Juan C. Zarate

Harnessing the Financial Furies: Smart Financial Power and National Security

Economic sanctions have long been the national security tool of choice when neither diplomacy nor military force proves effective or possible. This tool of statecraft has become even more important to coerce and constrain the behavior of non-state networks and recalcitrant, rogue regimes which often appear beyond the reach of classic U.S. power or influence. The challenge is often how to use power to affect the interests of regimes that are likely immune to broad effects of sanctions on their populations.

Over the past eight years, a new paradigm of smart financial power has emerged which has made a particular brand of financial suasion more targeted, effective, and central to critical issues of national security import. At the heart of this paradigm has been the integration of complementary financial and national security objectives to protect the integrity of the international financial system and isolate rogue financial activity. This evolution from classic, state-based sanctions has depended on a deeper involvement of the private sector in arenas previously confined to the halls of governments, with a commensurate and widening appreciation within governments of the power of markets and the private sector to influence international security.

What makes this approach so powerful is that it relies more on the risk-based compliance calculus of global financial institutions than the policy decisions

Juan C. Zarate is a senior adviser at CSIS. Before joining CSIS, he served as the deputy assistant to the president and deputy national security advisor for combating terrorism from 2005–2009. He also served at the U.S. Department of Treasury from 2001–2005, and was the first assistant secretary for terrorist financing and financial crimes. He can be reached at JZarate@csis.org.

The Washington Quarterly • 32:4 pp. 43–59
DOI: 10.1080/01636600903235890

> **This approach is powerful because it relies more on the calculus of financial institutions than the decisions of governments.**

of governments. For legitimate financial institutions, there are no benefits to the risk of facilitating illicit transactions that could bring high regulatory and reputational costs if uncovered. This means that rogue actors who try to use the financial system to launder money, finance terrorism, underwrite proliferation networks, and evade sanctions can be exposed and denied access by the financial community itself. It also means that the sanctions are based on the conduct of the rogues themselves, relying on the illicit or suspicious behavior of the actors trying to access the international financial system to trigger their isolation, and not on the political decisions of governments.

This new paradigm has done away with the old orthodoxy that defined sanctions as being either unilateral or multilateral. In essence, this new brand of financial power is multilateral by nature, given that the international financial community is the key protagonist in isolating rogue actors from the financial system. The United Nations and government actions are important and make financial pressure more effective, but those are not essential components of this power. If financial entities act according to their own commercial interests, targeted actors and their fronts will be denied access to the facilities of the international financial system such as bank accounts, cross-border money transfers, and letters of credit. If some banks decide to provide these services, they themselves run the risk of becoming financial pariahs, even before they become objects of sanctions themselves. In a system such as this, financial institutions act as the guardians at the gates of the financial system.

This new use of financial power was spawned by design and necessity, harnessed from the dramatic steps taken by governments around the world to build and adapt legislative, regulatory, and financial enforcement tools to prevent terrorist financing since the September 11, 2001 attacks. The international community has begun to expand these tools to address other transnational security threats that rely on, or touch, the international financial system, from narco-trafficking to kleptocracy and state-sponsored illicit financial activity. Yet, how has this system evolved and what factors make it effective? How will smart financial power most likely be applied in the coming months in Iran and North Korea? Most importantly, will this tool remain effective, and what are the challenges facing the application of this smart power in the years to come?

Developing Smart Financial Power

The emergence of this new brand of financial power can be explained by understanding three primary developments since September 11: the expansion of the international anti-money laundering regime; the development of financial tools geared specifically to affect issues of broad national security; and the centrality of the international financial system as well as the private sector to transnational threats and issues of primary national security concern.

Expanding the International Anti-Money Laundering Regime

In the wake of September 11, governments, in concert with the private sector, sought to leverage the existing global anti-money laundering system to prevent the financial system from being abused by al Qaeda and other terrorist organizations to perpetrate another attack or sustain their organizations. In this context, global anti-money laundering regulations and practices based on principles of financial transparency, information sharing, and due diligence were expanded and aggressively implemented. Regulations and obligations were applied to new sectors of the domestic and international financial community, such as insurance companies, brokers and dealers in precious metals and stones, and to methods of moving money such as *hawala* (a trust-based money transfer mechanism) and money service businesses.

