‘SWIFT’ Warfare
Power, Blowback, and Hardening American Defenses

Mark Dubowitz
Annie Fixler

Foreword by Juan C. Zarate

Center on Sanctions & Illicit Finance

FOUNDERATION FOR DEFENSE OF DEMOCRACIES

July 2015
‘SWIFT’ Warfare
Power, Blowback, and Hardening American Defenses

Mark Dubowitz
Annie Fixler

Foreword by Juan C. Zarate

July 2015

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

This report is included in the monograph, “Cyber-Enabled Economic Warfare: An Evolving Challenge,” edited by Dr. Samantha Ravich and published by the Hudson Institute.
# Table of Contents

Foreword by Juan C. Zarate ........................................................................................................ 3

**PART 1: SWIFT, SMART SANCTIONS, AND THE FINANCIAL WAR AGAINST IRAN** ........................................................................................................ 5

Introduction .................................................................................................................................. 5
Financial Intelligence ....................................................................................................................... 6
The Iran Playbook .......................................................................................................................... 8
From FININT to Economic Coercion: Disconnecting Iranian Banks ........................................... 10
The Impact of “De-SWIFTing” Iran ................................................................................................. 14
Contemplating Russia .................................................................................................................... 16

**PART 2: IF ECONOMIC WARFARE TABLES WERE TURNED** ......................................................................................................................... 21

From Old-School to Cyber-Based Sanctions Busting .................................................................. 21
Future Threats: The Use of Cyber-Enabled Economic Warfare Against the United States and U.S. Allies ............................................................................................................ 23
Hypothetical: SWIFT and the Crisis in the South China Sea ......................................................... 25

**PART 3: RECOMMENDATIONS** ............................................................................................... 29

Introduction ................................................................................................................................... 29

First Phase: Organizational Rearrangement .................................................................................. 32
  1. Create an Office of Policy Planning at the U.S. Department of the Treasury ....................... 32
  2. Set Up an Economic Coercion Directorate at the National Security Council ....................... 33
  3. Create a Doctrine on the Use of Economic Coercion ............................................................. 34

Second Phase: The Creation of an Economic Warfare Command ............................................... 35

CONCLUSION ............................................................................................................................... 37
Foreword

The financial wars of the future are upon us. The geo-economic landscape is changing, as power and security relationships are reshaped globally. The use of financial power and economic influence in national security has now taken pride of place as a strategy for great powers and their proxies. Just as the United States was unable to imagine the looming threats from global terrorism before 9/11, history may too judge an inability to understand and forecast the importance of financial power in the 21st century a collective failure of comprehension.

Over the past decade, the United States has taught the world how to use economic and financial power, and our adversaries have been watching. The United States has leveraged U.S. capital markets, the centrality of the dollar, and America’s ability to set global standards and norms to drive its national security goals. The power of this paradigm is derived from the centrality and stability of New York as a global financial center and the importance of dollar-clearing transactions. Our competitors have learned from and chafed at our use of such power. Our enemies have likewise witnessed our vulnerabilities and understood their own potential in using financial power directly or asymmetrically against the United States and its allies. In any comprehensive national security strategy, the U.S. government must develop a national economic security strategy and capabilities.

Mark Dubowitz and Annie Fixler, my colleagues at FDD’s Center on Sanctions and Illicit Finance, explore this very topic in a creative and important way in the paper that follows.

The first section presents a baseline to understand the geo-economic landscape of today, describing how the United States transformed tools of economic coercion for national and international security purposes. It details the development of “smart sanctions” and tracks the use of financial tools against Iran, one of the greatest threats to the global nonproliferation and counter-threat finance regimes and the broader integrity of the global financial system. The strategic paradigm deploying campaigns to expand the reach of the United States against rogue actors through the financial system has proven effective over the past thirteen years, but this arena is no longer the sole province of the U.S. government nor does this approach remain secret.

