CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

COMMENTARY

Smart Financial Power and International Security: Reflections on the Evolution of the Global Anti-Money-Laundering and Counterterrorist Financing Regime since 9/11

Juan C. Zarate

April 21, 2009

As the Obama administration determines how to address multiple foreign policy challenges, it is an important moment to reflect on the evolution and use of financial information and power to affect critical international security issues over the last eight years.

The historic steps taken by governments around the world to build and adapt legislative, regulatory, and enforcement tools to prevent terrorist financing since 9/11 has created—by design and necessity—a new paradigm for the use of financial power to affect issues of national security import—from terrorist financing and narcotrafficking to kleptocracy and state-sponsored illicit financial activity. This evolution has involved a deeper involvement by 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. There is no question that the international community—to include the private sector—has made the dual and complementary objectives of protecting the integrity of the international financial system and isolating rogue financial activity central international security and financial objectives.

This new paradigm in the use of "smart" financial power since 9/11 can be explained by understanding three primary developments that have combined to make financial regulation, sanctions, and the global financial system and players integral to the international security landscape.

Expansion of the International Money-Laundering Regime

The international community has collaborated to deepen, broaden, and adapt the global anti-money-laundering system to address national security concerns that touch the international financial system directly—starting with terrorist financing. In the wake of 9/11, governments, in concert with the private sector, sought to leverage the existing systems and regulatory structures 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 then, global anti-money-laundering regulations and practices—based on principles of financial transparency, information sharing, and due diligence—were expanded and aggressively implemented. This manifested itself in regulations and obligations applied to new sectors of the domestic and international financial community and to methods of moving money—like hawala and money service businesses—previously untouched by classic regulatory controls and reporting requirements.

In the United States, Title III of the U.S. 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 Bank Secrecy Act. The Patriot Act provided the legislative mandate (1) to extend anti-money-laundering requirements to a range of commercial and financial actors; (2) to expand financial information sharing between the government and the private sector (as well as among financial institutions); and (3) to develop more powerful tools with which to enforce the expanded policies and regulations.

Internationally, relevant multilateral fora became venues to address the issue of terrorist financing and to reiterate or define international obligations. Importantly, the Financial Action Task Force (FATF/GAFI) developed nine special recommendations (originally eight) for countering terrorist financing and amplified and updated the FATF 40 recommendations on money laundering—all with the effect of creating the expectation of greater financial transparency,

---

Note: A version of this essay appeared in the Spring 2009 *UBS Money Laundering Prevention Newsletter.*

accounting, and regulatory oversight around the world. These standards were later adopted by the World Bank, the International Monetary Fund, and the United Nations. At the same time, international associations like the Egmont Group of financial intelligence units (FIUs) committed to developing counterterrorist financing tools and to expanding the membership to ensure broader access to suspicious financial information. The nongovernmental organizations (NGOs) 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 bodies created in Eurasia and in the Middle East/North Africa. 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. The expansion of the international regulatory regime was matched by increased vigilance and enforcement by regulatory bodies and prosecutors around the world—with multinational banks and local institutions hit with significant investigations and penalties for anti-money-laundering and sanctions violations.

This expansion was not without controversy, cost, or difficulty. Applying classic money-laundering tools to more informal sectors and to terrorist-financing typologies that do not involve front-end illicit activity frustrated both the private sector and government authorities, with questions about the relevant costs and the usefulness of reporting and enhanced enforcement continuing to top the list of private sector concerns. These concerns were exacerbated by an increased reliance on the private sector to serve as "gatekeepers" for the financial system and the need for greater communication between the 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 has now come to be understood as 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, international organized crime, and kleptocracy.

Development and Application of Financial Tools to National Security Issues

After 9/11, the United States and the international community also engaged in the development of 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. In the United States, President George W. Bush signed Executive Order (EO) 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. This EO launched U.S. efforts to identify and sanction more than 400 individuals and entities, with the express purpose of corralling assets and transactions to prevent terrorist financing. At the United Nations, the pre-9/11 al Qaeda and Taliban sanctions regime (UNSCR 1267) was ramped up and served as the international community's primary method of identifying those Taliban and al Qaeda–supporting entities subject to global financial sanctions and travel and arms bans. The European Union—through the EU clearinghouse process—has applied targeted sanctions in a similar manner.

The use of such administrative, preventative sanctions in the post-9/11 context has served to stop suspect money flows and isolate those identified from the legitimate financial system. These sanctions have also served as diplomatic tools to raise the consciousness of the international community to issues of immediate concern, like al Qaeda's abuse of charities and al Qaeda's presence in Iran. The use of these sanctions aggressively and widely has come under direct attack by those arguing for ex ante due process for those individuals and entities designated, with litigation and political negotiations related to these tools still at play.

The United States added to these tools by implementing Section 311 of the Patriot Act—allowing the secretary of the treasury to apply regulatory measures to financial entities, jurisdictions, and classes of transactions identified as "primary money-laundering concerns." The U.S. Treasury used this authority aggressively to isolate those facilitating an assortment of illicit financial activity between 2003 and 2005 as part of a "bad bank initiative." The use of this regulatory tool against Banco Delta Asia in 2005, which 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.