In the United States, Title III of the USA PATRIOT Act ushered in this expansion, representing the most wide-sweeping expansion of the U.S. anti-money laundering regime since the inception of the 1970 Bank Secrecy Act. The PATRIOT Act provided the legislative mandate to extend anti-money laundering requirements to a range of commercial and financial actors, to expand financial information sharing between the government and the private sector, as well as between financial institutions, and to develop more powerful tools to enforce the expanded policies and regulations.[1]

Internationally, relevant multilateral fora became venues to address the issue of terrorist financing and to reiterate or define international obligations. In October 2001, the Financial Action Task Force (FATF), the world's anti-money laundering and counterterrorist financing standard setting body established in 1989, developed the Eight Special Recommendations (a ninth was added in 2005) for countering terrorist financing, and amplified and updated the FATF "40 Recommendations on Money Laundering" (originally adopted in 1990, revised in 1996 and 2003), all with the effect of creating the expectation of greater financial transparency, accounting, and regulatory oversight around the world.[2] These standards were later adopted by the World Bank, the International Monetary Fund, and the UN.

At the same time, international associations such as the Egmont Group of Financial Intelligence Units (FIUs)—an international network of units in countries around the world devoted to collecting, analyzing, and sharing financial information to prevent financial crimes such as money laundering and terrorist financing—committed to develop counterterrorist financing tools and to expand its membership to ensure broader access to suspicious financial information, required to be submitted by most banks around the world. Nongovernmental organizations, such as the Better Business Bureau's Wise Giving Alliance, also engaged with regulators and governments as concern over terrorists' abuse of charities became central to the international community's campaign against terrorist financing.

There was also a newfound focus on these issues in corners of the world that had been relatively detached from the global anti-money laundering system, with China and Russia eventually joining the FATF and new FATF-style regional style bodies created in Eurasia (e.g., the Eurasia Group on Combating Money Laundering and the Financing of Terrorism [EAG] founded in 2004), as well as in the Middle East and North Africa (e.g., Middle East and North Africa Financial Action Task Force [MENAFATF] founded in 2004). Countries around the world followed suit, passing new anti-money laundering laws, creating new units to apply sanctions and develop and share financial information, and committing politically to protecting their financial systems from illicit financial activity.

> Three primary developments since September 11 help explain this new brand of financial power.

The expansion of the international regulatory regime has been enforced by increasingly vigilant regulatory bodies and prosecutors around the world. As a result, multinational banks and local institutions were hit with significant investigations and penalties for anti-money laundering and sanctions violations. In the United States, investigations and multimillion dollar fines against well-established institutions such as Riggs Bank, UBS, and ABN Amro, among others, served to further sensitize the private sector to the reputational and financial risks of failing to observe the letter and spirit of these expanding anti-money laundering obligations. In the post-September 11 environment, financial institutions did not want to find themselves caught in the headlines of counterterrorist financing or anti-money laundering investigations.

This expansion was not without controversy, cost, or difficulty. Applying anti-money laundering tools built largely to address classic drug-based and bulk money laundering to the problem of terrorist financing (whose sourcing may not be criminal in nature) and to more informal sectors dealing with smaller and more opaque transactions frustrated both the private sector and government authorities. Questions about the relevant costs and usefulness of enhanced enforcement continue to top the list of private sector concerns. These concerns have been exacerbated by an increased reliance on the private sector to serve as "gatekeepers" for the financial system and the need for greater communication between governments and regulated entities.

Despite these concerns, the expanded global anti-money laundering regime stands as an embedded and lasting framework for the protection of the international financial system and is now understood as an essential part of a "safe and sound" financial system. Indeed, this framework has been the baseline from which the international community has expanded its focus and concern from money laundering and terrorist financing to proliferation finance, illicit use of front companies, sanctions evasion, and kleptocracy.

Applying Financial Tools to National Security Issues of Concern

After September 11, the United States and the international community also developed new and amplified tools to isolate rogue actors from the financial system. The campaign against terrorist financing was defined early through the use of targeted financial sanctions against terrorist-supporting individuals and entities. The "smart" sanctions of the late 1990s that targeted rogue leaders and entities they controlled were put on steroids.