The United States has been at the cutting edge of this 21st century geo-economic competition. But the fact that it was first to develop innovative and powerful financial tools to pursue its interests is no guarantee of continued success. Although the United States has had a near monopoly on the use of targeted financial pressure over the past ten years, this edge could erode, leaving the United States both more vulnerable to external financial pressure and less able to use financial suasion as a lever of foreign policy.

In this paper, Dubowitz and Fixler reinforce the idea that the United States must prepare for a reality where other countries—especially rising economic powers like China—purposely use financial and economic strategies to weaken U.S. and allied interests. They demonstrate that without deliberate strategic planning and structural reforms, the United States will be poorly equipped to defend its interests and its allies from the use of economic warfare tools by its adversaries.

The hypothetical scenario laid out in Part 2 imagines a moment in which China uses economic warfare against a U.S. ally in order to advance its own geopolitical goals. The purpose of the hypothetical is to provide a realistic scenario in which China uses its growing economic and financial influence within the current global system to isolate an adversary – and to mute a U.S. response. It is a realistic example of the type of economic conflict that might arise with a power willing to use the attractiveness of its markets and the financial weapons of the global system as part of a broader geo-
political offensive. It also underscores that the United States could find itself flat-footed and unprepared to confront this type of power and to roll back economic aggression in an increasingly interdependent global environment without proper planning and preparation.

Though the details of this scenario could change and countries like China may elect to leverage alternate channels or modes of financial influence outside the current global system, the authors paint a convincing picture of what economic warfare might look like. The hypothetical and the paper sharpen the reality of possible economic conflict and escalation in an ever more connected global system in which the United States remains vulnerable. By revealing a scenario where Chinese motivations and use of such power are clear, the hypothetical also puts recent developments like the Chinese movement to establish the Asia Infrastructure Investment Bank (AIIB) and an alternate international payment system into starker relief. The paper reinforces the need for a serious study of defensive economic warfare—from doctrine and strategy to tactics and decision-making.

The United States needs policies that recognize the vulnerabilities and opportunities in the changing national security environment and take into account the range of actors and tools that now occupy this asymmetric landscape. Confronting the new realities of this geo-economic ecosystem requires innovative policy, new institutions and doctrines, and new modes of public-private collaboration and international cooperation. The nuclear age brought nuclear doctrine and strategies; the development of long-range missiles led to the creation of missile shields and alliances; the proliferation of cyberattacks has led to the creation of a Cyber Command and consideration of new forms of warfare. The age of financial warfare should likewise bring new strategies, doctrines, alliances, defensive shields, and command and control structures. The winners in this new era of economic warfare will be those who can sharpen their offenses while complementing with economic defense-in-depth. To date, the United States has too often focused on the former and neglected the latter.

What is needed is a strategic framework for national economic security that accounts for the emerging economic security environment of the twenty-first century. The recommendations in Part 3 lay out a clear and logical path forward for the United States to prepare itself for the coming challenges. A policy planning function at the U.S. Treasury, greater depth and convergence of expertise within the White House staff on issues of financial power, a clearly defined doctrine on the use of economic coercion, and even the proposal for an Economic Warfare Command, among other recommendations, are important ideas to consider if the United States hopes to prepare to defend itself against potential financial and economic aggression. To address our vulnerabilities, we need to conceive of the global landscape differently and organize ourselves appropriately to use the full expanse of U.S. national power to defend our interests.

This paper puts these recommendations and the current context into sharp relief. The paper and the embedded hypothetical and policy recommendations are worthy of serious consideration. It is time to redesign a national economic security model to prepare for the coming financial wars. If we fail to do so, the United States risks being left vulnerable and left behind as other competitors race toward the future.

