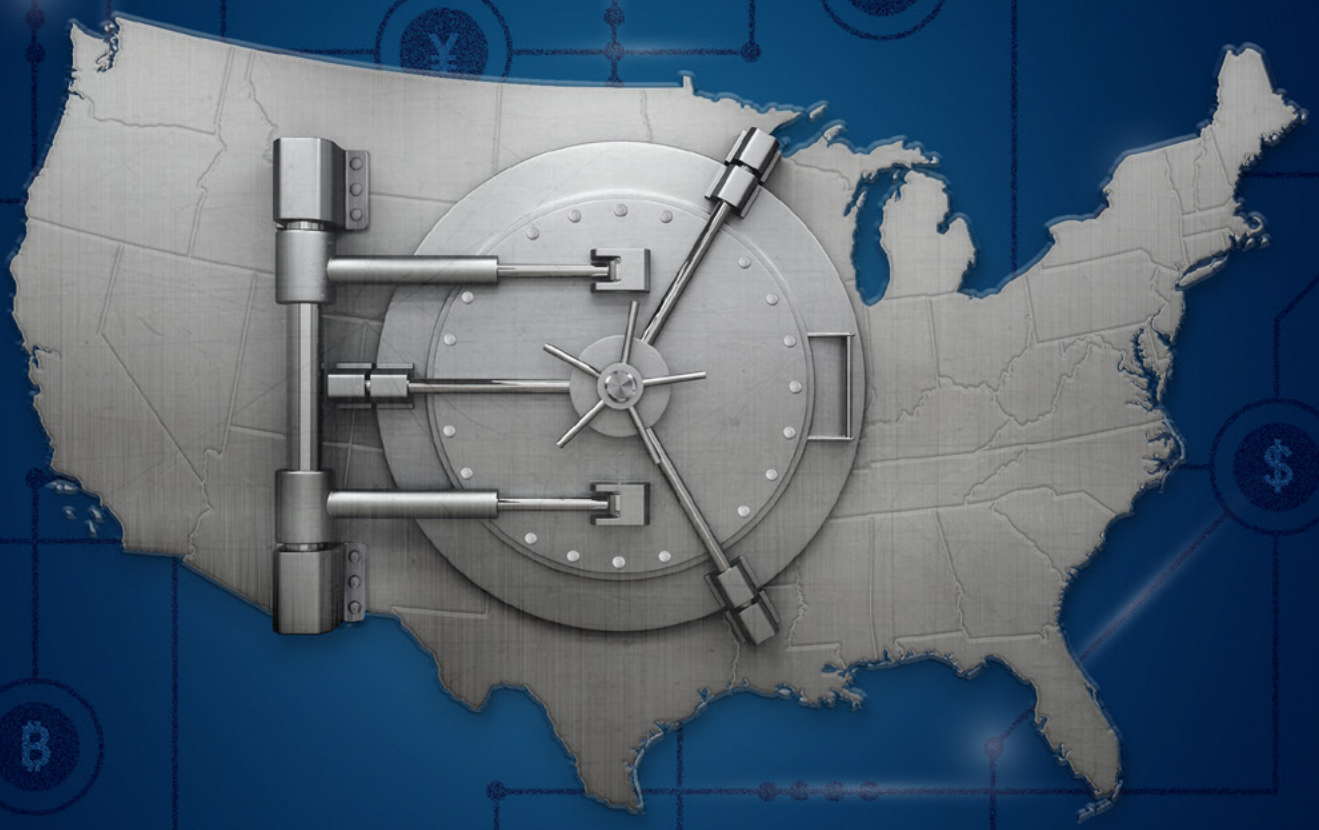
FOUNDATION FOR DEFENSE OF DEMOCRACIES

Securing American Interests

A New Era of Economic Power

February 2017



Center on Sanctions & Illicit Finance

FOUNDATION FOR DEFENSE OF DEMOCRACIES

Securing American Interests
A New Era of Economic Power

Eric B. Lorber

With contributions by

The Hon. Juan C. Zarate
Mark Dubowitz
Chip Poncy
Dr. Jonathan Schanzer
Dr. Zack Cooper
Elaine K. Dezenski
Adnan Kifayat
Dr. Michele Malvesti
J. R. (Bob) McBrien
Dr. Samantha Ravich
James Rickards
Amit Sharma
Amb. John Simon

February 2017

FDD PRESS

A division of the
FOUNDATION FOR DEFENSE OF DEMOCRACIES
Washington, DC

Table of Contents

Foreword

American economic power has become an increasingly critical national security tool in recent years. For well over a decade, the United States has leveraged the size of its economy, the centrality of the dollar, and America's ability to set economic and financial global standards and norms to drive its national security goals.

Yet the geo-economic landscape is changing, and a new era of economic statecraft is upon us. Our competitors have chafed at our use of such power. Our enemies have likewise witnessed our vulnerabilities and understood their own potential to use economic power directly or asymmetrically against the United States and its allies. As a result, the economic statecraft challenges facing the United States are daunting.

They include North Korea's growing use of offensive cyber capabilities that target the international financial system, in addition to the threat from its nuclear weapons and missile programs. Similarly, in the context of the Joint Comprehensive Plan of Action, identifying ways to put economic pressure on Iran for its malign activities throughout the Middle East will require immediate attention.

The administration and Congress will also need to address longer-term, but no less pressing, challenges to U.S. national economic security. Such challenges include an increasingly assertive China that is using all the elements of its national economic power to undercut U.S. interests in East Asia, steal American intellectual property, and pressure Washington's allies and partners. Likewise, the United States will need to address Russia's increasingly assertive use of its natural resources, cyber capabilities, and hybrid warfare, which threaten U.S. interests.

Moreover, as adversaries leverage mechanisms for blunting U.S. tools of economic coercion, such as alternative currencies and sophisticated sanctions-evasion techniques, it may become more difficult to impose the biting economic pressure that has until now proven successful in targeting terrorist financing and undercutting rogue states' economies.

Underpinning the United States' national economic security is the integrity of the international financial system. Washington, the private sector, and the international community have made great strides over the past decade in countering corruption, terrorist financing, and money laundering activities, but much remains to be done. Without a concerted effort to improve the transparency, accountability, and effectiveness of this system, America will be hamstrung in its ability to fight these destabilizing financial flows.

The United States is uniquely positioned to compete on this economic battlefield. U.S. markets are highly attractive and the dollar underpins the majority of cross-border international trade, providing America with unparalleled economic leverage and the ability to shape international standards and norms.

Nevertheless, the United States is unprepared to fully capitalize on these advantages. For example, U.S. economic statecraft is not driven by a coherent, unified strategy; elements of its coercive power, such as sanctions, are not effectively paired with other components of our economic power, such as strategic investments to advance our national security. Likewise, the United States lacks the organizational structure to further its national economic security and to coordinate with our allies and the private sector. Core components for this structure are dispersed across various agencies with little coordination between them.

In this report, experts from the Center on Sanctions and Illicit Finance at the Foundation for Defense of Democracies lay out the contours of this new economic battlefield, and how the United States can take the necessary steps to safeguard its national economic security. Drawing on unparalleled expertise in economic statecraft, coercive diplomacy, international banking and financial integrity, positive economic power, and a deep knowledge of the United States government, these experts identify key threats and opportunities.

The report is the first of its kind to bring together elements of America's economic power into a single,

coherent framework. Until now, policy memoranda, papers, and articles have focused on specific components of national economic security, but none has fully explained how these elements interact to best protect our security. This report endeavors to fill this crucial void and serve as the framework for developing the field of national economic security.

Competing successfully in the evolving economic security battlefield will require innovative strategies, structures, and authorities. The Trump administration and Congress must pay close attention to the economic security threats America faces, and devise sophisticated ways to overcome them. This report aims to provide a roadmap for doing just that.

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

Mark Dubowitz, Chief Executive Officer, Foundation for Defense of Democracies; Director, FDD's Center on Sanctions and Illicit Finance

Chip Poncy, Senior Advisor, FDD's Center on Sanctions and Illicit Finance

Dr. Jonathan Schanzer, Senior Vice President for Research, Foundation for Defense of Democracies

David Asher, former Senior Advisor, U.S. Department of State

Michael Braun, former Chief of Operations, Drug Enforcement Administration

John Cassara, former Special Agent detailee, Office of Terrorism Finance and Financial Intelligence, U.S. Department of the Treasury

Dr. Zack Cooper, Center for Strategic and International Studies

Toby Dershowitz, Senior Vice President, Government Relations and Strategy, Foundation for Defense of Democracies

Elaine K. Dezenski, CEO, LumiRisk, LLC; former Senior Director and Head of Partnering Against Corruption Initiative, World Economic Forum

Amb. Paula J. Dobriansky, former Under Secretary of State for Democracy and Global Affairs

Adnan Kifayat, former Acting Special Representative to Muslim Communities, U.S. Department of State

Dr. Matthew Levitt, former Deputy Assistant Secretary for Intelligence and Analysis, U.S. Department of the Treasury

Michael Madon, former Deputy Assistant Secretary, Office of Intelligence and Analysis, U.S. Department of the Treasury

Dr. Michele Malvesti, former Senior Director for Combatting Terrorism Strategy, National Security Council

J.R. (Bob) McBrien, former Associate Director for Global Targeting, Office of Foreign Assets Control, U.S. Department of the Treasury

Gretchen Peters, Executive Director, Satao Project; Author, *Seeds of Terror*

Dr. Samantha Ravich, former Deputy National Security Advisor to the Vice President

James Rickards, Editor, *Strategic Intelligence*; author of *Currency Wars* (2011), *The Death of Money* (2014), *The New Case for Gold* (2016), *and The Road to Ruin* (2016)

Amit Sharma, former Chief of Staff, Mitsubishi UFJ Securities; former senior official, U.S. Department of the Treasury

Amb. John Simon, former U.S. Ambassador to the African Union; former Executive Vice President, Overseas Private Investment Corporation

**The signatories above include members of CSIF's Board of Advisors. Affiliations noted here are for informational purposes only. Select members may be serving exclusively in their personal capacities. Board membership does not mean endorsement of every product produced by CSIF or FDD or the views expressed by individuals affiliated with CSIF or FDD.*

Introduction and Summary

On the eve of a state visit by Chinese President Xi Jinping in September 2015, the United States and China struck a major – if informal – agreement to limit the Chinese government's cyber theft of U.S. industries' proprietary information.[1] Chinese state-sponsored hacker units and state-owned enterprises were responsible for what then-NSA director Lt. Gen. Keith Alexander in 2012 called the "greatest transfer of wealth in history."[2] The timing of this agreement was no accident; in the lead-up to the visit, the United States threatened to impose powerful economic sanctions on Chinese hacker units and entities, as well as on Chinese companies that were benefiting from this illicitly-acquired information. Since the agreement, Chinese government-sponsored cyber theft of U.S. companies' proprietary information has seemingly declined somewhat, with reports suggesting that the threat of sanctions may have been a factor.[3]

This episode highlights the emerging tools of economic power that play an increasingly important role in U.S. national security. Popular attention is generally focused on the use of sophisticated economic sanctions to tackle difficult foreign policy challenges, such as Iran's nuclear program and support for terrorism, or Russia's cyber attacks against the United States, annexation of Crimea, and support for separatists in Ukraine. But in recent years, the United States has been using a wider set of economic tools to achieve its foreign policy objectives. These include punitive measures to influence private sector decision-making, like Section 311 designations under the USA PATRIOT Act, under which financial institutions or entire jurisdictions can be designated as a "primary money laundering concern," as well as economic power including strategically deployed aid. The United States has a full complement of non-kinetic tools for a range of foreign policy issues.

And the use of these tools comes none too soon. There is a growing recognition among policymakers that the United States faces myriad vulnerabilities and opportunities in this new landscape of national economic security competition. New technologies and novel means of financial influence are enabling

1. Ellen Nakashima and Steven Mufson, "U.S., China vow not to engage in economic cyberespionage," *The Washington Post*, September 25, 2015. (https://www.washingtonpost.com/national/us-china-vow-not-to-engage-in-economic-cyberespionage/2015/09/25/90e74b6a-63b9-11e5-8e9e-dce8a2a2a679_story.html)

2. Josh Rogin, "NSA Chief: Cybercrime constitutes the 'greatest transfer of wealth in history,'" *Foreign Policy*, July 9, 2012. (http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/)

3. David E. Sanger, "Chinese Curb Cyberattacks on U.S. Interests, Report Finds," *The New York Times*, June 20, 2016. (http://www.nytimes.com/2016/06/21/us/politics/china-us-cyber-spying.html?_r=0); For other sources suggesting that Chinese cyber attacks were already in decline before the threat of sanctions, see "Red Line Drawn: China Recalculates Its Use of Cyber Espionage," *Fireeye iSight Intelligence*, June 2016, page 10. (https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf)

old adversaries to employ new tactics alongside traditional economic statecraft for illicit or anti-American objectives.

Despite the aforementioned agreement, China continues to steal billions of dollars of intellectual property from the United States, with a particular focus on appropriating high-tech software to bolster its own economy, develop its military, and identify U.S. political, economic, and military vulnerabilities.[4] The resulting transfer of technology from U.S.-based multinationals has allowed Chinese companies to take larger chunks of the global solar, wind turbine, and high-speed rail markets. At the same time, Chinese infrastructure and extraction projects in Africa, Central Asia, and Latin America are facilitating access to raw materials and providing Beijing with significant political influence in ways that challenge U.S. interests.

China is also pulling pages from the United States' sanctions playbook. In 2010, for example, following the arrest of a Chinese ship captain after he rammed a Japanese Coast Guard vessel in a disputed maritime region, Beijing restricted exports to Japan of rare earth elements (essential to many high-tech industries).[5] Similarly, in response to U.S. threats to impose economic sanctions on Chinese individuals and entities for cyber attacks, Beijing was prepared to impose new banking sector regulations that would prohibit its firms from using non-Chinese technology, which would have encumbered U.S. companies doing business in China.[6] Recently, China also banned charter flights from South Korea after Seoul and Washington decided to deploy THAAD missile defense systems in South Korea.[7]

Moscow has also followed suit. In the December 2015 spat between Russia and Turkey over the downing of a Russian military aircraft along the Turkish border, the Kremlin imposed restrictions on Turkey's tourism industry, canceled visa-free travel between the countries, suspended a joint pipeline project, and banned the import of certain Turkish goods.[8]

Russia has also become increasingly aggressive in cyber space, including attempting to influence the 2016 U.S. presidential election, according to the U.S. intelligence community.[9] Similarly, Russian hackers – likely backed by Moscow – have attacked critical infrastructure to destabilize and coerce Russia's neighbors, such as the February 2016 cyber attack on Ukraine's power grid.[10]

These challenges are not limited to China and Russia. Rogue states have begun engaging in economic warfare in ways that directly threaten U.S. national security objectives, as well as the integrity of the international financial system. North Korea, for example, was recently implicated in using sophisticated cyber capabilities to steal more than 80 million dollars from a number of

4. Lesley Stahl, "The Great Brain Robbery," *CBS News*, January 17, 2016. (http://www.cbsnews.com/news/60-minutes-great-brain-robbery-china-cyber-espionage/)
5. Keith Bradsher, "Amid Tension, China Blocks Vital Exports to Japan," *The New York Times*, September 22, 2010. (http://www.nytimes.com/2010/09/23/business/global/23rare.html)
6. Cory Bennett, "Obama cyber sanctions could spur Chinese backlash," *The Hill*, September 15, 2015. (http://thehill.com/policy/cybersecurity/253713-obama-cyber-sanctions-could-spur-chinese-backlash)
7. Hyunjoo Jin, "South Korea considers 'measures' as China blocks charter flights," *Reuters*, Jan. 2, 2017. (http://www.reuters.com/article/us-southkorea-china-airlines-idUSKBN14M0F7)
8. "Travel, tourism sectors generate 12 pct of Turkey's GDP," *Hurriyet Daily News* (Turkey), May 28, 2015. (http://www.hurriyetdailynews.com/travel-tourism-sectors-generate-12-pct-of-turkeys-gdp-report.aspx?pageID=238&nID=83118&NewsCatID=349)
9. Dana Priest, Ellen Nakashima, and Tom Hamburger, "U.S. investigating potential covert Russian plan to disrupt November elections," *The Washington Post*, September 5, 2016. (https://www.washingtonpost.com/world/national-security/intelligence-community-investigating-covert-russian-influence-operations-in-the-united-states/2016/09/04/aec27fa0-7156-11e6-8533-6b0b0ded0253_story.html)
10. Evan Perez, "U.S. official blames Russia for power grid attack in Ukraine," *CNN*, February 11, 2016. (http://www.cnn.com/2016/02/11/politics/ukraine-power-grid-attack-russia-us/); See also Pasi Eronen, "Russian Hybrid Warfare: How to Confront a New Challenge to the West," *Foundation for Defense of Democracies*, June 2016. (http://www.defenddemocracy.org/content/uploads/documents/Russian_Hybrid_Warfare.pdf)

banks, including the Central Bank of Bangladesh.[11] In that case, North Korean hackers created false Society for Worldwide Interbank Financial Telecommunication (SWIFT) payment messages and, as a result, were able to trick unwitting financial institutions to transfer millions of dollars to fake accounts and into state-sponsored cyber criminals' coffers. Indeed, the continuing and aggressive threat posed by North Korea will require the Trump administration's concerted and immediate attention.

Likewise, non-state actors are also corrupting the international financial system by using it to finance terrorism. For example, the Islamic State has solicited and received significant sums of money from supporters in Western Europe, often through pre-paid credit cards, to augment its operations in Iraq, Syria, and Libya.[12] Stopping this activity is a focus of recent U.S. and international efforts to protect the integrity of the international financial system and prevent adversaries from using the system to their advantage.

The United States is ideally suited to take on these challenges. Our economy is the largest in the world, U.S. businesses are at the forefront of technological innovation, and countries and companies worldwide prioritize doing business with U.S. companies. On the other hand, the openness of the U.S. system exposes us to additional vulnerabilities that our adversaries may not have.

While the United States as a matter of course develops and implements a national security strategy, it has addressed its national economic security in a more piecemeal and uncoordinated fashion. This is due in large part to different agencies and offices having responsibility for various facets of U.S. economic power. The result is a failure to pair punitive and positive economic power for maximum effect.

The United States should develop a national economic security strategy that identifies how and when to use economic coercion like sanctions, but also how and when to help strengthen the integrity of the international financial system. Elements of such a strategy will require cooperation with the private sector – in particular the financial sector. A successful strategy will also rely heavily on our working with international partners – including the United Kingdom, Germany, and other EU member states, key financial and commercial centers, and international organizations like the Financial Action Task Force (FATF).