The use of the targeted financial sanctions and related international focus has also expanded to issues of international security concern, like proliferation finance and kleptocracy. As seen in the Iran-related sanctions at the United Nations and by the United States and Europe, there is a growing reliance on targeted sanctions and broader warnings to help pressure the Iranian regime by isolating those entities and activities possibly engaged in the development of a nuclear weapons program. In the United States, the president's signing of EO 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 Russia, China, and North Korea engaged in suspect proliferation activities. The use of such tools against autocratic regimes and leadership—in Zimbabwe, Burma, Sudan, Belarussia, Syria, and the former Taylor regime in Liberia—has also served to expand ongoing efforts in the European Union 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 attack points of vulnerability for illicit networks of concern. This was seen most visibly in the United States with the creation of the Office of Terrorism and Financial Intelligence in 2004, with a dedicated intelligence office within the Treasury charged with working with the intelligence community to develop financial information and analysis for potential use by policymakers and the private sector.

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.

Centrality of the International Financial Community and Private Sector

A key dimension of this new paradigm—often misunderstood and underestimated—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 9/11. Governments have relied more and more on the ability of financial institutions to act as protective gatekeepers to the financial system—identifying, reporting, and preventing the use of financial facilities by transnational actors and criminals of concern.

Importantly, 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. This sensitivity to both commercial and reputational risks has been shaped in large part by increased anti-money-laundering regulatory scrutiny globally, well-publicized enforcement actions by governments (e.g., penalties assessed against Riggs Bank), 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 vulnerabilities to the risks of illicit financial activity assessed by financial institutions as a business risk worth avoiding at all costs.

This has led to some distortions and unintended consequences—like diminishing access to the international financial system by smaller yet legitimate entities unable to prove their bona fides or vet customers. It has also led to the reality that the legitimate international financial community will ultimately act for its own benefit and interests in a manner aligned with the interests of governments desiring to isolate rogue financial actors. In this post-9/11 environment, there is a convergence of interests between responsible governments and the financial community to protect the integrity of the international financial system.

There is no better example of this 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 the closing of accounts and ending of banking relationships with North Korean and 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—like it or not—has become the frontline actor in the quest to protect the integrity of the financial system and to isolate rogue and illicit financial activity.

Challenges and Opportunities in the Coming Years

The evolution of the anti-money-laundering and counterterrorist financing regime over the last eight years has resulted in a focus on using financial power and suasion to influence international security issues of import. The original architecture and tools targeted at terrorist financing have been harnessed to address emergent as well as long-standing issues of concern like proliferation finance, kleptocracy, rogue regime behavior, and sanctions evasion. Though effective and established, this approach is not without drawbacks. The new Obama administration will no doubt rely heavily on these evolved tools of smart financial power as an alternate to the use of military force and to give teeth to its diplomacy; however, those now in power in Washington and the legitimate financial community will need to remain conscious of the challenges that lie ahead:

- Rogue actors—individuals, organizations, and states—that need access to the international financial system will attempt to circumvent financial restrictions. As has been seen already, they will do this by creating better front and cover operations; developing unholy financial alliances and partnerships with other rogue financial actors; and corrupting officials and private actors to look the other way to evade domestic laws and international sanctions.
- The regulatory burden and related costs on the private sector have increased over the last eight years, and governments need to remain acutely aware of the importance, burdens, and reliance on private sector actors. This means that governments need to check their regulatory practices and increase collaboration and useful information sharing so as to enlist as opposed to alienate financial institutions. This also means that governments need to work closely to build consistent regulatory requirements and regimes across borders to assist international financial institutions to operate effectively and efficiently. This need will be exacerbated as governments create new regulatory structures and requirements in the wake of the current financial crisis.
- The reliance on targeted financial sanctions has been critical, but those international tools are being challenged. The collapse of the system used by the international community to isolate suspected supporters of terrorism—being played out most vividly in Europe—could jeopardize all uses of targeted financial sanctions used by the United Nations and member nations to pressure rogue international actors. These tools need to be preserved while governments and the United Nations continue to refine and adjustment how these tools are used—to include allowances for redress of grievances and encourage U.S.-style delisting.
- 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 (e.g., 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 among 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.

Conclusion

As the Obama administration faces the challenges of North Korea, Iran, and Burma, it inherits a well-developed international system for the use of financial information, power, and suasion to isolate rogue actors from the legitimate financial system and to affect a range of issues of national security import. For governments around the world, this is a time to recommit to the effective and judicious use of these smart powers to deal with pressing international security issues. For the private sector, this is a time to recognize the enormous contributions it has made and the centrality of its role in security issues that were previously only the concern of government leaders and regulators.

This new paradigm will remain a cornerstone of the international community's efforts to keep the financial system and our citizens safe. This is something for which we can all be proud. This is also a smart power on which the new administration will need to rely heavily.

Juan C. Zarate is a senior adviser with the Transnational Threats Project at the Center for Strategic and International Studies in Washington, D.C. He was deputy assistant to the president and deputy national security adviser for combating terrorism from 2005 to 2009. Mr. Zarate served at the Department of the Treasury, from 2001 to 2005. He was the first assistant secretary for terrorist financing and financial crimes.