In the United States, then-President George W. Bush signed executive order 13224 on September 22, 2001, allowing for the broader use of U.S. authorities to freeze assets and transactions of designated terrorist supporters and facilitators, including financial institutions, and restricting commercial interactions between such designated parties and U.S. persons.[3] This order launched U.S. efforts to identify and sanction more than four hundred individuals and entities, with the express purpose of corralling assets and transactions to prevent terrorist financing. At the UN, the pre-September 11 al Qaeda and Taliban sanctions regime (as reflected in UN Security Council resolution 1267) was ramped up and served as the international community's primary method of identifying those al Qaeda and Taliban-supporting entities subject to global financial sanctions and travel and arms bans.[4] The European Union has applied targeted sanctions in a similar manner through what is known as the EU Clearinghouse process.

The use of such administrative, preventative sanctions since September 11 has served to stop suspicious money flows and isolate those identified with such activities from the legitimate financial system. Unlike criminal arrests and procedures, these asset freezes are often administrative actions designed to disable entire networks of businesses or related entities when tied to the funding of terrorism. Unlike civil or criminal forfeiture proceedings, this means that there are no trials, hearings, or notices before orders are issued to financial institutions to freeze bank accounts and transactions owned or controlled by the designated parties. These sanctions have also served as diplomatic tools to raise the consciousness of the international community to issues of immediate concern such as al Qaeda's abuse of charities and its presence in Iran. The use of such aggressive sanctions, however, has come under direct attack by those arguing for *ex ante* due process (e.g., advanced notice of designation or a judicial hearing to allow for rebuttal of evidence presented) for those individuals and entities, especially in Europe.

The United States supplemented these tools by implementing Section 311 of the PATRIOT Act, which allowed the secretary of treasury to apply regulatory measures to financial entities, jurisdictions, and classes of transactions identified as "primary money laundering concerns." The U.S. Department of Treasury used this authority aggressively between 2003 and 2005 as part of a "bad bank initiative" to isolate those financial institutions around the world facilitating an assortment of illicit financial activity. The use of this regulatory tool in 2005 against Banco Delta Asia—a private bank in Macau that was facilitating money laundering, proliferation, and counterfeiting on behalf of the North Korean regime—served as a way to notify the international financial community of the ongoing practices of concern by this financial entity and Pyongyang.

The power of this market-based financial isolation was made evident in 2005 against North Korea.

The use of targeted financial sanctions and related international focus has also expanded to issues such as proliferation finance and high-level or regime corruption, often referred to as "kleptocracy." In the United States, the president's signing of executive order 13382 on June 29, 2005, provided the domestic legal and regulatory framework to expand this paradigm to proliferation financing, which has been used to identify front companies from China, North Korea, and Russia engaged in suspect proliferation activities.[5] As seen in the Iran-related sanctions at the UN and by Europe and the United States, there is a growing reliance on targeted sanctions and broader financial warnings to help pressure the Iranian regime by isolating those entities and activities possibly engaged in the development of a nuclear weapons program. The use of such tools against autocratic regimes and leadership in countries such as Burma, Belarus, Liberia, Sudan, Syria, and Zimbabwe has also served to expand ongoing efforts in the EU and the United States to deter and prevent large-scale corruption.

The increasing use of these tools has spawned a new line of business within governments and the private sector focused on developing, analyzing, and using financial data and information to understand vulnerabilities and to prevent their exploitation by illicit networks of concern. In the United States, the Office of Terrorism and Financial Intelligence was established within the Department of Treasury in 2004, with a dedicated intelligence office charged with developing financial information and analysis within the intelligence community for potential use by policymakers and the private sector.

The effects of these sanctions were amplified by private lawsuits from victims of terrorism, which served as de facto sanctions on those individuals, companies, and financial institutions implicated in the lawsuits. The deterrent power of such lawsuits was seen most vividly in the case of victims of Hamas terror, whose threats of suits against institutions willing to provide financial services to Hamas entities effectively shut down Hamas' access to banks such as Arab Bank PLC and Cairo Amman Bank, especially after Hamas took over the Gaza strip.

The reliance on financial information and targeted financial sanctions to identify and isolate rogue actors from the financial system is a hallmark of the last eight years, with a broadening expansion of these powers. Though there are limitations and challenges to the use of such power and the information that can be used or shared, there is no question that such sanctions and related regulatory and prosecutorial actions remain a cornerstone of the international community's approach to using financial power and influence to affect a wide range of national security concerns.