The U.S. should also set up new federal government structures, including an Office of Policy Planning at the Treasury Department reporting to the Secretary of the Treasury, as well as better integrate the National Security Council and the National Economic Council to get the most out of our tools of economic coercive diplomacy.

This report provides President Donald Trump's new administration with an overview of the key national economic security issues he will face. The report suggests ways to better prepare the United States to compete successfully in the evolving national economic security enterprise. It also provides longer-term recommendations for using U.S. economic power to address pressing concerns.

11. Nicole Perlroth and Michael Corkery, "North Korea Linked to Digital Attacks on Global Banks," *The New York Times*, May 26, 2016. (http://www.nytimes.com/2016/05/27/business/dealbook/north-korea-linked-to-digital-thefts-from-global-banks.html?_r=0)

12. For a discussion of how the Islamic State has raised funds abroad and transferred it to its territory, see Magnus Ranstorp, "Microfinancing the Caliphate: How the Islamic State is Unlocking the Assets of European Recruits," *Combating Terrorism Center at West Point*, May 25, 2016. (https://www.ctc.usma.edu/posts/microfinancing-the-caliphate-how-the-islamic-state-is-unlocking-the-assets-of-european-recruits)

Sharpening U.S. Tools of Economic Coercion

In the early 2000s, the United States began refining powerful tools of economic statecraft to pressure rogue actors and prevent terrorist financing. These measures have become the tools of first, and in some cases only, resort in responding to many international challenges where military force is impractical but diplomacy alone has proven insufficient. As the United States uses these powerful coercive levers in increasingly sophisticated ways, policymakers need to ensure their continued effectiveness.

The New Tools of Economic Coercion

Economic warfare is now the default instrument for confronting challenges to the international order. Sanctions are Washington's weapon of choice to combat Iran's nuclear program, North Korea's nuclear weapons and missile programs, Russia's destabilizing activities in Ukraine, the Assad regime's slaughter in Syria, and the financing of terrorist groups such as the Islamic State, al-Qaeda, Hezbollah, and others.[13]

The power of these tools stems from the strength and centrality of the U.S. economy. The United States, which has the world's largest and most vibrant economy, and whose currency serves as the backbone of the international financial system, is in a powerful position to use its influence to achieve political objectives. U.S. financial sanctions rely on the attractiveness of U.S. and European financial markets. The strength and stability of the U.S. dollar make it the currency of choice for many types of international transactions. Denying access to U.S. dollars provides the key basis for many U.S. financial sanctions: If a company wants to transact in dollars, it needs access to U.S. financial markets to do so, and therefore must comply with U.S. sanctions policies. This underpins the United States' powerful economic pressure to achieve foreign policy objectives.

The transformation of blunt and broad comprehensive embargoes against states into the sophisticated, targeted sanctions we know today has its roots in the wake of 9/11 and the all-out offensive against al-Qaeda, when the U.S. government began targeting not only its top operatives, but also the funders that enable the terror group's activities.[14] With the passage of the USA PATRIOT Act, the United States was able to impose requirements related to anti-money laundering and financial crime compliance on a wide range of new commercial actors, and limit the ability of terrorist groups to use licit businesses and financial channels

13. Mark Dubowitz and Annie Fixler, "'SWIFT' Warfare: Power, Blowback, and Hardening American Defenses," *Foundation for Defense of Democracies*, July 2015, page 5. (http://www.defenddemocracy.org/content/uploads/publications/Cyber_Enabled_Swift.pdf)
Ibid, page 5; See also Juan Zarate, "Harnessing the Financial Furies: Smart Financial Power and National Security," *The Washington Quarterly*, October 2009, pages 45-50. (https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/twq09octoberzarate.pdf)

to finance their activities.[15] At the international level, the United Nations, the Financial Action Task Force, and the Wolfsberg Group also developed standards to combat terrorist financing.[16]

This focus on the financing of terrorism expanded in the mid-2000s as policymakers recognized the power of these financial tools. U.S. and international actors began targeting proliferation activities with these financial tools. In 2005, President George W. Bush signed Executive Order 13382, which provided the authority to block assets of persons engaged in or supporting the development of weapons of mass destruction.[17] This targeted North Korea, Iran, and Syria.

But the United States went far beyond simple designations against certain persons. In the fight to stop North Korea's nuclear weapons program, the United States leveraged the power of the private sector – exploiting financial institutions' reluctance to do business with any companies seen as tainted by North Korea's illicit activity.[18]

The United States also developed new ways to pressure Iran and Russia. For example, the U.S. more aggressively imposed secondary sanctions. This threatened foreign companies' access to U.S. markets if they did business with the Islamic Republic while it pushed forward with its illicit nuclear program.[19] Likewise, in response to Russia's annexation of Crimea and ongoing support for separatists in Ukraine, the United States moved beyond simply sanctioning particularly entities. It deployed so-called sectoral sanctions on particular types of business activity with targeted entities, prohibiting the issuance of new debt with over 30-day maturity and equity and certain energy-related transactions.[20]

The United States developed other tools, too. For example, Section 311 of the USA PATRIOT Act provides Treasury with the authority to designate illicit financial actors as entities of "primary money-laundering concern." On November 22, 2011, expanding on its designations of individual Iranian financial institutions, Treasury issued a Section 311 finding that Iran was "a jurisdiction of primary money laundering concern," citing its "support for terrorism," "pursuit of weapons of mass destruction," and "illicit and deceptive financial activities that Iranian financial institutions … engage in to facilitate Iran's illicit conduct and evade sanctions." Treasury targeted the Central Bank of Iran and made

15. Uniting and Strengthening America By Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. 107-56, 115 Stat. 272, codified as amended at 107 U.S.C. (https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf)

16. The Financial Action Task Force is an international standard-setting body that develops and implements key anti-money laundering and countering the financing of terrorism-related recommendations. The Wolfsberg Group is an organization of thirteen global banks that sets international banking standards related to anti-money laundering and countering the financing of terrorism. Juan Zarate, "Harnessing the Financial Furies: Smart Financial Power and National Security," *The Washington Quarterly*, October 2009, pages 45-50. (https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/twq09octoberzarate.pdf)

17. Executive Order 13382, "Blocking Property of Weapons of Mass Destruction Proliferators and Their Supporters," June 28, 2005. (https://www.federalregister.gov/documents/2005/07/01/05-13214/blocking-property-of-weapons-of-mass-destruction-proliferators-and-their-supporters)

18. Juan Zarate, "Harnessing the Financial Furies: Smart Financial Power and National Security," *The Washington Quarterly*, October 2009, pages 50-53. (https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/twq09octoberzarate.pdf)

19. Eric Lorber, *Testimony before the Senate Judiciary Committee, Subcommittee on Oversight, Agency Action, Federal Rights, and Federal Courts*, November 4, 2015. (https://www.judiciary.senate.gov/imo/media/doc/11-04-15%20Lorber%20Testimony1.pdf)

20. U.S. Department of the Treasury, Office of Foreign Assets Control, "Directive 1 (As Amended) Under Executive Order 13662," September 12, 2014. (https://www.treasury.gov/resource-center/sanctions/Programs/Documents/eo13662_directive1.pdf); U.S. Department of the Treasury, Office of Foreign Assets Control, "Directive 2 (As Amended) Under Executive Order 13662," September 12, 2014. (https://www.treasury.gov/resource-center/sanctions/Programs/Documents/eo13662_directive2.pdf); U.S. Department of the Treasury, Office of Foreign Assets Control, "Directive 3 (As Amended) Under Executive Order 13662," September 12, 2014. (https://www.treasury.gov/resource-center/sanctions/Programs/Documents/eo13662_directive3.pdf); U.S. Department of the Treasury, Office of Foreign Assets Control, "Directive 4 (As Amended) Under Executive Order 13662," September 12, 2014. (https://www.treasury.gov/resource-center/sanctions/Programs/Documents/eo13662_directive4.pdf)

it clear that the country's entire financial system posed "illicit finance risks for the global financial system."[21] As a result, financial institutions across the globe – fearful of doing business in a jurisdiction with such lax anti-money laundering and anti-terrorist financing controls – reduced their business, further pressuring the Islamic Republic to halt its nuclear activity.

Likewise, in June 2016, the United States designated North Korea as a jurisdiction of primary money-laundering concern, requiring U.S. banks to close down correspondent account access to North Korean entities.[22]

Yet the United States' ability to use these tools may be more complicated moving forward. First, in pursuit of its political goals, the U.S. government undercut its own warnings about the illicit conduct of rogue states by suspending or lifting sanctions on entities without evidence that they had ceased their malign conduct. This may make it more difficult to maintain the credibility of current and future warnings. That was the case when the U.S. allowed frozen assets to be removed from China's Banco Delta Asia to North Korea, and it is the case again on a much larger scale with many of the sanctions that have been lifted on Iran as a result of the Joint Comprehensive Plan of Action (JCPOA). Similarly, rolling back sanctions imposed for Russian violations of Ukrainian sovereignty while such violations continue would decrease the credibility of future U.S. sanctions and reward Russian aggression.

There are other indicators suggesting that U.S. financial sanctions may become *less* potent in the medium to long term. In November 2015, the International Monetary Fund added the Chinese renminbi as a Special Drawing Rights (SDR) currency, signaling its stability and elevating it to a similar status as the dollar, yen, euro, and British pound.[23] The rise of a non-dollar currency unaffiliated with the European Union or our East Asian partners poses a risk to the United States' ability to impose crippling financial sanctions. Indeed, if alternate reserve currencies such as the renminbi become more attractive, companies may no longer view the U.S. dollar and the U.S. financial system as crucial to conducting transactions. This could limit U.S. leverage on sanctions targets.

Our adversaries are also increasing their reliance on gold reserves, both to avoid the impact of U.S. sanctions and to create an offensive counterweight to U.S. dominance of dollar payment systems. Currently, U.S. dollar-denominated instruments and transactions constitute about 60 percent of global reserves and 80 percent of global payments, respectively. This gives the U.S. unrivaled dominance over the international monetary system. Gold offers adversaries an alternative in a world of U.S.-imposed dollar-based sanctions. Gold is physical, not digital, so it cannot be hacked or frozen. It is easy to transport by air to settle balance of payments or other transactions between nations. Gold flows cannot be interdicted at SWIFT or FedWire. And gold is fungible and non-traceable.[24]

---

21. Mark Dubowitz and Annie Fixler, "'SWIFT' Warfare: Power, Blowback, and Hardening American Defenses," *Foundation for Defense of Democracies*, July 2015, pages 11-12. (http://www.defenddemocracy.org/content/uploads/publications/Cyber_Enabled_Swift.pdf)

22. U.S. Department of the Treasury, Press Release, "Treasury Takes Actions to Further Restrict North Korea's Access to The U.S. Financial System," June 1, 2016. (https://www.treasury.gov/press-center/press-releases/Pages/jl0471.aspx)

23. Keith Bradsher, "China's Renminbi is Approved by I.M.F. as a Main World Currency," *The New York Times*, November 30, 2015. (http://www.nytimes.com/2015/12/01/business/international/china-renminbi-reserve-currency.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region&region=top-news&WT.nav=top-news)

24. To prepare for a physical gold alternative to the U.S. dollar, Russia increased its gold reserves 280 percent from the first quarter of 2006 to the second quarter of 2016 (from 386.5 metric tons to 1,498.7 metric tons), while China increased its gold reserves 203 percent in the same period (from 600 metric tons to 1,823.3 metric tons). China has been consistently non-transparent about its activities in the gold market. Based on China's mining output and reliable data on gold exports from Hong Kong and Switzerland to China, there is good reason to conclude that China's actual gold holdings are nearer 4,000 metric tons (a 5,670-percent increase since 2006). The comparable increase for Turkey is 308 percent. Reliable data is not available for Iran; however, exports from Turkey and Dubai to Iran are significant, and there is good reason to conclude that Iran is also a rising gold power relative to the size of its economy.

These developments suggest that policymakers at the White House, Treasury, State, and Commerce Departments will face new challenges ahead. They need to ensure that U.S. sanctions remain effective even as countries such as Russia and China, rogue states such as Iran and North Korea, and non-state actors attempt to blunt our economic coercion.

Key Principles for Strengthening Coercive Economic Power

When developing sanctions policy, policymakers need to ensure that our coercive economic statecraft will be successful in addressing traditional threats and emerging challenges:

How to More Strategically Use Economic Power

While economic statecraft has been a tool of first resort in recent years, policymakers need to do more to ground the use of such tools in a larger strategic framework. The following recommendations can help achieve that end:

- **Be clear about the purpose of employing sanctions.** Policymakers need to properly understand the purpose of imposing coercive leverage. For example, sanctions designed to make it more difficult for a terrorist organization to transfer funds or access the international financial system (degrading capabilities) should be designed differently than sanctions meant to deter a country like Russia from engaging in destabilizing activities in its region (deterrence). While evidence exists that certain tools can be effective in both cases, policymakers need to first consider what objective they are trying to achieve, and then consider whether sanctions are appropriate.
- **Emphasize proactive tools, not only reactive ones.** Policymakers often turn to sanctions *in response* to actions by states or illicit non-state actors. But sanctions should also be used as a tool for shaping positive outcomes. For example, with South Sudan, the United States is now using sanctions designations to compel key actors to come to the table to discuss and solidify peace settlements, before the country descends into civil war.[25] Policymakers should think more creatively about how these measures can be used across a wider range of situations.
- **Use economic statecraft in conjunction with other tools.** The Iran case illustrates that economic pressure – when coupled with other tools of statecraft such as offensive cyber operations and aggressive diplomacy – can coerce states into seeking negotiated agreements as a way to alleviate the economic pressure. Conversely, economic sanctions used in isolation are often unlikely to achieve ambitious objectives.[26] For example and as discussed in the Iran case study in this report, the diminishing credibility of the U.S. military threat undercut American negotiating leverage and led to a deal that did not permanently cut off Iran's pathways to a nuclear weapon.

Military threats can also impact the financial battlefield. For example, recently U.S. military forces have used kinetic operations to strike Islamic State-controlled banks in Iraq and Syria.[27] Given the difficulties U.S. and European authorities have had in using non-military methods to target the Islamic State (IS)'s fundraising, these operations were designed to impede the IS's self-sufficient financial system.

25. "US threatens South Sudan with UN sanctions if peace deal not reached soon," *The Guardian* (UK), August 18, 2015. (https://www.theguardian.com/world/2015/aug/18/south-sudan-war-un-sanctions)

26. Gary Clyde Hufbauer, Jeffrey J. Schott, Kimberly Ann Elliott, and Barbara Oegg, *Economic Sanctions Reconsidered, 3rd Edition*, (Washington, D.C.: The Peterson Institute for International Economics, 2009); Robert A. Pape, "Why Economic Sanctions Do Not Work," *International Security*, Fall 1997. (https://web.stanford.edu/class/ips216/Readings/pape_97%20(jstor).pdf); David A. Baldwin, "The Sanctions Debate and the Logic of Choice," *International Security*, Fall 1997. (http://www.princeton.edu/~dbaldwin/selected%20articles/Baldwin%20(1999-2000)%20The%20Sanctions%20Debate%20and%20the%20Logic%20of%20Choice.pdf)

27. Jack Moore, "U.S.-led Coalition Targets ISIS Banks in Mosul Strikes," *Newsweek*, February 15, 2016. (http://www.newsweek.com/us-led-coalition-targets-isis-banks-mosul-strikes-426604)

How to More Effectively Employ These Tools

- **Seek out narrow measures where the private sector can amplify the effects.** Narrow measures can have outsized strategic effects. The Banco Delta Asia designation impacted North Korea's willingness to bargain, thereby leading it back to the negotiating table. And the Sectoral Sanctions Identifications (SSI) List, which is a new type of sanctions list that prohibits U.S. persons from providing certain financial services such as debt and equity to targeted Russian entities, reduced investment in the Russian finance, defense, and energy sectors in ways that significantly amplified the designations.[28] The private sector's response is crucial to amplify these designations. Private businesses – and in particular financial institutions – view such designations with significant concern, and often will cease providing even permitted goods and services to target countries for fear of inadvertently running afoul of these prohibitions. When considering imposing economic sanctions, policymakers should assess whether they are practical for private sector implementation.

Another targeted approach with an outsized impact is leveraging U.S. export control law. In April 2016, the U.S. Commerce Department placed Chinese telecommunications maker ZTE on its "entity list," meaning that U.S. companies could not export most tech products to ZTE. The reason for the ban was that ZTE had exported U.S.-origin telecoms equipment to Iran. ZTE almost immediately began cooperating with Commerce, sacked several officials, and is in the process of overhauling its compliance program. In return, the Commerce Department has suspended the export ban.[29] The U.S. government may have had a more difficult time adding ZTE to the SDN (Specially Designated National) list given the political sensitivities of designating a large Chinese company, but a more limited sanction was more feasible, and offers a model for targeting non-U.S. enterprises engaging in illicit conduct.

- **Cut off sanctions targets from the international financial system in ways that limit pain to the United States and its allies.** The Europeans are feeling the brunt of sanctions on Russia, due in large part to their closer business connections with Vladimir Putin's regime. As a result, the EU is under increasing pressure to lift these economic penalties, regardless of whether Russia fulfills its obligations under the Minsk Agreement.[30] The more that U.S. sanctions programs strain our allies, the harder it becomes for them to support those programs in a meaningful way. The United States should identify targets that, if designated, would cause minimal damage to our allies for maximum impact on the target.
- **Develop financial measures that enjoy multilateral support, but are not beholden to multilateral institutions.** Where possible, the involvement of other countries makes sanctions more effective. In the case of Iran, the U.S. State and Treasury Departments successfully built international buy-in for broader sanctions. Even though significant compromises were necessary to get Chinese and Russian approval, UN resolutions provided a foundation for other countries to implement their own multilateral and unilateral sanctions.[31] In contrast, due to the Russian veto power at the UN Security Council, the Russia sanctions program could not rely on the United Nations even as it brought together a coalition of the U.S. and European countries.

