of being technically



focused on isolating underlying illicit financial activity. There should be an international goal of professionalizing and institutionalizing the work of sanctions within the authorities of key banking and commercial centers around the world, which will aid in raising the level of effectiveness globally.

This is more important than ever as other countries begin to use sanctions and financial pressure campaigns outside the bounds of UN, U.S., or EU leadership for their own purposes – and with the norms, expectations, and boundaries of how aggressively these authorities can be used continuing to be shaped. This is especially the case with respect to the use of anti-corruption laws and sanctions, which are strategically critical and essential to deploy but can be misused by regime leadership to consolidate power and marginalize or bankrupt political adversaries.

This is also important as the United States and its allies find new partners, including non-state actors, who are aligned in their interest for financial integrity and the protection of the financial system. There are new partners in the international system who need to be enlisted as we combat new forms of illicit finance, and they can be enlisted more easily if the campaigns are attached to defending legitimate international norms.

For example, a new coalition could 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. Treasury recently designated financial facilitators working with the Lord's Resistance Army to profit from this trade. The United States could help galvanize and energize additional international efforts to prevent these environmental 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.

- *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 Treasury and international community consider unwinding certain sanctions programs and delisting 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 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 alternate 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 and Cuba, and there are even lingering concerns with Burma. These are not just risky countries because they have fallen under sanctions. 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 a network 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 – and aid the local population. 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 in furtherance of its continued strategic goals.

- *Deploy Positive Economic Power.* With every financial exclusion strategy or campaign targeted at rogue actors, the U.S. government should devise a complementary strategy to leverage positive economic tools and greater financial inclusion to reward appropriate behavior and to support U.S. allies trying to do the right thing by complying with sanctions programs and financial measures. If human rights abusers are targeted with financial isolation, measures to support the cause and communications of human rights activists in that country or region should be supported. If corruption and kleptocratic regimes fall under the weight of a financial campaign, there should be financial benefits, regulatory relief, or investment incentives provided to market players willing to subscribe to the highest standards of anti-corruption practices and measures.

In addition, there is an argument for financial inclusion to serve as a national security imperative unto itself, to allow for greater transparency, improve economic development and prospects, and raise the level of compliance in developing and corrupt economies around the world. Governments have demanded that regulated financial communities serve as gatekeepers of the financial system, so as to ensure systems and institutions are not misused by criminal, sanctioned, 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.

Challenges Ahead

There are enormous challenges to the ability of the United States to use the tools of economic coercion to drive its national security goals, starting with the nature and complexity of the targets themselves to direct challenges to the American economic order.

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 al Qaida in the Islamic Maghreb (AQIM) have profited from the drug trade from South America through West Africa and the Sahel into Europe. In the past, al Qaida 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.

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 Drug Enforcement Administration (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 Federal Bureau of Investigation, 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 Makhlouf (the cousin of Bashar al Assad), and the former Qaddafi regime, to evade sanctions and move and hide millions of dollars in wealth. The 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 – revealed intricate schemes run by third-party money launderers to move money for clients in Venezuela, Russia, and China. And FinCEN's 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 report 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 Department of Justice and FinCEN's actions against BTC-e, a foreign digital currency exchange for money laundering, is an other example of growing scrutiny from U.S. authorities on the flows of illicit funds through cryptocurrencies and exchanges.

Authorities must continue to worry about the crypto-economy facilitating access to illicit capital. But digital currencies and underlying technologies and applications have emerged as efficient ways to store value, reduce payment friction, lower costs of transactions, and enable more people to interact directly and securely. Major global banks are now investing in new FinTech ventures and experimenting with the use of blockchain technologies for classic banking functions like cross-border payments. Central Banks are now considering whether and how to develop and deploy national digital currencies. All the while, new currencies, apps, and financial functionality are emerging on the digital scene, competing to create an ecosystem of digital commerce.

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.

In this context, regulators, policymakers, and enforcement agencies will need to understand better how these new technologies work and are evolving, how they may be helpful in uncovering illicit behavior, and how to distinguish between legitimate actors seeking to comply with the law and those trying to evade all scrutiny and facilitate illicit activity. They must do this in a rapidly changing environment where innovation should not be squelched and where illicit activity cannot be ignored. With the rapid increase in value and attention to bitcoin, the growing interest in "Initial Coin Offerings," and deeper investments and interest in blockchain



technologies and platforms, authorities will need to devise strategies to apply the principles of financial integrity and security in this environment.

The technology sector will need to work more closely with government agencies around the world to help inform regulators, standard setters, and investigators about how new technologies and innovations work. The private sector will need to design new models for the use of technologies like blockchain and digital currencies that enable financial inclusion, traceability, lower payment friction and costs, and enable accountability for transactions. Some of this is already happening in the marketplace. The private sector – technology companies, investors, and companies leveraging these new capabilities -- should take ownership together of designing technologies, platforms, and protocols that help solve the conundrum of needing to ensure security, transparency, and accountability with technologies created to deepen anonymity.

Systemic Weaknesses

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 and Paradise 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 Customer Due Diligence (CDD) 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.

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. 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.

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 a 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 have exited or stayed away 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 an 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 seen as complementary to the need to expand the



reach and capabilities of the legitimate financial system to manage and address illicit financing risks.

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.

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.



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. President Obama'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.

A Comprehensive U.S. National Economic Strategy

Ultimately, sanctions and financial measures cannot be viewed in isolation and cannot be assumed to be the province of the United States alone. As noted above, the tools 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. The President's new National Security Strategy begins to address this new landscape and the need to focus on national economic security.

For many years, countries such as China and Russia had been playing a new geo-economic game, where all forms of economic power are leveraged aggressively for national advantage. In this vein, the United States should concentrate on sharpening its tools and reinforcing 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 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.

Congress and the Administration 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, 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.

The power to affect the budgets of America's enemies is an enormous power that needs to be tended carefully and wielded wisely. America's enemies – especially nimble and sophisticated actors enabled by nation states -- will continue to find ways to work around the international pressure and strictures put on them. These are delicate but essential tools that if tended properly will continue to form a key part of American power projection and part of the international architecture to protect both the international financial system and security.

Thank you again for the privilege of testifying.