Juan C. Zarate
Former Deputy Assistant to the President and Deputy National Security Advisor for Combating Terrorism
Former Assistant Secretary of the Treasury for Terrorist Financing and Financial Crimes
Chairman and Senior Counselor, FDD’s Center on Sanctions and Illicit Finance


**PART 1: SWIFT, SMART SANCTIONS, AND THE FINANCIAL WAR AGAINST IRAN**

**Introduction**

Economic warfare is now the default instrument of coercive statecraft for confronting challenges to the international order. Sanctions have become President Barack Obama’s weapon of choice to combat Iran’s nuclear program, Russia’s invasion of Ukraine, the Assad regime in Syria, and the financing of terrorist groups such as the Islamic State, al-Qaeda, and others.

Leveraging the power of the U.S. dollar to isolate rogue actors—from the terrorists and nuclear proliferators of Iran’s Revolutionary Guards to Sunni jihadists to Russian arms dealers and oligarchs—the U.S. Department of Treasury has established itself as a key national security agency. Economic sanctions, once thought to cause humanitarian crises without impacting the calculus of authoritarian regimes, have become a sophisticated tool for targeting the financial resources of a range of rogue actors. Financial sanctions became the key driver of an overall economic sanctions architecture that used conduct-based sanctions to isolate illicit financial activities.

The transformation of blunt and broad state-based embargos into the “smart sanctions,” as they are characterized 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 and facilitate the terror group’s violent activities.

These tools of economic coercion treat reputation as a currency in an environment in which companies cannot afford the risk of being associated with bad actors. The rules of this new world are straightforward: You can do business with the United States or you can do business with rogue actors. You can choose, but you can’t do both. And if you choose the latter, prepare to be excommunicated from the global financial community.

The system is self-reinforcing: As rogue actors become more isolated, they engage in more suspicious behavior to evade restrictions. And the more suspicious their behavior, the more they find themselves isolated from financial networks. The approach is based on persuading private sector players—principally financial institutions—to act in their own self-interest to avoid unnecessary business and reputational risk.

As smart sanctions matured and the U.S. government discovered a new form of coercive power, the use of cyber-enabled financial measures became an integral part of the global financial sanctions architecture. At the heart of this architecture is SWIFT (the Society for Worldwide Interbank Financial Telecommunication), a financial messaging service that is the electronic bloodstream of the global financial system.

The story of how Iran became the first country to be expelled from the SWIFT system provides a glimpse into how economic warfare has changed in the past decade, and the importance of American economic preeminence in this pursuit. It also raises questions, however, about whether Washington is prepared to respond when states like China and Russia, looking to challenge the U.S.-led international order, turn their own economic power against the United States and its allies.

While tools of economic coercion in general, and cyber-enabled economic warfare in particular, have both offensive and defensive components, the United States, to date, has primarily used those of an offensive...
nature. This paper analyzes offensive tools while acknowledging the importance of, and the danger in neglecting, defensive planning. While economic warfare encompasses a broad range of tools, financial sanctions are the foundation for the larger architecture of economic sanctions. As a result, this study addresses the rise of financial tools generally and cyber-enabled financial and economic sanctions specifically. This study also focuses on the tools used by the U.S. Treasury Department rather than attempting to address the range of economic coercion tools available to all agencies of the U.S. government. In the final section of this paper, however, we provide broader economic warfare recommendations and highlight ways that greater coordination across agencies might be facilitated.

Financial Intelligence

Financial intelligence (FININT) is at the heart of American efforts to leverage its financial assets in the pursuit of rogue actors and key to understanding the central role of SWIFT in these efforts. In the years before the formal creation of the Treasury Department’s Office of Terrorism and Financial Intelligence (TFI) in 2004 and Treasury’s intelligence agency, the Office of Intelligence and Analysis (OIA), the Department developed a financial intelligence capability to block the assets of rogue actors and uncover and dismantle illicit financial networks. As a result, while the smallest agency in the U.S. government’s intelligence behemoth, OIA punches well above its weight, unraveling illicit financial networks and providing evidence for thousands of designations.