---

28. Juan Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare*, (New York: PublicAffairs, 2013), pages 239-247; See also Elizabeth Rosenberg, Zachary K. Goldman, Dr. Daniel Drezner, and Julia Solomon-Strauss, "The New Tools of Economic Warfare: Effects and Effectiveness of Contemporary U.S. Financial Sanctions," *Center for a New American Security*, April 15, 2016, pages 14-26. (https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-EconomicWarfare-160408v02.pdf)

29. Juro Osawa, "ZTE's Temporary Sanction Relief Extended by the U.S.," *The Wall Street Journal*, June 28, 2016. (http://www.wsj.com/articles/ztes-temporary-sanction-relief-extended-by-the-u-s-1467075408)

30. Howard Amos, "EU Unity Crumbles as Russia Sanctions Extension Debate Rages," *International Business Times*, June 2, 2016. (http://www.ibtimes.com/eu-unity-crumbles-russia-sanctions-extension-debate-rages-2376693)

31. Peter D. Feaver and Eric B. Lorber, "Coercive Diplomacy: Evaluating the Consequences of Financial Sanctions," *Legatum Institute*, November 2010, pages 27-31. (https://lif.blob.core.windows.net/lif/docs/default-source/publications/2010-publications-coercive-diplomacy.pdf?Status=Temp&sfvrsn=2)

Still, sanctions can work with minimal multilateral cooperation between the United States and its allies, and can even work without full multilateral cooperation. American financial power enforced by the consequences of secondary sanctions on private sector actors can be a key driver in persuading reluctant countries to join a U.S. effort to put significant economic pressure on a target state.

- **Focus sanctions and financial measures on illicit conduct.** While the United States can always use economic power broadly, focusing on underlying illicit conduct wherever possible will increase multilateral buy-in. In particular, sanctions measures that are focused on internationally-recognized illicit activity (such as terrorist or proliferation-sensitive financing, corruption, kleptocracy, and human rights abuses) are more likely to garner support from partners. To the extent that the use of sanctions is seen as "political," it may be more difficult to bring together a coalition of forces. For that reason, the U.S. should be careful in the unwinding of illicit conduct-based sanctions for any reason external to that conduct, such as the example of Iran's Bank Sepah, a missile-financing bank that was delisted by the U.S. to secure a nuclear agreement that did not target Iran's missile activities (the bank reportedly may also have been delisted in order to secure the release of U.S. hostages).[32] Another example would be the lifting of Ukraine-related sanctions without a concrete reversal of Russia's threats to Ukrainian sovereignty.
- **Increase the focus on non-financial companies.** The U.S. experience with Russia and Iran highlights the impact U.S. sanctions can have on energy companies, insurance companies, and shipping and ports operators. These sanctions can be a powerful complement to banking sanctions. Treasury should focus on expanding its expertise on non-financial sectors to identify other pressure points in the future. This will be particularly important if and when countries like China and Russia develop payment systems that let them operate outside of the U.S. financial system or in non-dollar denominations.
- **Track the benefits and threats of technological developments.** Changes in the technological landscape could see technology itself emerge as a potential sanctions pressure point. For example, the shift from local servers and computers to cloud networks could create major points of leverage. In the future, an SDN listing of a company may not only freeze its assets and cut it off from the U.S. financial system; it may knock out the company's ability to use cloud-based email servers or access corporate accounting tools. The Chinese are purportedly worried about this development and are pushing hard for their own government agencies and companies to develop workaround solutions.
- **Get the timing right.** With the Russia sectoral sanctions program, there was a mismatch between the intended time frame of the sanctions impact and Russia's ability to establish facts on the ground. The SSI (Sectoral Sanctions Identifications) sanctions were designed to target Russia's economy over a five to seven year time frame, yet Russia was able to continue to destabilize Eastern Ukraine in the short term and to establish facts on the ground. As a general rule, policymakers need to tailor their coercive tools to ensure that the pressure will impact the target's behavior in the appropriate time frame. In addition, officials should try to employ these tools at the right "market" time. For example, the sanctions on Russia had a short-term effect (even if not by design) because of the parallel drop in oil prices, which prevented Russia from blunting the sanctions' impact.

How to Expand the Power of U.S. Economic Coercion

- **Understand the power – and limits – of the U.S. economy.** In the case of Iran, when the U.S. government put foreign companies to a choice, most saw much greater opportunities in the U.S. than in Iran given the relative size and attractiveness of the two markets. This dynamic may not always hold,

32. Jay Solomon and Carol E. Lee, "U.S. Signed Secret Document to Lift U.N. Sanctions on Iranian Banks," *The Wall Street Journal*, September 29, 2016. (http://www.wsj.com/articles/u-s-signed-secret-document-to-lift-u-n-sanctions-on-iranian-banks-1475193723)

however. For example, if the United States were to consider imposing sanctions on China, the world's second-largest economy, many companies could choose to do business in the latter if forced to choose.

- **Pressure problematic U.S. allies that offer permissive jurisdictions for terror finance.** To make the Specially Designated Nationals list more effective, the U.S. government should take new steps to discourage U.S. allies such as Qatar, Turkey, Kuwait, Pakistan, and Saudi Arabia from allowing Specially Designated Global Terrorists to enjoy legal impunity in their territory.[33] Options include legislation such as the bipartisan Stop Terrorist Operational Resources and Money (STORM) Act that offers the president statutory penalties against such negligent jurisdictions,[34] requiring licensing of dual use items exported to countries that provide such safe haven to terrorist operatives pursuant to section 6(j) of the Export Administration Act of 1979, and simply naming and shaming these allies for their misconduct – either in public remarks or even by seeking the extradition of U.S.-sanctioned individuals from their territory.[35]
- **Beware of sanctions ambiguity.** U.S. sanctions regulations are often ambiguous. For example, Treasury's Office of Foreign Assets Control (OFAC) does not define with sufficient precision what providing a service, directly or "indirectly" means for purposes of liability. This ambiguity, particularly when ratcheting sanctions up on a target, can be useful, as it can deter activities beyond what is actually prohibited under U.S. law. At the same time, this ambiguity can be a significant obstacle when trying to unwind sanctions. Indeed, private businesses are extremely cautious in re-entering markets, and their reluctance can undermine the political agreements that led to the lifting of the sanctions in the first place (such as in the case of Iran).
- **Employ "targeted unwinding" and be strategic when releasing financial pressure.** Although U.S. policymakers have learned much about imposing sanctions, the inability to ease sanctions can seriously complicate Washington's diplomacy. Coercion, after all, is ultimately about following through on promises. When sanctions are used to bring about certain policy outcomes, they contain an explicit threat and an implicit guarantee: If a state continues the unwanted policy, it will continue to suffer sanctions; if the state changes course, the punishment will end. But if the United States proves incapable of ending sanctions after its demands are met, targeted states will have little incentive to favorably adjust their activities.[36]

  Policymakers grappling with these challenges should consider four core principles that can sharpen sanctions policy.

  - *Sanctions relief must be grounded in a clear understanding of sanctions objectives and results.*

    Just as sanctions must be tailored to the objectives of policymakers, sanctions relief must be carefully tailored and targeted to avoid undesirable outcomes, such as strengthening an ongoing repressive dictatorship or providing it with additional financial resources to commit aggressive actions outside its borders.

33. Daveed Gartenstein-Ross and Jonathan Schanzer, "Trump Wants to Shake Up the World Order? Here's Where He Should Start," *Politico Magazine*, December 11, 2016. (http://www.politico.com/magazine/story/2016/12/trump-administration-foreign-policy-middle-east-allies-enemies-214519)
34. David Andrew Weinberg, "Fifteen years since pivotal executive order, STORM Act could help fight terror finance," *The Hill*, September 23, 2016. (http://thehill.com/blogs/congress-blog/homeland-security/297342-fifteen-years-since-pivotal-executive-order-storm-act)
35. David Andrew Weinberg, "The Gulf Cooperation Council Camp David Summit: Any Results?" *Testimony before the House Committee on Foreign Affairs Subcommittee on the Middle East and North Africa*, July 9, 2015. (http://www.defenddemocracy.org/content/uploads/documents/testimony_weinberg_GCC.pdf)
36. Peter D. Feaver and Eric Lorber, "Penalty Box," *Foreign Affairs*, June 6, 2014. (https://www.foreignaffairs.com/articles/united-states/2014-06-06/penalty-box)

- *When ramping up sanctions programs, know how to unwind them.*

  Policymakers need to design sanctions programs that can be unwound in a way that will help the United States achieve its objectives. For example, sanctions prohibiting particular classes of transactions (such as debt and equity restrictions) may be easier to unwind than broad designations that prohibit all transactions with illicit actors based on underlying bad conduct. Indeed, such broad sanctions often create a reputational taint that deters companies from doing business with these actors long after they cease their illicit activity.

- *Unwinding sanctions provides additional opportunities to pressure rogues.*

  While unwinding sanctions is generally about removing pressure on a rogue regime, such unwinding can be done in ways that further pressures our adversaries to change their behavior. For example, in the case of Iran, the United States and its negotiating partners agreed to license the sale of aircraft to Iran as part of the JCPOA.[37] Yet the United States could have conditioned this license in a way that forced Iran to make a choice between using the aircraft for terrorism-related activities and losing billions in escrowed funds, for example, by requiring Iran to pay all contract costs up front and then including a clause in the contract making clear that if Iran used any of the delivered aircraft for terrorism-related activities, it would forfeit that money and would not receive additional aircraft.[38] In this way, the U.S. lost an opportunity to pressure Iran to cease its support for terrorism.

- *Temper expectations of what unwinding alone can achieve.*

  When unwinding sanctions, the United States must consider that certain risks may still be prohibitive to market participants. Policymakers should always make it clear that unwinding sanctions may not provide the relief these countries seek. For example, foreign banks and companies remain reluctant to engage with Iran even after the JCPOA because doing business with a regime that finances terrorism, backs Bashar al-Assad's slaughter in Syria, conducts missile tests, takes hostages, and carries out mass human rights abuses is a risk that many are not willing to take.

Underpinning all of this is the need to keep the American economy competitive. The United States economy, the central role of its financial system, and the U.S. dollar in the global economy are the source of our ability to impose biting economic sanctions and pressure adversaries to change their malign activities. Keeping the economy robust and attractive will mean that when threatened with a loss of access to U.S. markets, our allies and adversaries alike will be more likely to acquiesce to our political requests.

It remains important to combine these measures with other elements of economic statecraft noted in this report. For example, without continued structural reform and increased transparency in the international financial system, the United States' ability to continue to impose powerful financial sanctions will be hindered. Likewise, without incorporating these tools into a broader economic strategy that includes the use of positive economic power, the United States will undermine its own efforts to change the behavior of its adversaries.

37. U.S. Department of the Treasury, Office of Foreign Assets Control, "Statement of Licensing Policy for Activities Related to the Export or Re-Export to Iran of Commercial Passenger Aircraft and Related Parts and Services," January 16, 2016. (https://www.treasury.gov/resource-center/sanctions/Programs/Documents/lic_pol_statement_aircraft_jcpoa.pdf)

38. Eric B. Lorber, "The Implications of U.S. Aircraft Sales to Iran," *Testimony before the House Committee on Financial Services, Subcommittee on Monetary Policy and Trade*, July 7, 2016. (http://financialservices.house.gov/uploadedfiles/hhrg-114-ba19-wstate-elorber-20160707.pdf); See also Mark Dubowitz, "The Implications of U.S. Aircraft Sales to Iran," *Testimony before the House Committee on Financial Services, Subcommittee on Monetary Policy and Trade*, July 7, 2016. (http://financialservices.house.gov/uploadedfiles/hhrg-114-ba19-wstate-mdubowitz-20160707.pdf)

Case Study: Applying Lessons Learned from a Decade of Financial Pressure on Iran[39]

The United States has maintained sanctions on Iran in one form or another since 1979, but significantly expanded sanctions between 2006 and 2013. After reaching the July 2015 Joint Comprehensive Plan of Action, the United States reversed course and lifted or suspended many of the most significant economic sanctions. This case study discusses how the U.S. Treasury and Congress developed an innovative sanctions program that inflicted significant economic pain on the Iranian regime and how a new administration could rebuild this pressure. The key is to focus on the full range of Iran's illicit conduct.

Focus sanctions and financial measures on illicit conduct:

Then: In 2006, Treasury devised a new strategy aimed at restricting Iran's access to the international financial system by highlighting the money laundering, front companies, and other deceptive practices Tehran used to finance its illicit nuclear and ballistic missile program, as well as its support for terrorism and other rogue regimes. Treasury combined designations of weapons proliferators and terrorist supporters with robust private sector outreach, detailing the illicit finance risks posed by the Iranian regime.[40] As a result, a large number of financial institutions and foreign companies ended their business operations in the Islamic Republic.[41] The sanctions were effective because the private sector's concerns about doing business in Iran were amplified by the impact of Treasury's designations of proliferators and terror financiers.

Now: In the aftermath of the nuclear agreement, Obama administration officials, including Secretary of State John Kerry, repeatedly met with international bankers to encourage banks to reengage with Iran.[42] However, after a decade of heightened awareness of Tehran's continued illicit conduct and more rigorous U.S. sanctions enforcement, the private sector understood the risks that Iran continued to pose; many of the largest global banks kept Iran at arm's length despite strong client interest.[43]

39. Content in this case study adapted and expanded from Mark Dubowitz and Annie Fixler, "'SWIFT' Warfare: Power, Blowback, and Hardening American Defenses," *Foundation for Defense of Democracies*, July 2015. (http://www.defenddemocracy.org/content/uploads/publications/Cyber_Enabled_Swift.pdf); A more detailed list of possible steps a new administration could take to reinforce sanctions against Iran can also be provided upon request.

40. Robin Wright, "Stuart Levey's War," *The New York Times*, November 2, 2008. (http://www.nytimes.com/2008/11/02/magazine/02IRAN-t.html?pagewanted=all&_r=0)

41. Peter Feaver and Eric Lorber, "Coercive Diplomacy: Evaluating the Consequences of Financial Sanctions," *Legatum Institute*, November 2010, pages 28-29. (https://lif.blob.core.windows.net/lif/docs/default-source/publications/2010-publications-coercive-diplomacy.pdf?Status=Temp&sfvrsn=2)

42. David Brunnstrom, "Kerry seeks to soothe European bank nerves over Iran trade," *Reuters*, May 12, 2016. (http://www.reuters.com/article/us-iran-banks-kerry-idUSKCN0Y30OJ)

43. Stuart Levey, "Kerry's Peculiar Message About Iran for European Banks," *The Wall Street Journal*, May 12, 2016. (http://www.wsj.com/articles/kerrys-peculiar-message-about-iran-for-european-banks-1463093348)

The Trump administration can bring greater lucidity to U.S. sanctions policy by clarifying the remaining sanctions architecture, and by imposing new conduct-based sanctions targeting Iran's ballistic missile development, support for terrorism, human rights abuses, cyber activities, and regional aggression. Specifically, the new administration should reaffirm that Iran remains a jurisdiction of primary money laundering concern, as designated under Section 311 of the USA PATRIOT Act;[44] work with Congress to statutorily prohibit U-turn transactions and offshore dollar transactions; issue a clarification that financial institutions will be responsible for enhanced Know Your Customer's Customer (KYCC) rules; mandate enhanced audit standards for any auditor reviewing transactions with Iranian entities; and enforce penalties against any company doing business with the Islamic Revolutionary Guard Corps (IRGC).[45]

The new administration should also support congressional efforts to sanction sectors of the Iranian economy that support Iran's ballistic missile program, sanction the entire Revolutionary Guard as a terrorist entity, and designate the thousands of IRGC-controlled companies that are key players in strategic sectors of Iran's economy.[46] Meanwhile, the White House should task the intelligence community with developing an extensive list of the IRGC officials leading Iran's destabilizing activities in Syria, Iraq, and Yemen, and with examining the Iranian leadership structure and judicial and penal systems, including the IRGC and the Ministry of Intelligence, to identify individuals responsible for human rights abuses.

Escalate sanctions gradually to increase pressure and minimize blowback:

Then: As policymakers in both the executive and legislative branches sought to escalate sanctions on Iran in response to Tehran's nuclear mendacity, they deployed new sanctions tools. Between 2010 and 2012, Congress passed multiple pieces of legislation targeting Iran's banks, energy and automotive sectors, industrial trade, shipping, and insurance. Responding to congressional pressure, the European Union instructed SWIFT to remove designated Iranian banks from its network.[47] This unprecedented measure was made possible in large part by the U.S. and Europe escalating sanctions pressure over the prior six years amidst Iran's continued defiance.

Meanwhile, policymakers targeted Iran's central bank and slowly escalated sanctions on the country's crude oil exports while simultaneously allowing markets to adjust and other oil producers to bring supplies online to offset the reductions from Tehran.[48] First, Congress prohibited all non-humanitarian transactions with Iranian banks unless the transaction was for oil and the purchasing country was in the process of significantly reducing its crude oil purchases.[49] Then, after the EU implemented its own embargo of Iranian oil,[50] Congress took a further step of requiring countries importing Iranian oil to deposit payments in Iranian escrow

44. U.S. Department of the Treasury, Press Release, "Fact Sheet: New Sanctions on Iran," November 21, 2011. (http://www.treasury.gov/press-center/press-releases/Pages/tg1367.aspx)
45. Eric Lorber, "President Trump and the Iran Nuclear Deal," *Foreign Policy*, Nov. 16, 2016. (http://foreignpolicy.com/2016/11/16/president-trump-and-the-iran-nuclear-deal/)
46. Data on unsanctioned IRGC-controlled companies available upon request.
47. "Payments system SWIFT to expel Iranian banks Saturday," *Reuters*, March 15, 2012. (http://www.reuters.com/article/2012/03/15/us-nuclear-iran-idUSBRE82E15M20120315)
48. Ayesha Daya, "Saudi Arabia Can Raise Output 25% If Needed, Naimi Says," *Bloomberg*, March 20, 2012. (http://www.bloomberg.com/news/articles/2012-03-20/saudi-arabia-can-increase-oil-output-25-if-needed-naimi-says)
49. U.S. Department of the Treasury, Press Release, "Fact Sheet: Treasury Amends Iranian Financial Sanctions Regulations to Implement the National Defense Authorization Act," February 27, 2012. (http://www.treasury.gov/press-center/press-releases/Pages/tg1434.aspx)
50. Jerry Dicolo, "EU Embargo on Iran Oil Takes Effect," *The Wall Street Journal*, July 1, 2012. (http://www.wsj.com/articles/SB10001424052702303649504577496463851879258)

accounts that could only be used for the purchase of non-sanctioned local goods or humanitarian goods from other countries.[51] This innovation allowed Iran to continue selling its oil while ensuring the revenue could not be used to support illicit activities. It also severely restricted Iran's access to its overseas foreign exchange reserves.