Integrating the International Financial Community and Private Sector

A key dimension of this new paradigm is the central role and influence of the private sector for issues of international security import. There has been an enormous anti-money laundering/counterterrorist financing regulatory burden placed on financial and commercial actors since September 11. Governments have relied more and more on the ability of financial institutions to act as protective gatekeepers to the financial system by identifying, reporting, and preventing the use of financial facilities by transnational actors and criminals of concern.

The international banking community has grown acutely sensitive to the business risks attached to illicit financial activity and has taken steps to avoid the taint of such activities being facilitated through their institutions. Sensitivity by this community—the primary gatekeepers to international commerce and capital—has been the amplifying element that has motivated private sector actors to cease problematic or suspect business relationships, even absent government mandate or requirements. The legitimate international financial community will ultimately act based on its own business interests, which is aligned with the interests of governments desiring to isolate rogue financial actors. In this post-September 11 environment, there is a natural convergence between the interests of responsible governments and the financial community to protect the integrity of the international financial system.

This sensitivity to both commercial and reputational risks has been shaped in large part by increased anti-money laundering regulatory scrutiny at a global level, well-publicized enforcement actions by national governments, lawsuits brought on by victims of terror, and the explosion of available information sources on terrorist financing and transnational threats of concern (credible or otherwise) that form part of the required review and due diligence by compliance officers around the world. These factors have amplified the perceived risks of illicit financial activity assessed by financial institutions as worth avoiding at all costs. This has led to some distortions and unintended consequences such as diminishing access to the international financial system by smaller, yet legitimate, entities unable to prove their *bona fides* or ability to vet customers to larger financial institutions.

There is no better example of this dynamic than the efforts by the United States and other governments over the past four years to identify and isolate the illicit and dangerous financial activity of the regimes in North Korea and Iran. Government actions have spurred banks to make independent cost-benefit determinations leading to closing accounts and ending banking relationships with North Korean as well as Iranian organizations and front companies, shipping lines, and pass-through and shell account holders. In this field and in others related to issues of international security import, the financial community, for better or for worse, has become the frontline actor in the quest to protect the integrity of the financial system and to isolate rogue and illicit financial activity.

Unleashing the Financial Furies . . .

With few concrete levers to influence rogue regimes in Pyongyang, Tehran, and elsewhere, the United States will continue to rely heavily on this new brand of financial suasion to isolate those engaged in activities that threaten both national security and the integrity of the financial system. In this new paradigm, actors bring this financial isolation on themselves given the nature of their illicit or suspect activities and the manner by which they try to hide or mask the ultimate purposes of their financial dealings.

. . . Against North Korea

The power of this market-based financial isolation was made evident in 2005 against North Korea. As part of a strategic pressure campaign, the U.S. Department of Treasury issued a domestic regulation in September 2005, under Section 311 of the PATRIOT Act, ordering U.S. financial institutions to close any correspondent accounts for Banco Delta Asia, a small private bank in Macau. This bank was facilitating money laundering, proliferation, and counterfeiting on behalf of the North Korean regime. The regulation cut the bank off from the U.S. financial system.

> The implements to squeeze further the Iranian regime's abilty to do business internationally are in place

More importantly, what appeared to be a simple unilateral regulation against a private bank unleashed the market-based financial furies against North Korea. Banks in Asia and Europe stopped doing business with Pyongyang, ultimately denying North Korea access to the international financial system. North Korean bank accounts were closed, their transnational commercial transactions were cancelled, and their officials' financial activities were carefully scrutinized. Without further prompting from governments or the UN, the private sector reacted in this manner based on their own commercial interests. No bank wanted to be seen as the North Korean regime's bank of choice when the regime was engaged in both illicit and dangerous commercial activity, which would then put the financial institution's own access to the U.S. and international financial systems in jeopardy.

The pressure hurt the North Korean regime. Pyongyang scrambled to regain access to their money and accounts around the world while trying to undo the official damage done to its reputation in the international financial community. The key state actors, including China, had no incentive to block the full effect of the market reaction. On the contrary, they did not want their banks or financial reputation caught up in the taint of North Korean illicit financial activity. This pressure became the primary leverage for the United States to press North Korea's return to the Six-Party negotiating table, which it eventually did in late 2006. With the Six-Party Talks reassembled, the international financial squeeze was gently loosened, though a direct link was never officially acknowledged.