Now: By 2013, Iran's economy was in free fall and facing an imminent balance of payments crisis.[52] In the summer of 2013, Hassan Rouhani was elected president. The White House soon revealed that it had been conducting secret, back-channel negotiations between 2012 and 2013 and signaled its intention to conduct public negotiations with the Rouhani regime through the P5+1 negotiators. Between November 2013 – the conclusion of the Joint Plan of Action (JPOA) – and July 2015, when the JCPOA was finalized, the White House de-escalated the sanctions pressure by blocking new congressional legislation and providing limited sanctions relief.[53] As a result of the sanctions relief under the JCPOA, the Iranian economy stabilized and is now on a path to recovery and modest growth.[54] The Obama administration also backed down on its commitments to vigorously enforce non-nuclear sanctions to respond to Iran's continued ballistic missile tests, weapons shipments to Syria and Yemen, the taking of American hostages, aggressive action against U.S. naval ships in the Gulf, an increase in repression of Iranian citizens, and the transfer to Iran of the Russian S-300 air defense system, the sale of which violates U.S. law. Remaining sanctions pressure that might have persuaded Iran to alter its non-nuclear related illicit activities and that was fully consistent with the JCPOA has been significantly weakened.

Although market forces will take time to react to reinvigorated sanctions, the Trump administration can begin to change the direction of U.S. policy by imposing sanctions on IRGC entities that have previously escaped designations. Such designations would rightly target entities that are engaged in illicit activities.

Despite the IRGC's pervasive role in the Iranian economy,[55] very few companies have been sanctioned for their connection to the IRGC (Treasury has only sanctioned 25 companies, 25 individuals, and two academic institutions controlled by the IRGC, despite thousands of potential designation targets).

In the case of the Iran sanctions program, the new administration should take two steps. First, the Trump administration could immediately extend U.S. secondary sanctions to apply to foreign companies doing business with entities that are owned or controlled by the IRGC, even when they are not specifically listed on the SDN list. Many assume that majority IRGC-owned companies are already covered by U.S. secondary sanctions, but that is not the case. Under current U.S. law, foreign companies may be able to do business with many IRGC-owned entities without fear of running afoul of U.S. secondary sanctions, as the so-called "OFAC 50% rule" may not apply under remaining provisions of U.S. law that allow for the imposition of secondary sanctions. Rather, the remaining secondary

51. Iran Threat Reduction and Syria Human Rights Act of 2012, Pub. L. 112-158, 126 Stat. 1214, codified as amended at 112 U.S.C. §504. (https://www.treasury.gov/resource-center/sanctions/Documents/hr_1905_pl_112_158.pdf); Kenneth Katzman, "Iran Sanctions," *Congressional Research Service*, May 7, 2014, page 20. (http://fas.org/sgp/crs/mideast/RS20871.pdf)
52. Mark Dubowitz, Annie Fixler, and Rachel Ziemba, "Don't Buy the Spin: Iran is Getting Sanctions Relief," *Foundation for Defense of Democracies and Roubini Global Economics*, June 2016. (http://www.defenddemocracy.org/content/uploads/documents/Dont_Buy_The_Spin.pdf)
53. Mark Landler, "Senate Bill to Impose New Sanctions on Iran Spurs Veto Threat From White House," *The New York Times*, December 19, 2013. (http://www.nytimes.com/2013/12/20/world/middleeast/senate-bill-to-impose-new-sanctions-on-iran-spurs-veto-threat-from-white-house.html); International Monetary Fund, "IMF Survey: Iran Faces Multiple Challenges as Growth Prospects Brighten," January 20, 2016. (http://www.imf.org/external/pubs/ft/survey/so/2016/new012016a.htm)
54. Mark Dubowitz, Annie Fixler, and Rachel Ziemba, "Don't Buy the Spin: Iran is Getting Economic Relief," *Foundation for Defense of Democracies and Roubini Global Economics*, June 2016. (http://www.defenddemocracy.org/content/uploads/documents/Dont_Buy_The_Spin.pdf)
55. Emanuele Ottolenghi, Saeed Ghasseminejad, Annie Fixler, and Amir Toumaj, "How the Nuclear Deal Enriches Iran's Revolutionary Guard Corps," *Foundation for Defense of Democracies*, October 2016. (http://www.defenddemocracy.org/content/uploads/documents/IRGC_Report.pdf)

sanctions appear to apply only to agents and affiliates of the IRGC, which likely must be specifically demarcated by U.S. authorities. Closing this "IRGC Gap" could easily be done with an executive order or legislation.

Second, the Trump administration could lower the "shadow SDN" designation threshold from 50 percent majority ownership to 25 percent beneficial ownership, and designate all entities it knows to be controlled by the IRGC. The new administration could also support congressional efforts to designate sectors of the Iranian economy as "sectors of IRGC influence" and establish an "IRGC Watchlist" of entities with a significant IRGC presence but which do not meet the ownership threshold for designation.

While the JCPOA only addressed Iran's illicit nuclear activities, the agreement lifted U.S. sanctions on a number of entities sanctioned for other illicit activities. The new administration should order a review of these entities and make clear that if it finds evidence that these entities continue to engage in illicit activity, the United States will re-designate them. Key among these entities are Bank Sepah (the "financial linchpin" of Iran's ballistic missile procurement network),[56] Bank Melli (which provided financial services to the IRGC),[57] EIKO (the Supreme Leader's business empire responsible for corruption and illicit finance),[58] and Iran Air (which reportedly continues to fly regular routes between IRGC bases and Syria).[59] Re-listing unreformed entities for non-nuclear illicit activities carries the risk that Iran and its commercial partners will denounce Washington for a breach of the JCPOA. The administration will need to explain to companies and foreign allies that these steps are consistent with a decade of U.S. policy and within Washington's rights and commitments under the accord, which is strictly limited to nuclear activities.

Engage international allies and foreign companies to build support:

Then: As Treasury underscored the rationale for escalating sanctions on Iran to the private sector, the State Department supported Treasury's efforts through a diplomatic push to explain the financial campaign. Working bilaterally and within the United Nations, the State Department sought to build international buy-in for broader sanctions. This coordination between Washington and its allies contrasted sharply with the confrontations about Iran between the United States and Europe in the 1990s, which culminated in a U.S. pledge not to enforce sanctions against European energy firms that violated U.S. law. These diplomatic efforts provided a foundation for UN Security Council resolutions, providing international backing for U.S. and European measures against Iran.

Now: As the Trump administration considers ways to counter Iran's malign activities, engagement with international partners and the private sector will be critical. In particular, Washington can use market forces to amplify the message that Iran continues to pose a significant risk to global trade and finance. The new administration could condition the environment to diminish transatlantic discord – for example, by educating foreign companies about the IRGC's role in the Iranian economy – before imposing sanctions.

As European companies begin to re-enter the Iranian market, there is a significant risk that they will unwittingly partner with IRGC-linked companies. The new administration also should examine pending

56. U.S. Department of the Treasury, Press Release, "Iran's Bank Sepah Designated by Treasury Sepah Facilitating Iran's Weapons Program," January 1, 2009. (https://www.treasury.gov/press-center/press-releases/Pages/hp219.aspx)
57. U.S. Department of the Treasury, Press Release, "Fact Sheet: Designation of Iranian Entities and Individuals for Proliferation Activities and Support for Terrorism," October 25, 2007. (https://www.treasury.gov/press-center/press-releases/Pages/hp644.aspx)
58. U.S. Department of the Treasury, Press Release, "Treasury Targets Assets of Iranian Leadership," June 4, 2013. (https://www.treasury.gov/press-center/press-releases/Pages/jl1968.aspx)
59. Emanuele Ottolenghi, "Iran Air participates in Syrian airlift, but Obama does nothing," *The Hill*, September 16, 2016. (http://thehill.com/blogs/pundits-blog/international/296303-iran-air-participates-in-syrian-airlift-but-obama-does)

deals to determine the best levers to persuade foreign companies to avoid deals with IRGC counterparties. While pressure from Washington may cause friction with key allies, the new administration should stress to foreign companies and banks that avoiding the IRGC is in their own best business interests.

As one example, the Trump administration should expand efforts to block Mahan Air's flights to Europe, Gulf countries, and Asia. Despite existing terrorism-related sanctions against the airline, Mahan Air has expanded its routes over the past years while continuing to transport weapons on behalf of the IRGC to Lebanese Hezbollah in violation of UN Security Council Resolutions 1701 and 2231.[60] The Trump administration should consider using secondary sanctions targeting ticketing agents and ground service providers, as well as banks facilitating any of Mahan Air's payments for airport services. Likewise, the administration should order an investigation into whether Iran Air has violated a range of sanctions, including those prohibiting the transfer of conventional weapons, and support for the Assad regime, the IRGC, and Hezbollah. This may have a chilling effect on Iran Air's international activities and on pending aircraft sales.

Be clear about the purpose of employing and unwinding sanctions:

Then: As Iran sanctions were escalating, Treasury officials explained that the purpose of these measures was to "protect the integrity of the U.S. and international financial systems" from illicit activities.[61] However, after the nuclear agreement, Obama administration officials argued that the purpose of sanctions had been to convince Tehran to reach a negotiated agreement over its nuclear program. Officials explained that Washington must be prepared to lift sanctions when rogue actors change their behavior,[62] and yet the Obama administration lifted sanctions before Iran addressed the underlying behavior that prompted many of the sanctions in the first place. This disconnect between Treasury officials, on the one hand, and White House and State officials, on the other, explains the reluctance of global banks to re-enter Iran, Iran still poses significant financial crimes risks.[63]

Now: The Trump administration should re-articulate the purpose of its sanctions against Iran, focusing on the full range of its illicit conduct. In particular, the new administration should draw attention to Iran's actions that have violated the JCPOA.[64] While the Obama administration minimized these violations, the new administration could make clear that it will publicize and punish all incidents that violate the JCPOA, including sanctioning all entities involved in the violation and invoking Article 37 of the JCPOA to re-impose previous sanctions.

The United States and its partners should remain focused on protecting the international financial system from continued illicit Iranian conduct. These risks are real and well understood by the market; they need to be consistently reinforced by the new administration.

60. Dana Somberg, "Israel: Iran is smuggling weapons to Hezbollah on commercial flights," *The Jerusalem Post* (Israel), November 22, 2016. (http://www.jpost.com/Middle-East/Iran-News/Israel-Iran-is-smuggling-weapons-to-Hezbollah-on-commercial-flights-473344)
61. David Cohen, "The Law and Policy of Iran Sanctions," *Remarks before the New York University School of Law*, September 12, 2012. (http://www.treasury.gov/press-center/press-releases/Pages/tg1706.aspx)
62. Jacob Lew, "The Evolution of Sanctions and Lessons for the Future," *Remarks before the Carnegie Endowment for International Peace*, March 30, 2016. (https://www.treasury.gov/press-center/press-releases/Pages/jl0398.aspx)
63. Eric Lorber, "The Implications of U.S. Aircraft Sales to Iran," *Testimony before the House Committee on Financial Services, Subcommittee on Monetary Policy and Trade*, July 7, 2016. (http://financialservices.house.gov/uploadedfiles/hhrg-114-ba19-wstate-elorber-20160707.pdf)
64. David Albright and Andrea Stricker, "Analysis of the IAEA's Fourth Iran Deal Report: Time of Change," *The Institute for Science and International Security*, November 15, 2016. (http://isis-online.org/uploads/isis-reports/documents/Analysis_of_IAEA_Fourth_JCPOA_Report_15Nov2016_Final.pdf)

Defensive Economic Approaches

As the United States has sharpened its tools of economic coercion in recent years, other countries and groups have taken notice and have begun developing similar ways to employ economic pressure, often threatening U.S. interests. The United States and its allies must develop strategies to counter these developments and protect itself and its allies.

Adversaries' Use of Offensive Tools

Economic Sanctions

Over the past few years, U.S. adversaries and allies have stolen a page from the United States' sanctions playbook. In response to Turkey's downing of a Russian military aircraft in Turkish airspace in December 2015, Russia imposed a number of economic sanctions designed to hurt key sectors of Turkey's economy.[65]

Like the United States, certain foreign countries have also begun using economic pressure that goes beyond simple asset freezes and embargoes. For example, to pressure regional neighbors, China has used regulations and purchasing decisions, refused to import certain goods, and limited exports of strategic materials to the markets of its adversaries. In response to recent U.S. threats to impose economic sanctions on Chinese individuals and entities for cyber attacks, Beijing was reportedly prepared to impose new banking sector regulations that prohibit U.S. firms from using non-Chinese technology that would encumber U.S. companies in the country.[66]

China has also used economic pressure more overtly, wielding economic sanctions in response to a variety of maritime disputes.[67] For example, during a dispute over the Senkaku/Diaoyu Islands with Japan, China cut quotas for the export of rare earth minerals to Japan.[68] Similarly, Beijing quarantined imports of tropical fruits from the Philippines during a territorial spat in 2012.[69] China has typically maintained that its actions are unrelated to maritime or territorial disputes, but they

65. Andrew Roth, "Putin signs sweeping economic sanctions against Turkey," *The Washington Post*, November 28, 2015. (https://www.washingtonpost.com/world/putin-signs-sweeping-economic-sanctions-against-turkey/2015/11/28/f3f5fff4-9603-11e5-befa-99ceebcbb272_story.html)

66. Cory Bennett, "Obama cyber sanctions could spur Chinese backlash," *The Hill*, Sept. 15, 2015. (http://thehill.com/policy/cybersecurity/253713-obama-cyber-sanctions-could-spur-chinese-backlash)

67. James Reilly, "China's Unilateral Sanctions," *The Washington Quarterly*, Fall 2010, pages 121-133. (http://www.tandfonline.com/doi/abs/10.1080/0163660X.2012.726428?needAccess=true&journalCode=rwaq20)

68. Keith Bradsher, "Amid Tension, China Blocks Vital Exports to Japan," *The New York Times*, September 22, 2010. (http://www.nytimes.com/2010/09/23/business/global/23rare.html)

69. Andrew Higgins, "In Philippines, Banana Growers Feel Effect of South China Sea Dispute," *The Washington Post*, June 10, 2012. (https://www.washingtonpost.com/world/asia_pacific/in-philippines-banana-growers-feel-effect-of-south-china-sea-dispute/2012/06/10/gJQA47WVTV_story.html)

exhibit all the characteristics of state-directed economic coercion.[70]

In addition, China has threatened to use secondary sanctions against U.S. companies, similar to those employed by the United States against Iran from 2010-2015. In response to the announcement of a significant arms sale by the United States to Taiwan, China threatened that any U.S. defense firm associated with the deal would lose access to Chinese markets and to the Chinese supply chain.[71]

The Boycott, Divestment, and Sanctions Movement

Non-state actors are also becoming increasingly adept at using economic coercion to achieve political objectives. The Boycott, Divestment, and Sanctions (BDS) movement against Israel exemplifies the damage that non-state entities can inflict upon an American ally with economic warfare. BDS is an international campaign that uses political pressure to discourage investment in Israel. Businesses, NGOs, universities, and sovereign wealth funds have joined the campaign.[72]

Pressure from the BDS movement includes:

- In September 2009, Norwegian Finance Minister Kristin Halvorsen announced that the Norwegian State Pension Fund would divest $5.4 million in shares from Elbit, an Israeli defense electronics firm;[73]
- In May 2011, German railway company Deutsche Bahn pulled $550 million in investment on a train line connecting Jerusalem to Tel Aviv;[74] and
- In February 2006, the Church of England voted to divest from companies operating in the West Bank, including a £2.5 million investment in the U.S. construction company Caterpillar.[75]

This movement provides crucial lessons for U.S. policymakers. First, the fact that a loosely organized non-state movement can directly induce the divestment of millions of dollars shows the damage adversaries can cause through targeted campaigns. Second, divestment by a major company such as Deutsche Bahn will create international headlines even if it does not lead to immediate harm. Third, divestment by a state entity such as Norway's sovereign wealth fund might serve as a harbinger for the U.S. and other allied countries. Over time, the United States will need to consider how allied states wield their investments in its economic defense strategy.

Cyber-Enabled Economic Warfare

In the 21st century, technology that can cause widespread economic damage is available to state and non-state actors alike. This is spurring the rapid evolution of cyber-enabled economic warfare, a new form of economic warfare not well understood by decision makers.

---

70. "China denies banning rare earths exports to Japan," *Reuters*, September 23, 2010. (http://www.reuters.com/article/us-china-japan-minerals-idUKTRE68M0PF20100923); "Palace exec: PHL moving on from banana row with China," *GMA News*, May 27, 2012. (http://www.gmanetwork.com/news/story/259576/money/economy/palace-exec-phl-moving-on-from-banana-row-with-china)

71. "China threatens sanctions against U.S. companies: Is this the future?" *Reuters*, January 27, 2016. (http://www.reuters.com/article/harrell-china-idUSL2N15B28B)

72. Mark Dubowitz, "Impact of the Boycott, Divestment, and Sanctions Movement," *Testimony before the Committee on Oversight and Government Reform, Subcommittee on National Security*, July 28, 2015. (https://oversight.house.gov/wp-content/uploads/2015/07/7-28-2015-Natl-Security-Hearing-on-BDS-Dubowitz-FDD-Testimony.pdf)

73. Adri Nieuwhof, "Scandinavian financial institutions drop Elbit due to BDS pressure," *The Electronic Intifada*, February 19, 2010. (https://electronicintifada.net/content/scandinavian-financial-institutions-drop-elbit-due-bds-pressure/8685)

74. Nora Barrows-Friedman, "BDS VICTORY: German company pulls out of illegal Israeli railway project," *The Electronic Intifada*, May 10, 2011. (https://electronicintifada.net/blogs/nora-barrows-friedman/bds-victory-german-company-pulls-out-illegal-israeli-railway-project)

75. "Church of England votes to divest from Caterpillar," *The Electronic Intifada*, February 6, 2006. (https://electronicintifada.net/content/church-england-votes-divest-caterpillar/5867); For a more extensive list, see Mark Dubowitz, "Impact of the Boycott, Divestment, and Sanctions Movement," *Testimony before the Committee on Oversight and Government Reform, Subcommittee on National Security*, July 28, 2015. (https://oversight.house.gov/wp-content/uploads/2015/07/7-28-2015-Natl-Security-Hearing-on-BDS-Dubowitz-FDD-Testimony.pdf)

Examples of malicious cyber-enabled actions against economic targets include cyber crime (such as cyber fraud against banking and payment platforms),[76] cyber espionage (like stealing trade secrets and intellectual property or U.S. government personnel information),[77] cyber sabotage (including the Iranian malware attack on Saudi Aramco in 2012 and against Saudi energy assets in 2016),[78] and cyber terrorism (like jihadists' alleged theft of data from retail companies to identify military-affiliated U.S. citizens).[79] The United States needs to better understand these incidents to determine if they are isolated or rather coordinated acts of cyber-enabled economic warfare designed to weaken the U.S. economy and thereby reduce U.S. political and military power.[80]

For example, in October 2014, JPMorgan Chase & Co., the largest American bank by assets, announced that a cyber attack had compromised the accounts of 76 million households and seven million small businesses. The attack – which began in June and likely originated in Russia – went unnoticed for two months. Hackers gained access to the bank's servers containing the names, email addresses, phone numbers, and addresses of both current and former customers. The same group of overseas hackers appears to have attempted to infiltrate at least twelve other financial institutions, including Fidelity Investments.[81] When briefed by national security officials on the ongoing JPMorgan breach, President Obama reportedly asked his team whether this could be Putin's retaliation for Western sanctions. The U.S. government could not provide a definitive answer.[82]

Other U.S. adversaries are also relying on cyber tools to target U.S. interests. In September 2012, a Middle Eastern hacker group identifying itself as Izz ad-Din al-Qassam Cyber Fighters conducted a massive denial-of-service attack against JPMorgan Chase, Citigroup, PNC Bank, Wells Fargo, U.S. Bancorp, and Bank of America.[83] By launching a heightened attack to overload the banks' websites with fake traffic, the group was temporarily able to suspend access to checking accounts, mortgages, and other bank services. Troublingly, the mysterious group warned these financial institutions that an attack was imminent, but the banks proved unable to stop it.

Though Izz ad-Din al-Qassam is also the name of the military wing of Hamas, Senator Joseph Lieberman, then-chairman of the Homeland Security Committee, asserted that the attacks were connected to the Iranian Islamic Revolutionary Guard Corps' external arm, the Quds Force.[84]

Similarly, North Korea also engages in cyber-enabled economic warfare. For example, the March 2013 "Dark Seoul" attacks, believed to have originated from the country, targeted South Korean ATMs, mobile

76. Nicole Perlroth and Michael Corkery, "North Korea Linked to Digital Attacks on Global Banks," *The New York Times*, May 26, 2016. (http://www.nytimes.com/2016/05/27/business/dealbook/north-korea-linked-to-digital-thefts-from-global-banks.html)
77. Josh Rogin, "NSA Chief: Cybercrime constitutes the 'greatest transfer of wealth in history,'" *Foreign Policy*, July 9, 2012. (http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/)
78. Jose Pagliery, "The inside story of the biggest hack in history," *CNN*, August 5, 2015. (http://money.cnn.com/2015/08/05/technology/aramco-hack/)
79. Lauren C. Williams, "ISIS Releases Military Personnel Addresses, Calls for Attacks," *ThinkProgress*, March 23, 2015. (https://thinkprogress.org/isis-releases-military-personnel-addresses-calls-for-attacks-b77b9c81bcf6#.r7tm8mcbs)
80. Samantha Ravich, "Cyber Enabled Economic Warfare: An Evolving Challenge (Vol. 2)," *The Hudson Institute*, November 2015, page 29. (https://s3.amazonaws.com/media.hudson.org/files/publications/20151117RavichCyberEnabledEconomicWarfareAnEvolvingChallengeVol2.pdf)
81. Juan Zarate, "The Cyber Financial Wars on the Horizon: The Convergence of Financial and Cyber Warfare and the Need for a 21st Century National Security Response," *Foundation for Defense of Democracies*, July 2015, page 4. (http://www.defenddemocracy.org/content/uploads/publications/Cyber_Financial_Wars.pdf)
82. Ibid, page 4.
83. Ibid, page 10.
84. E. Scott Reckard, Andrew Tangel and Jim Puzzanghera, "Banks fail to repel cyber threat," *Los Angeles Times*, September 27, 2012. (http://articles.latimes.com/2012/sep/27/business/la-fi-bank-attacks-20120927)

payment platforms, and bank servers.[85] North Korea often uses cyber capabilities to steal money for state income; the purpose of Dark Seoul was simply to send a message about Pyongyang's ability to inflict damage upon its southern neighbor.

Likewise, Chinese firms and state-owned enterprises have engaged in cyber espionage to steal critical data and technology, including commercial and military technology. These actions have helped bolster Chinese economic competitiveness and limit the qualitative military advantage enjoyed by the United States.[86] In many cases, Chinese actors have used cyber intrusions to pilfer information and convey it to government and commercial actors.[87] This has undermined U.S. firms' commercial viability, both within the Chinese market and in the broader global market.[88]

Chinese hacker units and state-owned enterprises have also formed strategic partnerships to manipulate Western firms' revenue data, reduce their value, and consequently purchase those companies and access important technology or remove major competitors – often producers of key military and technological goods and services – from the market.[89] The fields of biotechnology, communications, finance, energy, agriculture, and real estate have all been targeted.[90]

Strategic Investment

Adversaries – particularly China – have grown adept at strategically investing in U.S. and allied countries' industries in ways that allow them to procure advanced defense-related technology and deny the U.S. military access to key materials and territory. This strategy has also enabled China to threaten coercive economic pressure in times of conflict.

For example, China has been actively investing in Silicon Valley high-tech startup firms, both for economic gain and to exploit these companies' defense technologies.[91] Such strategic investment to acquire technology is part of a larger Chinese attempt to use its economic clout to gain competitive advantages.

Likewise, China is using strategic investments in attempt to block American power in the Western Pacific. Chinese investments in locations critical to U.S. military basing potentially limit U.S. freedom of access in the Pacific. Examples include large hotel and casino projects in Tinian and Saipan that are unlikely to be economically viable, but may curry favor with

85. Choe Sang-Hun, "Computer Networks in South Korea are Paralyzed in Cyberattacks," *The New York Times*, March 20, 2013. (http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html)
86. William C. Hannas, James Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization*, (New York: Routledge, 2013).
87. "Red Line Drawn: China Recalculates Its Use of Cyber Espionage," *Fireeye iSight Intelligence*, June 2016. (https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf)
88. Commission on the Theft of American Intellectual Property, *The IP Commission Report*, (Seattle, WA: National Bureau of Asian Research, May 2013). (http://ipcommission.org/report/IP_Commission_Report_052213.pdf)
89. U.S. House of Representatives, "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," October 8, 2012. (https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf)
90. Keith Bradsher, "Political Backlash Grows in Washington to Chinese Takeovers," *The New York Times*, February 16, 2016. (http://www.nytimes.com/2016/02/18/business/dealbook/china-fairchild-semiconductor-bid-rejected.html); Isabella Steger, "CNOOC's Unocal Lessons," *The Wall Street Journal*, July 23, 2012. (http://blogs.wsj.com/deals/2012/07/23/cnoocs-unocal-lessons/)
91. Elizabeth Dwoskin, "China is flooding Silicon Valley with cash. Here's what can go wrong," *The Washington Post*, August 6, 2016. (https://www.washingtonpost.com/business/economy/new-wave-of-chinese-start-up-investments-comes-with-complications/2016/08/05/2051db0e-505d-11e6-aa14-e0c1087f7583_story.html)

local governments and populations and consequently prevent U.S. military bases and training ranges from being developed for use in a contingency.[92]

In addition, Chinese investments in other locations – from the port of Darwin in Australia to military facilities in the continental United States – have drawn the attention of security experts.[93] In one example, Australia recently blocked a Chinese state-owned enterprise's attempt to purchase a majority share in Ausgrid, the Australian state-owned power grid.[94] The Australian government, when reviewing the sale, concluded that in the event of a conflict, Chinese ownership of critical infrastructure could seriously undermine Australia's national security.[95] Another example is when the Chinese-owned Ralls Corporation attempted to acquire of a facility located next to a U.S. naval weapons systems training facility in Oregon.[96]

In the Chinese strategic investment model, economic power and reach are enmeshed directly and intentionally with geopolitical influence and national security strength. This model also draws upon the resource pool and investment reach of sovereign wealth funds. Chinese sovereign wealth fund investment was worth $200 billion in 2007, and the Chinese government could add liquidity to the fund at any time and without constraint. Similar investment parastatals (quasi-state entities) have converted national resource wealth into national investment strategies.

Shoring Up Our Defenses

While the United States has amassed its own tools of economic coercion, our adversaries are now also using a wide range of powerful economic levers to threaten U.S. interests. The United States needs to develop capabilities and strategies to blunt the effectiveness of adversaries' economic coercion.

Defenses Against Economic Sanctions

If adversaries threaten U.S. companies with denying access to their markets, the United States should be prepared to impose reciprocal punishment, which will serve as a powerful deterrent. Likewise, the United States should be prepared to assist its allies if they are threatened with sanctions. For example, if Beijing attempts to use economic coercion against Japan or the Philippines in the East and South China Seas, the U.S. should provide these countries with or facilitate access to key materials that China has cut off, such as rare earth minerals. The United States could also incentivize the diversification of export/import markets to decrease dependence on Chinese materials. In addition, Washington should consider economic sanctions against China for its actions.

Specific policies to accomplish this might include tax breaks to export key materials to Japan, or deregulation on some export materials. Likewise, if China bans imports of some agricultural products from neighboring countries, the United States can

92. Farah Master, "HK-listed Imperial Pacific to invest $7 bln in Saipan casino complex," *Reuters*, September 25, 2014. (http://www.reuters.com/article/gambling-imperial-pac-saipan-idUSL2N0RQ0IK20140925); Michael Cole, "New Wave of Chinese Real Estate Investment Pushing $1.2b Casino in the South Pacific," *Mingtiandi* (China), May 26, 2015. (http://www.mingtiandi.com/real-estate/outbound-investment/new-wave-of-chinese-real-estate-investment-pushing-1-2b-casino-in-the-south-pacific/)

93. Amos Aikman, "Chinese Deal to Run Darwin Port 'Clear as Mud,'" *The Australian* (Australia), March 2, 2016. (http://www.theaustralian.com.au/national-affairs/foreign-affairs/chinese-deal-to-run-darwin-port-clear-as-mud/news-story/4099355aaf3c505ad638d29d9a5b743f); "Land grabs raise security issues," *Japan Times* (Japan), April 23, 2012. (http://www.japantimes.co.jp/opinion/2012/04/23/commentary/world-commentary/land-grabs-raise-security-issues/)

94. Perry Williams, "Australia Blocks Bid for Ausgrid, Triggering Warning from China," *Bloomberg*, August 19, 2016. (http://www.bloomberg.com/news/articles/2016-08-19/australia-bars-foreign-investors-from-buying-50-4-of-ausgrid-is1gmaue)

95. Treasurer of the Commonwealth of Australia Hon. Scott Morrison MP, Media Release, "Foreign investment applications for the 99-year lease of Ausgrid," August 11, 2016. (http://sjm.ministers.treasury.gov.au/media-release/067-2016/)

96. Stephen Dockery, "Chinese Wind Company Settles with U.S. in CFIUS," *The Wall Street Journal*, October 9, 2015. (http://blogs.wsj.com/riskandcompliance/2015/10/09/chinese-wind-company-settles-with-u-s-in-cfius-battle/)

pledge to buy previously banned imports or provide tax incentives for U.S. companies to import from these countries.

More broadly, the United States should prepare to deter Chinese adventurism in the South and East China Seas. It should limit China's willingness to use economic and military pressure against U.S. allies by threatening to impose sanctions on Chinese companies engaged in such activity. One option might be legislation such as Senator Marco Rubio's recently proposed bill threatening asset freezes and secondary sanctions on Chinese companies engaged in developing Beijing's military build up and aggressive activities in the South and East China Seas.[97]

Defenses Against BDS

The United States has already started to defend Israel against the BDS movement, but more can be done. Congress should expand upon the anti-BDS amendment included in the Trade Act of 2015 under the Trade Promotion Authority. The amendment discourages BDS measures by requiring U.S. trade negotiators to make rejection of BDS a "principal trade objective" in the Transatlantic Trade and Investment Partnership (TTIP) negotiations with the European Union. More federal legislation could be crafted to defend against economic and financial warfare, including by prohibiting transactions broadly with companies (both U.S. and foreign) that participate in BDS activities against U.S. allies.[98]

In addition, Congress and the administration could work to strengthen the Office of Anti-Boycott Compliance in the Bureau of Industry and Security at the Department of Commerce as a way to ensure U.S. and foreign companies do not participate in the BDS movement.

Congress could also consider further steps to encourage similar work being done at the state level, including by working with state legislatures to craft regulatory anti-BDS language and passing resolutions expressing support for such efforts.

Defenses Against Cyber-Enabled Economic Warfare

To date, the United States' response to cyber-enabled economic warfare has been undercut by the lack of cooperation and coordination between relevant government agencies and the private sector, in particular the financial industry. The key players in government, industry, and academia have not put the pieces together. To be sure, considerable resources are expended in all three sectors to studying cyber attacks, U.S. vulnerabilities, and cyber threats posed by major threat actors. To date, however, little of this work adequately addresses the dynamics of cyber-enabled economic warfare. As a result, the government's ability to effectively combat this threat is limited.

In contrast, the private sector has begun coordinating responses to cyber attacks. For example, the Information Sharing and Analysis Centers (ISAC's) fora have served as important venues for information sharing, and they have gained momentum in the financial services and technology industries. The Financial Services Information Sharing and Analysis Center (or FS-ISAC) is the first widespread not-for-profit intelligence service designed to assist with cyber defense and analysis, and has recently attracted extra funding from twelve large companies – including those in the financial, energy, transport, and healthcare sectors.[99]

Congress could further empower the private sector by creating a 21st century cyber-privateering regime that

97. Emily Tamkin, "Rubio Calls for Sanctions on Beijing for South China Sea Antics," *Foreign Policy*, December 7, 2016. (http://foreignpolicy.com/2016/12/07/rubio-calls-for-sanctions-on-beijing-for-south-china-sea-antics/)
98. Mark Dubowitz, "Impact of the Boycott, Divestment, and Sanctions Movement," *Testimony before the Committee on Oversight and Government Reform, Subcommittee on National Security*, July 28, 2015. (https://oversight.house.gov/wp-content/uploads/2015/07/7-28-2015-Natl-Security-Hearing-on-BDS-Dubowitz-FDD-Testimony.pdf)
99. Hannah Kuchler, "U.S. Financial Industry Launches Platform to Thwart Cyberattacks," *Financial Times* (UK), Sept. 24, 2014. (http://www.ft.com/intl/cms/s/0/080092b2-437a-11e4-8a43-00144feabdc0.html?siteedition=intl#axzz3FOFcGxgh)

helps the business community defend itself in concert with government. This model could be based on the tradition of congressional issuance of "letters of marque and reprisal," as provided for explicitly in Article 1, Section 8 of the U.S. Constitution. Governments provided these letters to private merchant ships, granting them the authority and monetary incentive to attack enemy vessels and bring the cases before admiralty courts. In the age of piracy, this was a legitimate method of providing maritime security.[100]

New authorities, cyber forensic teams, and private litigants that protect U.S. systems should be considered. Those building cases against cyber hackers and state sponsors should be rewarded. Victims of attacks should be given the right to sue the perpetrators and those benefiting directly from cyber infiltrations, just as victims of terrorism are afforded the right to sue terrorists, state sponsors, and terrorist financiers and facilitators. Shareholders and companies should be given the right to sue as well. The United States government should also be prepared to work with litigants to declassify enough information to help advance key court cases as a means of punishment and deterring future attacks.

Moreover, the U.S. Department of Justice, Department of Homeland Security, and Department of the Treasury could create and issue special cyber warrants – another type of "letter of marque and reprisal" – to allow U.S. private-sector actors to engage in active defense or otherwise track and disrupt cyber attacks. The issuance of warrants by the government would allow for legal and diplomatic considerations before any preemptive or counter-attacks were approved.[101]

Likewise, the United States could work to establish a "cyber alliance" with our closest allies. To blunt our adversaries' activities, the United States could rely more on our allies' technological advancements, particularly those by Israel, Canada, Australia, and the UK. But beyond technology, the combined economic might of Western allies represents the comparative advantage for cyber-enabled economic war. Members of this alliance would have to commit to not engage in economic or financial warfare including boycotts, sanctions, and divestment against any other alliance member.

Fundamentally, the U.S. government needs a better understanding of the goals of its adversaries in order to craft strategies to counter them. Washington needs to stop looking at each individual attack in isolation. The problem is not primarily one of capabilities; it is a failure of policy and analysis. The U.S. government should therefore task the intelligence community with providing an in-depth study of the strategies, doctrines, and escalatory ladders of the primary state and non-state adversaries in cyber space.

Defenses Against Threatening Strategic Investment

The Committee on Foreign Investment in the United States (CFIUS), led by the Treasury Department and composed of sixteen government agencies that review foreign investments in U.S. companies to assess national security risks, is the primary mechanism to assess potentially threatening investments in U.S. companies, critical infrastructure, and technology. Yet CFIUS only reviews approximately 100-150 transactions each year, and usually only in circumstances where the relevant parties submit the transaction for CFIUS review.[102] As countries such as China increasingly view strategic investment as an important tool to achieve foreign policy objectives, the gap in investment review is concerning.

The United States must take concrete steps to limit investment that threatens U.S. national security. First, the United States could adjust the scope of CFIUS

100. Juan Zarate, "The Cyber Financial Wars on the Horizon: The Convergence of Financial and Cyber Warfare and the Need for a 21st Century National Security Response," *Foundation for Defense of Democracies*, July 2015, page 23. (http://www.defenddemocracy.org/content/uploads/publications/Cyber_Financial_Wars.pdf)

101. Ibid, page 24.

102. James K. Jackson, "The Committee on Foreign Investment in the United States (CFIUS)," *Congressional Research Service*, August 12, 2016. (https://www.fas.org/sgp/crs/natsec/RL33388.pdf)

review to impose a mandatory submission requirement for any transactions involving a list of sectors with high national security risks, Chinese or Russian state-owned enterprises, and enterprises closely linked with the Chinese or Russian governments. Likewise, the federal government – in addition to further developing its well-publicized public-private defense partnership Defense Innovation Unit-Experimental (DIUx)[103] – could create a CFIUS subcommittee focusing specifically on foreign investment into startups and high-tech that could pose national security risks in the medium- to long-term. Such a subcommittee would help blunt our adversaries' ability to invest in U.S. companies before they either obtain the developed technology or shutter U.S. companies that may be developing defense-related technologies important for the United States.