In the face of North Korean recalcitrance and belligerence, this type of financial smart power is being leveraged again, with the elements of a financial pressure campaign emerging. The UN adopted Security Council resolution 1874 on June 12, 2009, serving as a rejuvenated international baseline to ramp up financial pressure, along with an amplified arms ban and a new system for inspection of North Korean cargo.[6] This was quickly followed on June 18, 2009, by the U.S. Department of Treasury advising the financial community of the dangers of doing business with North Korea and the threat to the integrity of the financial system, given the likelihood of continued deceptive and criminal activities. That advisory also listed 17 North Korean banks whose commercial connections and financial activity should be viewed with great suspicion, given the use of such institutions by the regime to evade sanctions, engage in proliferation activities, and in broader illicit activity. Late in June and July 2009, the Departments of State and Treasury designated three North Korean commercial entities tied to the regime's missile proliferation and nuclear weapons programs.

North Korea's suspect activities—proliferation, sanctions evasion, counterfeiting, drug trafficking, and smuggling—provide the continued seeds of their own isolation. These revelations and sanctions will be the heart of this new pressure campaign against Pyongyang. Along with Japan and South Korea, the United States will use North Korea's recalcitrance and illicit behavior to drive public and private sector efforts to stop North Korea's international commercial activity critical to the development of their weapons program, financing, and potential proliferation.

Over time, this will include public and private threats of sanctions, regulatory actions, or public revelations against those financial institutions that continue to do business with suspect North Korean entities and officials. If fully realized, it will also include a more aggressive use of targeted financial sanctions and regulatory actions, including an aggressive campaign to uncover and freeze leadership assets. As leadership assets are critical to regime loyalty, an international campaign to freeze those assets would build tension and suspicion within the leadership's ranks.

. . . and Iran

The financial pressure campaign against Iran using this same paradigm and playbook has been a slower, yet more consistent effort, relying on sanctioning Iranian banks and companies at the UN and by the United States for proliferation violations and support for terrorism. The private sector has reacted to Iran's activities by reducing, and in some cases ceasing, business with Iranian banks and companies. The decisions by Swiss banking giants UBS and Credit Suisse Group along with energy companies, such as BP PLC of London and Conoco Phillips, to curtail if not cease business ties and relations in Iran and with Iranian entities were emblematic of this trend. Meanwhile, governments, led by the U.S. Department of Treasury, have been reaching out more frequently to the private sector to provide them with briefings and information about the nature of Iran's illicit activity and use of the international financial system.

Critical to the effectiveness of these measures has been the public and private revelations of the growing reach of the Iranian Revolutionary Guard Corps (IRGC) in the Iranian economy and its control of major overseas companies and operations including in the oil, defense production, and construction industries.

The IRGC serves as the parallel military and intelligence arm of the Iranian clerical regime committed to defending the regime. This includes supplying organizations like Hezbollah, Hamas, and Iraqi militants with weapons, training, and funding, and in developing the Iranian ballistic missile system. The IRGC's deep involvement in commercial ventures proves problematic for the international financial community because financial institutions are not able to discern legitimate activity from what may be illegal or suspect transactions furthering the IRGC's mission. Thus, no bank or company wants to find itself in the position of unwittingly assisting or facilitating activities that are viewed as dangerous, if not illegal, by the international community. The risks of doing business with Iranian entities that may be acting as direct agents of the regime to assist in proliferation, terrorist financing, or sanctions evasion represent major international and financial security concerns for both governments and banks.

On October 25, 2007, the U.S. Departments of State and Treasury took a series of important steps to drive this narrative and the related international pressure campaign by designating the IRGC, nine IRGC front companies, five of its leaders, the Ministry of Defense and Armed Forces Logistics (MODAFL), and Bank Melli and Bank Mellat of Iran as proliferators of weapons of mass destruction. At the same time, the United States also designated the IRGC-Qods Force (the external arm of the IRGC) and Bank Saderat of Iran as supporters of terrorism. These actions were intended to encapsulate the dangers of doing business with Iran and solidify the financial isolation that had already begun to take hold in the international financial system.

To maintain the sharp edge of this smart power, it is important to understand the challenges that lie ahead

These actions have been buttressed by multilateral measures, including UN sanctions against the IRGC, Iranian officials, Iranian banks and companies, and multiple calls by the world's anti-money laundering body, the FATF, for members to take necessary actions to protect their respective financial systems against the inherent dangers of the Iranian financial system. All of these measures create a deepening sense for the private sector of an inhospitable, if not dangerous, business environment in which legitimate financial and commercial ventures cannot ensure that they are doing business with credible business entities. As a result of almost three years of these efforts, most major financial institutions and numerous commercial entities, including energy companies, have stopped doing business with Iranian banks and entities. All of this makes it costlier and more complicated for Iran to conduct business internationally.