In addition, the United States government could expand the scope of the CFIUS review process to include foreign investment not traditionally reviewed for national security concerns. In its current form, CFIUS scrutinizes strategic sectors related to critical infrastructure and technology. The committee does not review investment deals related to broader national security concerns, such as those related to soft power like entertainment and media. Yet, Chinese attempts to acquire U.S. levers of soft power – particularly Hollywood film studios and production houses – have raised fears that new Chinese ownership, which is often directly linked to the Chinese Communist Party, will subtly censor the films that American studios produce. Several Hollywood productions backed by Chinese investment in recent years have edited content to reflect sensitivity toward how well China is portrayed.[104] To address these concerns, Congress can amend the CFIUS charter and update legislation to cover certain assets closely linked to U.S. public opinion and media sources.[105]

The United States should also work with like-minded countries – in particular the Five Eyes group, composed of the United States, Canada, Australia, New Zealand, and the United Kingdom – to share information about adversaries' strategic investments, strategies, and actions. Offensive strategic investment threatens many of these partners, and to the extent that the Five Eyes countries can work together, each may be able to make more informed decisions.

Likewise, the United States should use elements of its positive economic power, such as strategic investment through USAID, to counteract strategic investment by our adversaries in jurisdictions of national security interest, such as certain islands in the Western Pacific. Such efforts would not only blunt threatening strategic investment, but would also curry favor with local governments thanks to economic benefits to the local economy.

103. Cheryl Pellerin, "DoD's Silicon Valley Innovation Experiment Begins," *DoD News,* October 29, 2015. (http://www.defense.gov/News/Article/Article/626602/dods-silicon-valley-innovation-experiment-begins)
104. Edward Wong, "Chinese Purchases of U.S. Companies Have Some in Congress Raising Eyebrows," *The New York Times*, September 30, 2016. (http://www.nytimes.com/2016/10/01/world/asia/china-us-foreign-acquisition-dalian-wanda.html)
105. Richard Berman, "China's rising threat to Hollywood," *Politico*, October 4, 2016. (http://www.politico.com/agenda/story/2016/10/china-hollywood-movies-threat-000216#ixzz4M7IGhtpn)

Positive Economic Power

Positive economic power is the use of a nation's economic means to incentivize financial transparency, encourage economic growth, and create conditions conducive to trade, entrepreneurship, and income-generative activities, particularly in areas of strategic national security interest and regions considered high risk to the United States. While such power cannot solve all problems, targeted efforts can further U.S. foreign policy objectives by tackling illicit finance, corruption, and financial crime. More important, over the long term, the economic development such programs foster can enhance political stability, increase opportunities for U.S. corporate trade and investment, and heighten hope for the future, denying extremists the recruiting fuel of despair.

Positive economic power is an important U.S. foreign policy tool for advancing the principles of competitive markets, greater integration between foreign and U.S. companies, and facilitating the economic conditions that enhance stability and good will toward the U.S. These levers have an even greater impact on our national security when paired with coercive or defensive measures. For example, making it more difficult for illicit financiers to operate in weakly regulated jurisdictions while also designating them as sanctioned persons can greatly inhibit their ability to aid and abet corruption and terrorism.

The Dangers of Illicit Finance, Corruption, and Political and Economic Instability

The UN Office on Drugs and Crime estimates the amount of money laundered annually is 2-5 percent of global GDP, or up to $2 trillion.[106] Unfortunately, law enforcement and judicial authorities globally have managed to freeze or seize less than one percent of those proceeds, at best.[107] In 2013 alone, the value of money exported illegally from the developing world was estimated by Global Financial Integrity (GFI) at over $1 trillion per year.[108]

Such illicit flows undercut the viability of political and governmental institutions, for example, by siphoning off significant funds that could serve as tax bases to

106. United Nations Office on Drugs and Crime, "Money-Laundering and Globalization," accessed December 1, 2016. (https://www.unodc.org/unodc/en/money-laundering/globalization.html)

107. United Nations Office on Drugs and Crime, Press Release, "UNODC estimates that criminals may have laundered US$ 1.6 trillion in 2009," October 25, 2011. (https://www.unodc.org/unodc/en/press/releases/2011/October/unodc-estimates-that-criminals-may-have-laundered-usdollar-1.6-trillion-in-2009.html)

108. Dev Kar and Joseph Spanjers, "Illicit Financial Flows from Developing Countries: 2004-2013," *Global Financial Integrity*, December 2015. (http://www.gfintegrity.org/wp-content/uploads/2015/12/IFF-Update_2015-Final-1.pdf)

increase public services.[109] Illicit finance also funds militant organizations, proliferators, and arms dealers.

The lack of strong enough institutions to counter illicit financing has consequences. Rogue actors and terrorist groups can continue to fund their operations, both in direct terrorism-related activities but also, in the case of the Taliban, Hezbollah, the Islamic State, and Hamas, activities aimed at co-opting local populations. When terrorist and related organizations develop political offices within their jurisdictions – supported in part by illicit financing – this presents the United States with even greater challenges. Groups such as Hamas, Hezbollah, and others garner support from local populations by providing social services and filling a vacuum left by weak governments and private sectors.

While the international effort to counter illicit financing has made it more costly and riskier for terrorists, rogue states, and criminals to abuse the formal financial system, these efforts have also led to unintended consequences. In recent years, the strict regulatory and enforcement environment has led many financial institutions to vacate significant geographic areas and to stop conducting banking for large swaths of customers because the banks view the risks as too high.[110] "De-risking" has disproportionately impacted poorer nations[111] and lower-income households and communities.[112]

For example, in 2015, Bank of America and CitiGroup's Banamex closed branches on the U.S.-Mexican border and other individual accounts over concerns of money laundering.[113] Similarly, few international banks were willing to establish correspondent relationships in post-conflict Liberia, greatly hindering transactions necessary for economic growth. Many countries' banks throughout South America, the Caribbean, South and Southeast Asia, and Africa have experienced losses of correspondent banking relationships with U.S. and European financial institutions due to fear of uncontained risk and enforcement actions.

The consequence of de-risking has had a disproportionate impact in emerging and frontier markets – in particular those that rely on international remittances. As a result, many individuals in these areas cannot gain access to the formal financial sector. Even diaspora communities within the United States continue to struggle to gain sustainable formal financial sector access. Too often, the de-risked are forced to turn to alternative financial services (AFS) providers, such as payday lenders, check cashers, and pawn shops – many of whom do so at predatory rates that exacerbate economic risks. Individuals may also turn to militant groups, drug traffickers, and other illicit networks to conduct financial transactions.

Strategic Investments in Social Enterprises

Countering the threats posed by illicit actors requires a comprehensive approach not simply limited to punitive or defensive measures, but also one that provides alternative support mechanisms to at-risk communities.

One effective mechanism of positive economic power is so-called Impact Investments. Impact Investments are those that serve U.S. national security interests by deploying government or corporate capital in high-risk

109. Brigitte Unger and Elena Madalina Busuioc, *The Scale and Impacts of Money Laundering*, (UK: Edward Elgar Publishing Limited, 2007), page 110.
110. The World Bank Group, "Withdrawal from Correspondent Banking: Where, Why, and What to Do About It," November 2015. (http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2015/11/24/090224b083395501/3_0/Rendered/PDF/Withdraw0from000what0to0do0about0it.pdf)
111. Clay Lowery, "Unintended Consequences of Anti-Money Laundering Policies for Poor Countries," *Center for Global Development*, November 9, 2015. (http://www.cgdev.org/sites/default/files/CGD-WG-Report-Unintended-Consequences-AML-Policies-2015.pdf)
112. Bottom-of-the-pyramid or base-of-the-pyramid (BOP) refers to the poorest socio-economic segment of society, most often cited as earning $2/day or $3000/year or less in income. Estimates range from 25-40 billion of the world's population.
113. Lainer Saperstein and Geoffrey Sant, "Account Closed: How Bank 'De-Risking' Hurts Legitimate Customers," *The Wall Street Journal*, August 12, 2015. (http://www.wsj.com/articles/account-closed-how-bank-de-risking-hurts-legitimate-customers-1439419093)

or conflict zones to mitigate risks. Impact Investments deploy risk capital to address societal, environmental, or governance issues and do not sacrifice on financial return. These investments are meant to strengthen targeted communities and deliver positive economic returns to investors.

Targets of strategic investments that enhance security and open new markets include:

- **Basic human services** – water and sanitation, rural development and energy access, financial and capital access, and literacy. Communities with better access to basic human services are better equipped to withstand economic shocks.
- **Facilitating entrepreneurship.** Greater financial access combined with better business acumen leads to greater labor productivity.
- **Macro-level projects and investments.** This includes more efficient supply chains for rural agriculture, water, and energy products, or the provision of financial services and economic assets.
- **Critical infrastructure for transport.** This includes rails, ports, and highways to ensure the more efficient and secure flow of goods and services.
- **Access to technology.** Media outlets, social media, and mobile technology can build resiliency against propaganda and violent narratives.

Working closely with the U.S. investor community can encourage the adoption of new norms for transparency. For example, investors backing new projects to promote access to water and sanitation in African rural communities might insist that all bidders, operators, and contract awardees subscribe to certain transparency rules to protect their investment.

If targeted measures against illicit actors are undertaken in tandem with investments in legitimate, community-driven commercial enterprise in conflict zones, American security interests can be enhanced while constricting the operating environment for rogue actors.

Several existing U.S. initiatives in this field include: the White House Office of Social Innovation and Civic Participation,[114] the State Department and USAID's Global Development Lab,[115] and the Overseas Private Investment Corporation's Impact Investing initiatives.[116] These efforts underscore the importance of a strong and stable U.S. economy to its national security, and engaging the financial and commercial sectors to help advance U.S. interests.

The following are examples of where such Impact Investing has occurred:

Mortgage market in Ghana

In 2004, Ghana's mortgage market was still in its infancy. Most mortgage lenders were only within reach of a few rich people.[117] The government provided mortgages but was very ineffective. Then support from the International Finance Corporation, Dutch development bank FMO, and the U.S. Overseas Private Investment Corporation provided capital to mortgage banks in Ghana like HFC bank and Ghana Home Loans. These banks had mandates to serve the middle-income market (homes valued at less than $50,000), as well as higher income segments. Since this intervention, the industry has grown steadily. Mortgage debt outstanding as a percent of GDP grew

114. See White House Office of Social Innovation and Civic Participation, "Community Solutions Initiatives," accessed January 18, 2017. (https://www.whitehouse.gov/administration/eop/sicp/initiatives/community-solutions)
115. See U.S. Agency for International Development, "Entrepreneurship," November 3, 2016. (https://www.usaid.gov/GlobalDevLab/entrepreneurship)
116. The Overseas Private Investment Corporation's Impact Investing initiatives leverage public capital to stimulate and catalyze private capital to drive financially attractive commercial enterprise initiatives in overseas markets across sectors which address pressing development challenges that can be directly applicable in regions in which the U.S.'s punitive, sanctions, diplomatic and military tools are already being deployed.
117. Callistus Mahama, "The Mortgage Market in Ghana," *Mortgage Markets Worldwide*, Eds. Danny Ben-Shahar, Charles K Yui Leung, Seow Eng Ong, (UK: Blackwell Publishing Ltd, 2008).

from 2.5 percent in 2004 to 3.9 percent in 2006.[118] In addition, according to the World Bank's Doing Business Indicators, the time taken to register land in Ghana has fallen from 169 days in 2005 to 34 days in 2012,[119] making Ghana the easiest country to register property in sub-Saharan Africa. The growth of the mortgage market required and encouraged the development of a functional property registration system enforced by the government.

Health insurance in Nigeria

In Nigeria's Kwara state, the publicly funded Health Insurance Fund (HIF) subsidized the provision of prepaid health insurance to a group of low-income farmers through the Nigerian private health insurer Hygeia. Initially, in 2007, demand was low and the uptake and renewal rate of the insurance was limited to the people who were ill. However, as farmers learned more about its benefits, uptake increased. In 2013, the number of enrollees was close to 70,000 and the renewal rate had risen to 52 percent. The subsidy and associated impact triggered private sector investment in Hygeia, while HIF's resources were also used to upgrade medical and administrative capacity of the insurer and contracted providers. In February 2013, the state government and Hygeia signed a memorandum of understanding to expand the program to cover 600,000 people within the next five years.[120]

Managing De-Risking

De-risking is an increasing source of concern among regulatory and enforcement agencies worldwide. The ultimate goal is to ensure that underserved populations have access to financial services in a way that also limits illicit activity and economic and political instability. Regulators such as the Financial Conduct Authority in the United Kingdom and the Financial Crime Enforcement Network (FinCEN) in the United States have encouraged an alternative risk-based approach. FATF has also released guidance to a number of financial institutions on this issue.[121] And the Office of the Comptroller of the Currency may also produce de-risking guidance to mitigate the impact.

In the United States, we can and should do more to ensure that blunt de-risking does not threaten our ability to combat illicit financing. This should include better information sharing among banks, facilitated by regulatory reforms related to Section 314(b) of the USA PATRIOT Act, as well as other mechanisms designed to encourage banks to experiment with more effective forms of information transfer that limit the need to engage in blunt de-risking. Additionally, the use of emerging financial and regulatory technologies can serve to meet regulatory anti-money laundering and combating the financing of terrorism (AML/CFT) compliance goals to protect our financial system while creating a more secure and transparent environment for financial inclusion. Suggestions include:

- Big data analytics (transactions, communications, social media, etc.) can be leveraged for enhanced due diligence to track potential illicit finance, and for anti-fraud/anti-corruption efforts, credit history, economic tracking, and credit worthiness;

118. Nicholas Addai Boamah, "Housing Affordability in Ghana: A focus on Kumasi and Tamale," *Ethiopian Journal of Environmental Studies and Management*, 2010.
119. The World Bank and the International Finance Corporation, "Doing Business 2012: Doing business in a more transparent world," 2012, page 97. (http://www.doingbusiness.org/~/media/WBG/DoingBusiness/Documents/Annual-Reports/English/DB12-FullReport.pdf)
120. Emily Gustafsson-Wright and Onno Schellekens, "Achieving Universal Health Coverage in Nigeria One State at a Time," *Brookings Institution*, July 29, 2013. (https://www.brookings.edu/wp-content/uploads/2016/06/Achieving-Universal-Health-Coverage-in-Nigeria.pdf)
121. See Financial Action Task Force, "Risk-Based Approach for the Banking Sector," October 2014. (http://www.fatf-gafi.org/publications/fatfrecommendations/documents/risk-based-approach-banking-sector.html) and Financial Action Task Force, "Money or Value Transfer Services," February 2016. (http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-money-value-transfer-services.pdf); See also Financial Crimes Enforcement Network Director Jennifer Shasky Calvery, *Remarks at the 2014 Mid-Atlantic AML Conference in Washington, DC*, August 12, 2014. (https://www.fincen.gov/news/speeches/remarks-jennifer-shasky-calvery-director-financial-crimes-enforcement-network-10) and U.S. Department of the Treasury, Financial Crimes Enforcement Network, "Guidance and Advisory Issued on Banking Services for Money Services Businesses Operating in the United States," April 26, 2005. (https://www.fincen.gov/news_room/nr/pdf/20050426.pdf)

- Predictive analytics and artificial intelligence-based learning tools can drive financial access by better predicting areas of heightened risk and driving responsible financial activities;
- Digital identify programs can ensure that non-traditional bank customers and less-documented individuals transact in the system securely and transparently;
- Secure mobile payment and credit technologies allow for financial access in remote zones via mobile phones, while bringing greater transparency to global financial flows. Such efforts can be done securely through fiat currencies and digital/token-based transfers;
- More nimble middle- and back-office data-sharing capabilities within and between banks can facilitate more comprehensive screening of financial activities to highlight anomalies, detect illicit financial patterns, and capture additional touch-points within the financial transactions chain;
- Geospatial and biometrics can aid in customer verification and validation globally; and
- Engagement of community-based organizations (houses of worship, schools, community centers, and local non-profits), to better understand customer background and as a distribution channel for financial products and services, can lower overhead costs while enhancing customer knowledge for both due diligence and service needs.

Ensuring the Integrity of the Financial System

Since September 11, 2001, the United States has led the global campaign to counter the financing of terrorism and to increase the integrity and transparency of the international financial system. The ongoing global CFT campaign is now unquestionably a pillar of U.S. economic statecraft.

And yet, the CFT challenges facing the United States and the international financial system now are greater than ever. The rise of the Islamic State, the resiliency of al-Qaeda, and the expansion of Iran's terrorism activities directly or through its surrogates like Hezbollah demonstrate the ongoing urgency of the terrorist threat. While Washington and its allies have succeeded in restricting more overt forms of support to terrorist organizations, these and other groups have adjusted their methods.

Further, while the modern AML/CFT system is intended to deter, detect, and disrupt illicit financing, it cannot stop all illicit activity. Indeed, the current AML/CFT system is inefficient in how it prevents financial crimes and ineffective in protecting the financial system from illicit financing. Recent cases such as the Panama Papers and the 1MDB scandal in Malaysia – where senior government officials siphoned off $3.5 billion in state funds – make clear that a wide range of criminals, corrupt actors, and terrorist groups continue to abuse the international financial system.

The United States needs to address these challenges head on, both to ensure its success in the fight against terrorist financing and to tackle other activities such as kleptocracy and corruption, which threaten the integrity of the international financial system.[122]

Increasing Transparency and Accountability in the Financial System

The ultimate goal of the AML/CFT regime is to empower financial institutions to help government authorities guard the gates of the global financial system. Key to these efforts are the twin principles of transparency and accountability. Financial transparency is crucial to financial integrity because it allows authorities to identify, track, and trace the sources, conduits, and uses of terrorist financing that transit the financial system. Without financial transparency, financial institutions and regulators cannot identify risks ranging from financing al-Qaeda to brokering nuclear proliferation. Law enforcement cannot track progressively globalized criminal networks. States cannot identify stolen assets or proceeds of tax evasion. And financial pressure to address gross violations of international law by Iran, Syria, Russia,

122. For more information, see: Chip Poncy, Testimony before the House Financial Services Committee Task Force to Investigate Terrorism Financing, June 24, 2015. (http://www.defenddemocracy.org/content/uploads/documents/Poncy_Evaluating_Security_Of_US_Financial_Sector.pdf)

or others becomes a hollow talking point rather than an operational instrument of global security.

Accountability is crucial to financial integrity because it provides confidence that the rule of law is enforced across the financial system. Accountability drives financial integrity in two respects. First, accountability is needed to enforce requirements of, and responsibilities for, financial transparency across the financial system, including with respect to the customers, institutions, and ultimately the authorities that access, service, and govern the financial system. Second, accountability is needed to pursue, disrupt, punish, and deter those who abuse the financial system.

Designed with these principles in mind, the international AML/CFT regime has expanded to include a preventative web of sanctions and regulations to deny rogue actors access to commercial and financial facilities. This evolution has yielded an increasingly robust system, but one that has placed enormous stress on the financial community to meet the expanding definitions of financial crime, the complexities of sanctions regimes, and the heightened expectations of compliance.[123] The costs have been high. Billions of dollars of fines have been collectively levied against banks for failure to comply with legal requirements, and billions more have been invested in compliance systems.

Yet estimates suggest that well over a trillion dollars of illicit financing are raised and moved globally every year, fueling everything from arms and human trafficking to environmental crimes and kleptocracy.[124] Successful efforts to prevent illicit financing, uncover criminal networks, or trace rogue capital seem difficult and sporadic at best. Even with increased vigilance and more reporting of suspicious activity, the volume of illicit financing presents systemic challenges to AML/CFT regimes around the world.

The Panama Papers leak exposed the opacity in corporate formation, placement, and layering of money that facilitate financial crime and sanctions evasion.[125] The continued prosecutions of banks for failing to meet sanctions obligations underscore the fact that compliance culture has not met policy expectations. And global corruption investigations reveal the corrosive force of unbridled power, not to mention the exploitation of the world's seemingly most well-regulated banks.[126]

Such shortcomings are cause for concern on several levels. First, regulators will face serious challenges in rooting out corruption, sanctions evasion, and terrorism financing. Second, and as discussed in this report's "Positive Economic Power" chapter, corruption and money laundering threaten economic growth in critical jurisdictions. And to the extent that illicit financial activity creates political instability and extremism, the inability of the global financial system to root out such activities presents a national security risk.

Addressing Key Gaps in the AML/CFT System

To improve the integrity of the international financial system, the White House should take a number of steps.

First, it can support the Treasury Department's efforts to improve information sharing both among financial

123. Juan C. Zarate and Chip Poncy, "Designing a New AML System," *The Clearing House*, Q3 2016, pages 26-36. (https://www.theclearinghouse.org/-/media/tch/documents/research/banking%20perspectives/2016/q3/2016-q3-bp-issue-web.pdf?la=en)
124. Dev Kar and Joseph Spanjers, "Illicit Financial Flows from Developing Countries: 2004-2013," *Global Financial Integrity*, December 2015. (http://www.gfintegrity.org/wp-content/uploads/2015/12/IFF-Update_2015-Final-1.pdf)
125. "The Panama Papers: Politicians, Criminals, and the Rogue Industry that Hides Their Cash," *The International Consortium of Investigative Journalists*, accessed January 18, 2017. (https://panamapapers.icij.org/)
126. U.S. Department of Justice, Press Release, "United States Seeks to Recover More Than $1 Billion Obtained from Corruption Involving Malaysian Sovereign Wealth Fund," July 20, 2016. (https://www.justice.gov/opa/pr/united-states-seeks-recover-more-1-billion-obtained-corruption-involving-malaysian-sovereign); Complaint, *United States of America v. "The Wolf of Wall Street" Motion Picture*, No. CV 16-16-5362 (C.D. Cal. filed July 20, 2016). (https://www.justice.gov/opa/file/877166/download)

institutions and between the private sector and regulators, as well as to pursue greater accountability abroad. Such measures would include:

- **Support Treasury's contemplated extending of AML/CFT preventive measures to real estate agents.** The longstanding global vulnerability of the real estate industry to money laundering is well known. For this reason, FATF global standards direct countries to extend AML/CFT preventive measures to real estate agents. Several recent cases have indicated that this vulnerability continues to be exploited in the United States, most prominently in New York City and Miami. This move, coupled with Treasury's recent Geographic Targeting Order focusing on title insurance companies, is a positive step.[127]
- **Support Treasury's extension of AML/CFT preventive measures to investment advisers, consistent with FATF global standards.** As reported by Treasury in the 2015 National Money Laundering Risk Assessment, as of April 2015, investment advisers registered with the SEC reported more than $66 trillion assets under management. The current lack of AML/CFT regulation over this sector creates a blind spot, substantially undermining financial transparency in our capital markets. This gap also puts broker-dealers in the unfair position of trying to manage illicit financing risks of the investment adviser sector they service.
- **Expand the scope of Section 314(b) of the USA PATRIOT Act.** Section 314(b) of the USA PATRIOT Act is designed to facilitate greater insight into financial flows, patterns, and data. Increased visibility could significantly increase financial institutions' and regulators' abilities to track financial crime. Yet to date, Section 314(b) has primarily focused on transactional information sharing. Some initial efforts to expand Section 314(b) to network analysis are currently underway and appear to be generating encouraging results. Such efforts would have immediate impacts on the international financial community's ability to combat illicit activity.[128]
- **Raise the bar at Intergovernmental Organizations (IGOs).** The U.S. should push the UN Security Council for mandated reporting and penalties on states that do not implement required travel bans and asset freezes on rogue actors such as terrorist operatives under UNSCR 1267. For example, Qassem Soleimani, the commander of the IRGC's Quds Force, traveled repeatedly to Russia, Iraq, and possibly other jurisdictions in defiance of a UN travel ban.

Second, the administration can encourage congressional action to strengthen the integrity of the financial and business formation sectors. Legislation bolstering transparency and accountability in the financial-commercial system would include:

- **Requiring the disclosure and maintenance of meaningful beneficial ownership information in company formation processes.** In the United States, almost two million corporations and limited-liability companies are formed under the laws of the states each year. Yet few states obtain meaningful information about the beneficial owners of the

127. U.S. Department of the Treasury, Financial Crimes Enforcement Network, "FinCEN Expands Reach of Real Estate 'Geographic Targeting Orders' Beyond Manhattan and Miami," July 27, 2016. (https://www.fincen.gov/news/news-releases/fincen-expands-reach-real-estate-geographic-targeting-orders-beyond-manhattan)

128. For example, in recent years U.S. financial institutions have observed suspicious activity related to funnel accounts. Financial institutions can track those related accounts within their own systems, but once those funds hit outbound gateways, financial institutions face significant challenges in tracking the pathway of those funds. If financial institutions were more easily able to share information about these networks, they could better identify illicit activity such as drug trafficking and money laundering. Encouraging financial institutions to utilize Section 314(b) will require the government to offset the costs such mechanisms impose on banks. One of the primary deterrents to financial institutions taking advantage of 314(b) is the increased demands that regulators place on those banks collecting such information. The administration should take steps to offset such regulatory burdens and in turn encourage the collection of such valuable information.

corporations and the limited-liability companies formed under their laws. The lack of a requirement to understand the beneficial owners of corporations during the company formation process can help sanctions evaders, drug kingpins, and tax dodgers continue and expand their illicit activities. For example, Mossack Fonseca, the law firm at the heart of the Panama Papers scandal, relied on a dearth of beneficial ownership identification requirements in Panama to facilitate a wide range of illicit activity. This included: assisting sanctioned individuals linked to Syrian President Bashar al-Assad in funneling funds to Hezbollah;[129] assisting narcotics dealers in purchasing high-end real estate as a means to launder money;[130] and assisting U.S. persons in creating offshore shell companies to evade taxes.[131] Legislation requiring the collection of beneficial ownership information is necessary to address the abuse of legal entities to mask the identities and illicit financing activities of criminal actors.

Third, the administration can actively push for additional "protected" resources (i.e. dedicated resources) for entities engaged in strengthening the integrity of the financial system.

- **Treasury needs resources to enhance its targeting of primary money laundering concerns under Section 311 of the USA PATRIOT Act and targeting illicit financing networks under the International Emergency Economic Powers Act (IEEPA).** Such action is needed to give Treasury the resources to continue applying targeted financial measures against a growing range of criminal and national security threats. The clearly disruptive impact of financial crimes justifies additional resources that match Treasury's expanding role in combating threats to our financial integrity.
- **Treasury's Internal Revenue Service (IRS) and the Asset Forfeiture and Money Laundering Section of the Department of Justice require the capability to enhance financial investigations of illicit financing networks.** Such action is needed to strengthen the systematic pursuit of these networks by criminal investigative and prosecutorial authorities.

Longer Term Challenges to the AML/CFT System

The Trump administration should also begin addressing broader challenges to the AML/CFT system.

Structural Challenges

As designed, the current system is intended to support law enforcement in the investigation and prosecution of financial criminal cases, but not as a way to defend the entire financial system from abuse. Traditionally, law enforcement agencies viewed the financial system as a means to discover and obtain information on criminals.[132] AML/CFT reporting requirements are built on a "one-to-one" model, where each institution typically reports to an authority about singular customers and transactions. The stove-piping of information is intended to protect customer data. But this model does not create a dynamic flow of information between authorities and institutions within the private sector, or across borders. In short, there is no facility for real-time responses, dynamic feedback, or collective learning.

129. Will Fitzgibbon and Martha M. Hamilton, "Law Firm's Files Include Dozens of Companies and People Blacklisted by U.S. Authorities," *The International Consortium of Investigative Journalists*, April 4, 2016. (https://panamapapers.icij.org/20160404-sanctioned-blacklisted-offshore-clients.html)

130. Martha M. Hamilton, "Cartel-Linked Suspects Arrested After Panama Papers Revelations," *The International Consortium of Investigative Journalists*, April 25, 2016. (https://panamapapers.icij.org/20160425-cartel-arrests-uruguay.html)

131. Michael Hudson, Jake Bernstein, Ryan Chittum, Will Fitzgibbon, and Catherine Dunn, "Panama Papers Include Dozens of Americans Tied to Fraud and Financial Misconduct," *The International Consortium of Investigative Journalists*, May 9, 2016. (https://panamapapers.icij.org/20160509-american-fraudsters-offshore.html)

132. National Commission on Terrorist Attacks Upon the United States, "Chapter 4: Combating Terrorist Financing in the United States: The Role of Financial Institutions," *Monograph on Terrorist Financing*, August 21, 2004. (http://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Ch4.pdf)

As a result, each institution's visibility into illicit activity ends with its touch points with customers and transactions, and most authorities are unable to see systemic vulnerabilities across institutions in real time. Within institutions, information sharing between lines of business (such as corporate and retail) and compliance teams happens on a customer-by-customer basis. It is difficult for both the public and private sectors to monitor and respond to systemic vulnerabilities without expending prohibitive resources. And if the private sector proactively uncovers vulnerabilities, they are often "rewarded" with additional regulatory scrutiny.

Policy Challenges

The increased use and blending of sanctions and the AML/CFT system to exclude financial rogues and maximize financial transparency has created a series of escalating risks and policy challenges for the private sector. Regulators and policymakers within the United States, in other countries, and in international fora continue to demand that the financial community understand and manage its risk.[133]

These escalating risks are compounded by the real costs of catching up with financial transparency expectations now codified with Treasury's new customer due diligence (CDD) rule and the heightened global importance of understanding ultimate beneficial ownership.[134]

Technical Challenges

The mission of countering illicit finance also faces massive technical challenges. The 1980s analog model that was developed to understand, screen, and monitor customers and transactions has not kept pace with the volume, speed, and fluidity of data available in the 21st century. This has put a premium on creating more sophisticated compliance processes and tweaking the algorithms and models used to flag suspicious behavior. The refinement of these systems is limited, however, by unstructured or missing data, as well as a lack of connectivity between internal and external data sources. Even with attempts at technical patches and greater automation in the public and private sectors, the Suspicious Activity Report (SAR) processes often rely on manual reviews for many transactions, which often overburden financial institutions. The result is an almost impossible mission of fighting 21st century financial crimes using 20th century technologies.

Reforming the AML/CFT System

Experts and policymakers recognize that there needs to be a new cost-effective and sustainable model for managing compliance risk. New technologies are blazing the trail. Capabilities that allow organizations to collect, share, analyze, and protect mass amounts of data in real time and establish more reliable customer and transaction identification are the cornerstone for a new model.

Such a new system would involve participating institutions automatically sharing bulk customer and transaction information. Automated analytics would be applied to transactions to screen sanctioned and suspect parties and identify patterns of concern. Red flags would be provided to participating institutions, relevant authorities, and financial intelligence units (FIUs). Information could be anonymized to protect customer privacy, while transactions and reports would be provided to relevant parties in real time. This model could be applied on different platforms and involve different actors, in some cases with government, including FIUs, at the center. In others, a private

133. For example, see Financial Action Task Force, "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation," February 2012. (http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf)

134. Customer Due Diligence Requirements for Financial Institutions, U.S. Department of the Treasury, Financial Crimes Enforcement Network, 81 Federal Register 29398, May 11, 2016. (https://www.gpo.gov/fdsys/pkg/FR-2016-05-11/pdf/2016-10567.pdf)

sector actor or consortium could act as the trusted clearinghouse.

While much remains to be done to develop this revitalized AML/CFT system, the new administration should take steps to encourage new technologies, data aggregation mechanisms, platforms, and pilot programs that could help build confidence in this new system.

Innovative Technologies

New payment models and the financial technology market are transforming the way customers access financial services. Alternative payment providers are challenging banks' traditional dominance of the sector, and younger consumers and those outside of the traditional banking system are adopting a wider range of payment options.

The rise of digital ecosystems provides opportunities for innovation that could enhance financial efficiency. Many financial institutions are beginning to embrace the technology underlying the bitcoin cryptocurrency known as blockchain technology, which facilitates transactions through a public ledger distributed across multiple computer networks. Other banks are joining consortia to collaborate on exploring and leveraging distributed ledger technologies in the financial sector.

Financial institutions are envisioning distributed ledger technology as a secure way to record contracts, facilitate remittance payments, and revamp trade finance.[135] Technology giants are moving toward promoting the technology, and in May 2016, Microsoft announced that it had joined the Chamber of Digital Commerce, the world's largest trade association representing the digital asset and blockchain industry.[136] Although many current blockchain technology projects are isolated efforts, some of which are in the proof of concept stage, the movement to place asset and transaction information into distributed ledgers provides opportunities to more easily detect fraud, money laundering, and other criminal activity. The data captured and shared via blockchain allows for analysis well beyond the immediate transaction, thus offering targeted insights into global illicit financial streams.[137] If these new technologies are adopted widely within the financial system, the potential for identifying suspicious patterns and networks increases exponentially.

Aggressive Information-Sharing Structures

Emerging information-sharing platforms are optimizing how parties are sharing information and creating possibilities for more collaborative models. In the United Kingdom, for example, the Joint Money Laundering Intelligence Taskforce (JMLIT) links government agencies, law enforcement bodies, and 25 major UK and international banks. JMLIT's approach is based on a model of "collaboration, collective ownership and prioritization" to combat high-end money laundering.[138] The approach has worked well. Since 2015, JMLIT members have developed legal cases, identified and closed banks accounts, obtained 50 new court orders, and made numerous arrests. As a result, the UK government now plans to move JMLIT to a more permanent footing and expand its membership.[139]

135. For example, see "Here's What 8 Financial Institutions Are Doing to Save Billions on Currency Trades," *Reuters*, August 17, 2016. (http://fortune.com/tag/distributed-ledger-technology/)
136. Suzanne Choney, "Microsoft joins blockchain-focused Chamber of Digital Commerce," *Microsoft Blog*, May 4, 2016. (http://blogs.microsoft.com/firehose/2016/05/04/microsoft-joins-blockchain-focused-chamber-of-digital-commerce/#sm.0001bjtqdat2fee10kl1ce7o4aq4i)
137. Kristofer Readling and Justin Schardin, "Why Blockchain Could Bolster Anti-Money Laundering Efforts," *Bipartisan Policy Center*, June 2, 2016. (http://bipartisanpolicy.org/blog/blockchain-anti-money-laundering/)
138. "Public-private information sharing partnerships to tackle money laundering in the finance sector: The UK Experience," *Joint Money Laundering Intelligence Taskforce*, accessed January 18, 2017. (http://thecommonwealth.org/sites/default/files/inline/4%20UK%20approach%20to%20public-private%20partnerships.pdf)
139. City of London Police, "New taskforce brings together law enforcement, Government and the financial sector to crack down on fraud," February 10, 2016. (https://www.cityoflondon.police.uk/news-and-appeals/Pages/New-taskfirce-brings-together-law-enforcement.aspx)

The cyber domain is also providing an arena and models for greater collaboration. Major U.S. banks have recently announced efforts to collaborate to protect against cyber attacks, and FinCEN has recently required that certain banks also report cyber attacks.[140]

Screening Platforms

Common screening systems and platforms present a promising opportunity to consolidate compliance risk management and to share the risks associated with illicit finance.

In Mexico, the Central Bank has established the Banco de México's Domestic USD Transfer System (SPID), an electronic domestic payment system designed for the settlement of U.S. dollar payments between Mexican banks. Launched in 2016, SPID was developed in part to increase traceability and transparency of dollar-denominated transactions within the Mexican financial system, and it requires enhanced AML/CFT obligations of all participating banks.[141]

SPID has not yet become fully functional, and financial crime risks and questions remain, including how transparent the system will be, whether it could shield suspect dollar transactions from U.S. authorities, and how it responds to real risks to the Mexican system.[142] Despite those questions, SPID provides an opportunity to think creatively about how a credible national authority might use the real-time collection, screening, and analysis of financial data to identify and respond to vulnerabilities and threats to the banking sector.

The United States has long evaluated the possibility of systemic reporting of cross-border wire transfer information. In September 2010, FinCEN proposed a regulatory requirement that would obligate certain banks and money transmitters to report cross-border electronic transmittals of funds.[143] Officials argued that "by establishing a centralized database, this regulatory plan will greatly assist law enforcement in detecting and ferreting out transnational organized crime, multinational drug cartels, terrorist financing, and international tax evasion."[144]

In 2015, FinCEN announced its intent to revisit its 2010 proposal to capture information on all bank cross-border wires and non-bank remittances of $1,000 or more.[145] FinCEN's renewed interest was sparked by the completion of the FinCEN IT Modernization Project, which now gives the bureau the systems and information technology platforms required to collect and analyze large volumes of cross-border electronic funds transfers.[146] The U.S. government has not yet moved toward the capture of all cross-border wire information, but the technical possibilities may spur this to happen.