Unlike North Korea, Iran has the advantage of being a major oil producer and having deeper financial and trading ties with countries in Europe and Asia. To a certain extent, this tempers and complicates the willingness of commercial entities and banks to cleave all business relations with Iran. Yet, it has been the Iranian regime's continuous involvement with illicit activities and unwillingness to adhere to international law that has proven to be the driver of their own isolation. In addition, statements by President Mahmoud Ahmadinejad denying the Holocaust and threatening Israel have added to the sense of political tension and turmoil in Iran. All of this weighs in the minds of chief executive officers and boards of directors calculating whether to drop investments or opportunities in and with Iran. Decisions by some of the major non-U.S. financial institutions in the world and European companies to withdraw their presence and exposure in Iran, when there are clear economic benefits to be had from such engagement, demonstrate the importance of these risks and factors to the legitimate financial and commercial world.

Iran remains susceptible to additional pressure in other segments of their economy reliant on external financing and suppliers, such as shipping, insurance, and refined oil imports, at a time of diminishing revenues due to relatively low oil prices. If European, Gulf, and Asian allies order even greater restrictions on dealings with certain Iranian entities, the financial squeeze could continue to prove quite painful to Iran. Pending legislation in Congress, such as the Iran Refined Petroleum Sanctions Act and the Iran Sanctions Enabling Act, has in mind an even broader expansion and hardened sanctions against Iran including mandatory divestment from those companies continuing to do business with Iran. This approach would begin to convert the financial suasion approach into a mandatory, secondary boycott approach against non-Iranian entities.

To date, the Obama administration has not refreshed a financial campaign against Iranian banks and companies, but the ability to further squeeze the Iranian regime's ability to do business internationally is in place. With President Barack Obama putting a September deadline on the proposed outreach to Tehran, there will be opportunities in the fall, with the UN General Assembly and through the Group of 7 (G-7) and Group of 20 (G-20), to set a course for additional sanctions against Iran's various business sectors. This would include an expansion of targeted financial sanctions, restrictions on refined oil imports and insurance, and possible action against Iran's central bank for facilitating illicit financial activity and sanctions evasion.

The perceived threat to both international security and the integrity of the financial system is the leverage that will allow this new type of financial pressure to work. The Obama administration has been reluctant to unleash the financial furies again against Tehran, with both the prospects of dialogue still alive and a concern that any U.S. action will only serve to complicate matters in the wake of the regime's controversial electoral fraud and crackdown on demonstrators following the June 12, 2009 elections. The Obama team has wanted to deny the regime the "American bogeyman" argument and avoid the perception of provocation. With the administration's own September deadline for dialogue looming with little prospect that a weakened Iranian regime can deliver meaningful results from such dialogue, it is likely that the administration is already preparing the financial battle plan for the fall.

There is a risk of overusing these financial tools for all national security issues.

The effects of this smart financial power against Iran, North Korea, or other rogue actors are important. In the first instance, this market-based financial isolation has the ability to complicate, make more costly, and even impede the international commercial activity that facilitates and finances the activities of greatest concern such as ballistic missile system development, nuclear arms programs, support to terrorist and non-state networks of concern, and proliferation of knowledge and materiel. Just as important, this tool may provide the United States and its allies the best source of diplomatic leverage to affect regimes' behavior and calculus.

Challenges to the New Paradigm

Though effective, this approach is vulnerable to direct attempts to blunt its reach, overuse, complications in implementation, and changes in the balance of global economic power. The new administration will certainly rely on this new brand of financial power to give teeth to its diplomacy and to pressure regimes around the world when the reach of the United States is otherwise limited. To maintain the sharp edge of this smart power, it is important to understand the challenges that lie ahead.

Unholy Alliances of Financial Rogues

The initial challenge comes from rogue actors themselves. Criminal and terrorist networks and organizations, along with sanctioned states, will continue to need access to the international financial system. This need will breed innovation in circumventing sanctions ranging from recreating targeted companies to hiding the nature of suspect transactions with creative fronts or corrupted banking officials and regulators. This may create a market with incentives for organized criminal actors, such as high-end money launderers, and poorly regulated institutions to provide a full suite of banking and commercial services to the isolated actors. The key then is to continue to shine the light on those actors engaged in illicit and suspicious conduct through regulatory and enforcement actions, with the private sector and regulatory maintaining diligence of those transactions that may be subject to manipulation.

The need to counter or neuter the reach of smart financial power will also create incentives for those isolated states and entities to forge new business or banking relationships as a means of creating alternate shadow networks to fund and facilitate commercial transactions across borders. For example, Belarussian, Burmese, Iranian, North Korean, and Syrian banks or entities would have incentives to create business relationships of convenience providing access to the international financial system while also facilitating cooperation between the state actors. These unholy alliances already exist in some cases. On June 30, 2009, the U.S. Department of Treasury designated Hong Kong Electronics, a North Korean company that formed part of North Korea's nuclear weapons proliferation and ballistic missiles and weapons program. This company was based on Kish Island, Iran and had been transferring money from Iran to North Korea.[7]

Such networks would be amplified by banks or countries willing to flout, for economic or political reasons, the legitimate financial system's isolation of these actors or states. This makes alternate banking outlets in places such as China, Malaysia, Russia, Qatar, and Venezuela all the more important and potentially problematic, given the potential for lax enforcement of anti-money laundering rules and principles as well as the penchant of those countries' governments to oppose Western policies and interests, especially those that directly concern the United States. These countries could then serve as international financial outlets for rogue regimes not because they overtly approve of the activity being financed or facilitated but simply as a way of countering the influence of the Western banking system. In this regard, such countries and some financial institutions backed by governments may be willing to assume the risk of potential taint by labeling the international community's use of financial sanctions and power as being purely politically motivated. An important issue then is to create incentives, as well as potential punishment, with the international financial community that encourage such states to act in line with the legitimate financial system and to preserve the sense that the use of such measures is driven by suspect conduct and not solely by politics.

Regulatory Burden and Overuse

The regulatory burden and related costs on the private sector have increased over the last eight years. Governments need to remain acutely aware of the importance, burdens, and reliance on those private actors. As noted above, the United States needs to ensure that it maintains a focus on conduct-based sanctions that have direct relevance to the private sector and the integrity of the financial system. Renewed financial pressure campaigns against countries such as North Korea and Iran focused on their illicit conduct in the international financial system such as counterfeiting, sanctions evasion, and money laundering can help. Though such campaigns would be undertaken to address international security problems, rejuvenating such a focus on illicit financial activity would restore confidence in the U.S. Department of Treasury's tools, which should not be seen as being arbitrarily driven by political and diplomatic factors alone.

Governments should increase collaboration with financial institutions, not alienate them.

At the same time, there will be a tendency to overuse these financial tools for all national security issues for which there is not a ready solution. In some cases, as with the problem of piracy in East Africa, these tools will prove less relevant and effective because certain money flows and economies do not link as directly or neatly into the international or regional financial systems that can be affected. The attempts to overuse them, especially if unsuccessful, could dull their broader utility and strain relations with the private sector.

In addition, governments should increase collaboration and useful information sharing so as to enlist, as opposed to alienate, financial institutions. Information sharing and transparency will continue to be the engine that drives the effective protection of the financial system from illicit financial activity. Governments around the world need to find better ways of leveraging data already available, such as in the data sharing agreement of the Egmont Group of FIUs, and more frequent sharing of specific information or intelligence with the financial community. Banks and other financial institutions also need to take advantage of provisions, as found in Section 314 of the PATRIOT Act, to share information between respective institutions to build common awareness of those threatening the financial system. All of this needs to be done within the framework of consistent multinational practices that protect privacy and individual civil liberties.

This also means that governments need to check their regulatory practices and to work closely to build consistent regulatory requirements and regimes across borders to assist international financial institutions to operate effectively and efficiently. This challenge will be exacerbated as governments create new regulatory structures and requirements in the wake of the current financial crisis.