Another important step toward greater transparency and risk management is a new FinCEN reporting

140. U.S. Department of the Treasury, Financial Crimes Enforcement Network, "Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime," October 25, 2016. (https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf)
141. Banco de México, "Domestic USD Transfer System (SPID)," March 2016. (http://www.banxico.org.mx/sistemas-de-pago/servicios/sistema-de-pagos-interbancarios-en-dolares-spid/%7B3DBBBDBD-055F-1289-0201-9C307BB9EA63%7D.pdf)
142. Benjamin Bain and Alan Katz, "Money-Launder Woes Push Mexico into Dollar-Transfer Business," *Bloomberg*, February 12, 2016. (http://www.bloomberg.com/news/articles/2016-02-12/money-laundering-woes-push-mexico-into-dollar-transfer-business)
143. U.S. Department of the Treasury, Financial Crimes Enforcement Network, "FinCEN Proposes Regulatory Requirement for Financial Institutions to Report Cross-Border Electronic Transmittals of Funds," September 27, 2010. (https://www.fincen.gov/news_room/nr/html/20100927.html)
144. Ibid.
145. Brian Monroe, "With IT Modernization Finished, FinCEN Again Raising Cross-Border Funds Transmittal Initiative," *Association of Certified Financial Crime Specialists*, June 4, 2015. (http://www.acfcs.org/news/300828/With-IT-modernization-finished-FinCEN-againraising-cross-border-funds-transmittal-initiative.htm)
146. U.S. Department of the Treasury, Financial Crimes Enforcement Network, "FinCEN's IT Modernization Efforts." (https://www.fincen.gov/fincens-it-modernization-efforts)

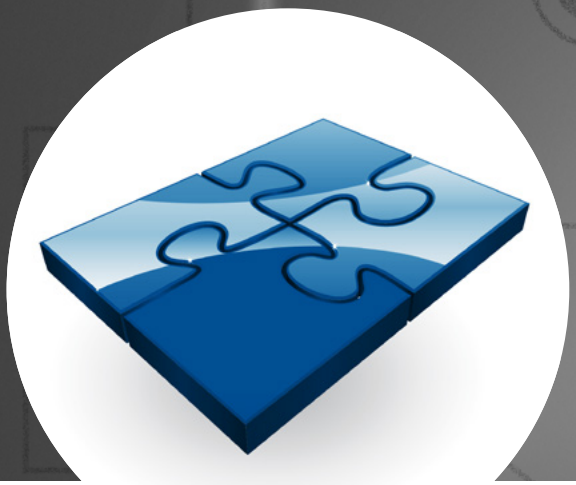
requirement announced in May 2016. It requires financial institutions to identify and verify the beneficial owners of certain customers, which would help analyze cross-border wire transfer information.[147]

Such national centralization efforts are echoed by corresponding supranational developments, such as the consolidated transaction monitoring and analytic systems from SWIFT. In late 2014, SWIFT launched its KYC (know-your-customer) Registry, a secure shared platform for financial institutions to exchange and manage standardized KYC data, developed in collaboration with others in the industry.[148] To date, approximately two thousand banks in 191 countries are using it as a cost-effective way to improve the efficiency of their operations, reduce cost, and mitigate risk.[149] SWIFT has also launched a Sanctions Screening service, which allows for real-time message screening for institutions, especially midsize institutions, against 30 sanctions lists.[150]

These types of platforms and screening models could be expanded beyond sanctions screening to include the monitoring, analysis, and flagging of illicit financing. They could also be combined with models to centrally collect transaction information to supplement enhanced KYC information sharing.

While the private sector will lead efforts to develop and incorporate these and other new technologies, the United States government can assist by encouraging financial technology companies and traditional financial institutions to determine the most effective ways to analyze big data to fight money laundering, sanctions evasion, and corruption.

147. Customer Due Diligence Requirements for Financial Institutions, U.S. Department of the Treasury, Financial Crimes Enforcement Network, 81 Federal Register 29398, May 11, 2016. (https://www.gpo.gov/fdsys/pkg/FR-2016-05-11/pdf/2016-10567.pdf)
148. Society for Worldwide Interbank Financial Telecommunication (SWIFT), "The KYC Registry," accessed December 1, 2016. (https://www.swift.com/our-solutions/compliance-and-shared-services/financial-crime-compliance/the-kyc-registry)
149. Bryan Yurcan, "Banks Prove Willing to Band Together Under KYC Pressure," *American Banker,* Jan. 14, 2016. (http://www.americanbanker.com/news/bank-technology/banks-prove-willing-to-band-together-under-kyc-pressure-1078835-1.html)
150. Society for Worldwide Interbank Financial Telecommunication (SWIFT), "Sanctions Screening," accessed December 1, 2016. (https://www.swift.com/our-solutions/compliance-and-shared-services/financial-crime-compliance/sanctions-screening)



Strategic and Structural Changes

In an age of globalization, free flow of information, and digital dependencies, the economic and national security spheres overlap more than ever. National economic security must encompass a wide spectrum of policies, ranging from macro-level factors such as national debt and GDP to specific threats with economic repercussions, such as terrorist attacks on Wall Street or U.S. ports. It entails preparing for defense-related and economic risks, including cyber defense and supply-chain vulnerabilities, but also systemic threats to the financial system, market manipulation, long-term cyber espionage, and cyber attacks, as well as our adversaries' resource access and investment reach.[151] It also includes ensuring that the United States retains its positive economic power.

Developing a National Economic Security Strategy

To ensure that the United States sustains its competitive advantage, the Trump administration needs to conduct a long-overdue strategic assessment of the impact that economic, financial, and commercial activity now has on the conduct of its foreign policy.

As part of this assessment, the United States needs to consider new doctrines that will serve as the template for effectively employing U.S. economic power to achieve political objectives. For example, the Treasury Department should develop a doctrine on the use of both offensive economic coercion and deploying defenses against economic coercion by others. The Defense Department has well-developed doctrines on the use of military force, and it is creating a cyber warfare doctrine. There is also an increasing interest in developing an all-of-government "lawfare" doctrine to guide how legal tools can be used as instruments of offensive and defensive legal warfare.[152] The Pentagon has created clear rules of engagement on the use of the tools at its disposal, and so should the Treasury Department and the National Security Council (NSC) on matters of national economic security.

Reforming the U.S. Government to Better Address These Issues

One of the primary impediments to developing and employing a successful economic security strategy is that responsibility for the levers of U.S. economic power are widely dispersed across the government, with limited coordination between them. For example, while the Treasury Department handles most of the U.S. sanctions regime in coordination with the State and Commerce Departments, positive economic tools such as investment and private sector coordination are generally deployed by agencies such as the State Department and USAID, often with little coordination with Treasury.

151. Juan Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare*, (New York: PublicAffairs, 2013), Chapter 16.
152. Orde Kittrie, *Lawfare*, (New York: Oxford University Press, 2016).

The idea of creating structures and strategies designed to safeguard national economic security is not new; in 1943, the U.S. government established the Office of Economic Warfare, an agency charged with safeguarding the U.S. dollar. More than 200 market analysts around the world and nearly 3,000 experts in Washington accomplished their mission by helping U.S. producers increase exports and secure vital imports at favorable terms.[153]

Seventy years later, the United States must renew its commitment to ensuring its national economic security. The federal government can take a number of steps to better coordinate its various tools of economic statecraft to ensure they are mutually supportive:

- **Establish greater economic statecraft expertise within the White House.** U.S. officials have informally made clear that the White House staff need more in-depth understanding of coercive economic tools and view economic coercion as a central component of national security policymaking. The National Security Council staff has a directorate of international economics. It is from this – as a subcomponent or as a reconfiguration of its priorities – that a directorate of economic coercion ought to be created, either within the NSC or, as discussed below, as a major component of the National Economic Council (NEC). This directorate would focus broadly on economic coercion and would need to cooperate closely with other experts in the NSC. It is important that when the NSC chairs its senior level meetings (assistant-secretary level and above), they include the NSC (senior) director with sanctions expertise.
- **Create an Office of Policy Planning at Treasury.** Unlike the State Department and the Pentagon, the Treasury Department does not have an office responsible for policy planning. Treasury's Office of Policy Planning would report to the Secretary of the Treasury and emphasize creativity in the development of new economic and financial tools. It would assemble experts from outside government and from offices throughout the department who can bring diverse expertise to the table. These would include specialists from the Office of Foreign Assets Control (in charge of U.S. sanctions programs); the Office of Terrorist Financing and Financial Crimes; the Office of Intelligence and Analysis; and the financial crimes experts from the Financial Crimes Enforcement Network; as well as Treasury's International Affairs office. The new Office of Policy Planning should develop long-range strategies to deal effectively with economic and financial warfare, including how to create a defensive shield architecture to protect the U.S. and allied economies. The director of this office could have an ambassador rank to allow for engagement with other countries and finance ministries.
- **Better intertwine the National Security Council and the National Economic Council.** These bodies have traditionally been separated, with the NSC focusing on national security and the National Economic Council addressing domestic economic issues. As the United States has increasingly used economic coercion abroad, this divide makes less sense. Giving the NEC a greater seat at the NSC table (and vice versa) would help elevate important economic statecraft issues and ensure that many different angles of the same challenges would be considered. Former Deputy Treasury Secretary Robert Kimmitt and others have argued for making the Treasury secretary a statutory member of the National Security Council.[154]

New Private-Public Sector Coordinating Mechanisms

The government needs to do a better job explaining to businesses the various U.S. policies and requirements

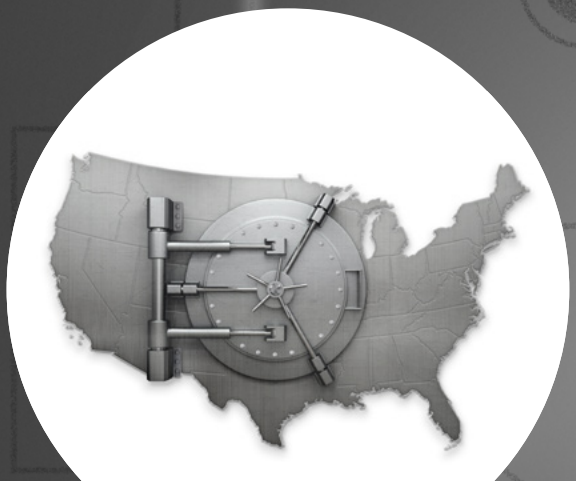
153. Robert D. Blackwill and Jennifer M. Harris, "The Lost Art of Economic Statecraft," *Foreign Affairs*, March/April 2016. (https://www.foreignaffairs.com/articles/2016-02-16/lost-art-economic-statecraft)

154. Robert M. Kimmitt, "Give Treasury Its Proper Role on the National Security Council," *The New York Times*, July 23, 2012. (http://www.nytimes.com/2012/07/24/opinion/give-treasury-its-proper-role-on-the-national-security-council.html)

related to coercive, defensive, and positive economic power. The United States lacks systemized, effective measures for engaging the private sector on sanctions-related matters. Too often, private sector companies feel like the government is hiding the regulatory ball and imposing draconian penalties without providing sufficient information. As a result, companies refuse to engage in permissible and desirable activities because they fear running afoul of U.S. sanctions regulations.

One way to address this gap is to create an Economic Sanctions Advisory Board, which would advise heads of relevant agencies and offices (such as the Office of Foreign Assets Control and the Bureau of Industry and Security). Crafting effective sanctions frequently requires private sector buy-in, and insights offered by financial institutions and other businesses can be invaluable in calibrating these coercive tools. The board could consist of government officials at relevant departments (NSC, Treasury, State, Commerce, and Justice), as well as leaders in the private sector and academia. Those in the private sector should come from a range of industries, with a particular focus on the financial, trade, insurance, and related sectors. The board could discuss and provide insight into what is – and is not – working in U.S. sanctions policy, and how the U.S. government can continue to sharpen its tools of economic statecraft while also limiting unintended consequences.

Finally, regulators and policymakers need to encourage private sector innovations for risk management, as discussed in this report (see "Ensuring the Integrity of the Financial System"). Regulators need to allow for greater experimentation and be open to collectivized models of risk management, including between government and private sector entities. In the United States, a more permissive use of Section 314(b) of the USA PATRIOT Act to include involvement of technology companies may provide greater freedom to experiment with information-sharing platforms and mechanisms.



Conclusion

As President Trump takes office, he has powerful tools of economic statecraft at his disposal, yet he also faces a challenging environment where state and non-state adversaries are also learning to more effectively use such levers. This report provides the Trump administration with an overview of the national economic security issues it will face, as well as recommendations for how to better prepare the United States to compete successfully in this complicated and evolving national economic security game.

The Trump administration should be prepared to use its economic power in a number of key areas, including pressuring China to cease its destabilizing activities in the South and East China Seas by imposing sanctions on Chinese companies supporting such actions. Likewise, it should consider ways to increase the pressure on North Korea, both by targeting Chinese companies supporting North Korea's continued nuclear and ballistic missile proliferation and by better uncovering additional North Korean illicit financing and smuggling networks.

On Iran, the administration should aggressively enforce existing sanctions, hold Iran to account for any violations of the JCPOA, and ramp up sanctions on the country for its ballistic missile development, support for terrorism, human rights abuses, and other malign activities. It should also identify ways to strengthen the JCPOA so that it permanently blocks Iran from developing nuclear weapons.

The administration should further consider ratcheting up its economic power on Russia. Given Russia's aggressive actions towards Crimea – as well as the intelligence community's conclusions that it engaged in a cyber campaign to impact the outcome of the 2016 presidential election – the administration should be prepared to support efforts by Congress to punish Russia and deter it from future destabilizing activities.

On the defensive side, the administration should immediately make clear to China and Russia that they will pay a heavy price for stealing U.S. intellectual property and engaging in cyber-enabled economic warfare. Likewise, the administration should also begin to reform the CFIUS process as a means to block dangerous strategic investment into the United States.

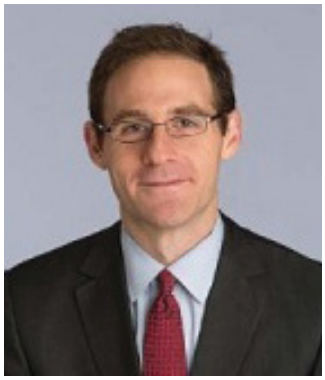
At the same time, the administration must work towards increasing financial transparency and accountability by encouraging financial institutions to innovate and share information. It should continue to press the federal government to work more closely with the private sector while reforming government agencies and institutions to more easily address and tackle these issues in a more comprehensive way.

The economic statecraft challenges will undoubtedly evolve over time. And these recommendations are only a first step. But it is crucial that the United States successfully compete in this challenging environment. It is our hope that this report will help in meeting these challenges head on.

Acknowledgments

We wish to thank FDD's Yaya Fanusie, Annie Fixler, Oren Kessler, Emanuele Ottolenghi, Anthony Ruggiero, Nicole Salter, and David Weinberg for their feedback and edits, both substantive and stylistic. Thank you to our external readers Peter Harrell and Rafi Danziger who provided crucial feedback to the report. We are also grateful to Daniel Ackerman and Erin Blumenthal for the graphics, design, and production of this report. Finally an immense thank you goes to Allie Shisgal whose diligence, attention to detail, and excellent oversight ensured the success of this project. This report and the issues discussed within have benefited greatly from the tremendous thought leadership of FDD's Center on Sanctions and Illicit Finance.

About The Author



Eric B. Lorber, an expert on anti-money laundering policy and terror finance issues, is senior advisor at the Foundation for Defense of Democracies' Center on Sanctions and Illicit Finance. At CSIF, Mr. Lorber works on issues related to economic statecraft, with a particular focus on how China and Russia will increasingly employ economic coercion. He also researches financial sanctions and their impact on the global financial system, as well as the relationship between the private sector and government in achieving national security objectives.

Mr. Lorber is a senior associate at the Financial Integrity Network, where he advises financial clients on issues related to economic sanctions, anti-money laundering, and regulatory compliance. Prior to working at FIN, he was an attorney in the Washington, D.C. office of Gibson, Dunn & Crutcher, where he advised clients in the areas of international trade regulation, compliance, and anti-corruption, with particular emphasis and experience assisting clients in complying with the economic sanctions and embargo regulations administered by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC).

This report was aided by many members of FDD's Center on Sanctions and Illicit Finance (CSIF), including: The Hon. Juan C. Zarate, Mark Dubowitz, Dr. Jonathan Schanzer, Chip Poncy, Dr. Zack Cooper, Elaine Dezenski, Adnan Kifayat, Dr. Michele Malvesti, J. R. (Bob) McBrien, Dr. Samantha Ravich, James Rickards, Amit Sharma, and Amb. John Simon. Several important pieces of research by the CSIF team were included and used as a basis for components of this report, including: Juan Zarate's *Treasury's War: The Unleashing of a New Era of Financial Warfare* (PublicAffairs, 2013); Samantha Ravich's *Cyber-Enabled Economic Warfare: An Evolving Challenge* (Hudson Institute, 2015); Chip Poncy's June 2015 testimony before the House Financial Services Committee Task Force to Investigate Terrorism Financing; Juan Zarate's "The New Geo-economic Game" (European Council on Foreign Relations, 2016); Juan Zarate and Chip Poncy's "Designing a New AML System" (The Clearing House, 2016); and Mark Dubowitz and Annie Fixler's *'SWIFT' Warfare: Power, Blowback, and Hardening American Defenses* (FDD's Center on Sanctions and Illicit Finance, 2015), among others.

For more information on this research and CSIF, visit www.defenddemocracy.org/csif.

About the Foundation for Defense of Democracies' Center on Sanctions and Illicit Finance

The Foundation for Defense of Democracies (FDD) is a Washington, DC-based non-partisan policy institute focusing on foreign policy and national security. FDD's Center on Sanctions and Illicit Finance (CSIF) expands upon FDD's success on the use of financial and economic measures in national security. The Center's purpose is to provide policy and subject matter expertise in areas of illicit finance, financial power, and economic pressure to the global policy community.

CSIF seeks to illuminate the critical intersection between the full range of illicit finance and national security, including money laundering, terrorist financing, sanctions evasion, proliferation financing, cyber crime and economic espionage, and corruption and kleptocracy. This includes understanding how America can best use and preserve its financial and economic power to promote its interests and the integrity of the financial system. The Center also examines how America's adversaries may be leveraging economic tools and power.

CSIF focuses on global illicit finance, including the financing of terrorism, weapons and nuclear proliferation, corruption, and environmental crime. It has a particular emphasis on Iran, Saudi Arabia, Kuwait, Qatar, Turkey, Russia, and other autocratic states as well as drug cartels and terrorist groups including Hamas, Hezbollah, al-Qaeda, and the Islamic State.

For more information, please visit www.defenddemocracy.org.

FDD
FOUNDATION FOR
DEFENSE OF DEMOCRACIES

P.O. Box 33249
Washington, DC 20033-3249
(202) 207-0190
www.defenddemocracy.org