Implementation Challenges

There are also some critical challenges emerging to the tools that undergird the ability of the United States and its allies to use this financial suasion effectively, especially in Europe. The European Court of Justice has called at least part of this system into question, noting that the EU's automatic listing of individuals based on UN action and without prior notice or opportunity to challenge lacks requisite due process to protect human rights. Yet, this system is built on the chapter VII obligations of the UN charter and forms part of the broader targeted financial sanctions regime used by the international community across the board. If the system of judicious use of targeted financial sanctions used by the UN and member nations to pressure rogue international actors is dismantled in Europe, then the system of targeted financial sanctions might potentially collapse. These tools need to be preserved while governments and the UN continue to refine and adjust how they are used. These tools should include allowances to redress grievances and encourage U.S.-style delisting processes.

The financial crisis threatens the effectiveness of this new tool.

More fundamentally, the current financial crisis and attendant questions of the global capitalist system, along with the challenges to the predominance of the U.S. dollar, potentially threaten the effectiveness of this new tool. As the effects of the financial crisis continue to ripple throughout the international financial and economic systems, banks in dire need of capital and liquidity may alter their business risk calculus, making them more willing to take on suspect clients or facilitate activities with less focus on anti-money laundering compliance and reputational risk.

In addition, much of the power behind this new paradigm stems from the ability of the United States to use its sanction powers with global effect. This, in turn derives from the centrality and stability of New York as a global financial center, the importance of dollar-clearing transactions, and the demonstration effects of any regulatory or other steps taken by the United States or major U.S. financial institutions in the broader international system. Countries such as Russia will continue to challenge the predominance of the U.S.-led international system and the dollar itself. If such attacks succeed fundamentally, they could potentially weaken the ability of the United States to affect or move private sector decisionmaking in line with national security interests regardless of what other governments do.

What buttresses this tool, though, is the broad agreement in the international community, especially the private sector, about the types of activities which are threatening and bad for business such as front companies or sanctions evasion. Thus, business risk and reputational calculus, not the economic dominance of the United States, will ultimately determine how effective these measures will be. In addition, current discussions about global regulatory reform in the G-20 and elsewhere provide an opportunity to clarify and enhance the international community's responsibilities to protect the financial system against the risks attendant to illicit financial transactions, regardless of the U.S. share of global gross domestic product.

An Effective Cornerstone

As the world faces challenges from rogue states, networks, and actors, there now exists a well developed international system to use financial information, power, and suasion to isolate rogues from the legitimate financial system. Though this alone can not solve the issues of deepest national security concern, this private sector-based paradigm gives the Obama administration and its allies the tools and leverage to affect rogue actors and their interests, which historically would have been considered out of reach. If maintained properly, this new paradigm of smart financial power will remain an effective cornerstone of the international community's efforts to keep both the financial system and global citizens safe.

Notes

1. See *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001*, Public Law No: 107–56, 107th Cong., 1st sess. (October 24, 2001) http://epic.org/privacy/terrorism/hr3162.pdf.
2. Financial Action Task Force, "40 Recommendations," Web site, October 2003, http://www.fatf-gafi.org/document/28/0,3343,en_32250379_32236930_33658140_1_1_1_1,00.html.
3. Executive Order 13224, Office of Foreign Assets Control, U.S. Department of Treasury, September 23, 2001, http://www.treasury.gov/offices/enforcement/ofac/programs/terror/terror.pdf.
4. See UN Security Council Resolution 1267, S/RES/1267 (1999), October 15, 1999, http://www.treas.gov/offices/enforcement/pdf/unscr1267.pdf.
5. Executive Order 13382, Office of Foreign Assets Control, U.S. Department of Treasury, June 29, 2005, http://www.treas.gov/offices/enforcement/ofac/programs/wmd/wmd.pdf.
6. UN Security Council Resolution 1874, S/RES/1874 (2009), June 12, 2009, http://daccessdds.un.org/doc/UNDOC/GEN/N09/368/49/PDF/N0936849.pdf?OpenElement.
7. "Since 2007, Hong Kong Electronics has transferred millions of dollars of proliferation-related funds on behalf of Tanchon and KOMID. Hong Kong Electronics has also facilitated the movement of money from Iran to North Korea on behalf of KOMID. Tanchon, a commercial bank based in Pyongyang, North Korea, is the financial arm for KOMID - North Korea's premier arms dealer and main exporter of goods and equipment related to ballistic missiles and conventional weapons." See U.S. Department of Treasury, "Treasury Targets North Korea's Missile Proliferation Network," June 30, 2009, http://www.ustreas.gov/press/releases/tg191.htm (press release).