The use of financial intelligence has been instrumental in disrupting terrorist cells and foiling plots including, for example, the planned attack on JFK airport in 2007—an attack linked to Iran’s intelligence and covert networks in Latin America.3

FININT relies on traditional sources and methods of intelligence gathering and also on financial papers found in terrorist safe-houses, detailed records from formal and informal financial institutions, suspicious activity reports from banks, and wire-transfer records. One of the critical elements of cyber-enabled, financial intelligence is messaging data from SWIFT.

Formed in 1973, SWIFT replaced telex messages between banks with a more secure, highly encrypted communications system. The consortium, headquartered in Belgium with 23 offices worldwide, has “the mission of creating a shared worldwide data processing and communications link and a common language for international financial transactions.”4 While other companies can enable secure financial transactions, SWIFT is the worldwide leader, far and away, with estimates of $6 trillion each day in payments value. SWIFT claims to link more than 10,500 institutions in 215 countries,5 allowing the daily exchange of millions of standardized financial messages between banks, corporate customers, and financial institutions. SWIFT “does not hold funds nor does it manage accounts on behalf of customers, nor does it store financial information on an on-going basis.”6 SWIFT is merely the courier that delivers financial messages between banks.

In the 1990s, the CIA tried to access SWIFT clandestinely to gather information on al-Qaeda’s financial network, but the Treasury Department blocked the operation over concerns about a backlash from the banking community and perceptions that it would compromise the integrity of the financial

After 9/11, however, Treasury officials immediately began to reconsider how information from SWIFT could be legally and effectively leveraged as part of counterterrorism operations.

Within six weeks, Treasury built an innovative program, which became known as the Terrorist Finance Tracking Program (TFTP), to leverage SWIFT data to expose links between terrorists and their funders. The program analyzed the cyber data that formed the language of global financial transactions. Prior to the widespread adoption of SWIFT, such analysis may only have been possible by subpoenaing individual banks, compiling records from thousands of financial institutions (mindful that the worst offenders would be least likely to comply), and then analyzing the data to establish links. Instead, using data from SWIFT alone, Treasury was able to build a highly effective program for uncovering terrorists’ financial ties.

Treasury built a separate database to search SWIFT records and provided SWIFT with subpoenas on a monthly basis for select tranches of data that were then entered into the quarantined database. Only select officials could access the database and only for counterterrorism efforts—not operations related to proliferation, money laundering, or other criminal activities. SWIFT had negotiated the most stringent restrictions to protect its data. To ensure compliance, SWIFT “scrutineers” had access to the system to verify each query was based on a counterterrorism investigation. Former SWIFT chief executive Leonard Schrank, who worked with Treasury to create the program, noted, “The use of the data was legal, limited, targeted, overseen and audited,” and the program could be considered the “gold standard” for how to balance national security and civil liberties. Although kept secret from the public for five years, the program was known to a targeted group in the intelligence community and executive branch, select members of Congress, and numerous banking officials in Europe and the United States.

Carefully constructed by the leadership of SWIFT and Treasury’s general counsel David Aufhauser to protect customer privacy, while also providing vital information to disrupt terrorist financing, the program proved invaluable to disrupting terrorist networks and uncovering dangerous plots. The TFTP provided information on “a key facilitator of terrorism in Iraq” and led to the capture of Riduan Isamuddin, aka Hambali, who was believed to be the mastermind of a string of bombings in Asia including the 2002 bombing in Bali and the 2003 attack on the Marriott hotel in Jakarta. According to the Treasury Department, the program “helped to disrupt terrorist cells and operations and has helped save lives.”

Despite the program’s legality and its importance to U.S. counterterrorism efforts, on June 23, 2006, The New York Times revealed the existence of TFTP, jeopardizing not only its effectiveness but also U.S. relations with countries in Europe. Treasury tried to


---

persuade The New York Times not to publish the article by explaining the details of the program and its legality. But Treasury was unsuccessful at persuading The New York Times after its editors learned that the Los Angeles Times was going to run a similar story. Treasury, it should be noted, was prepared for public revelations about the program since its inception. When the article came out, the administration launched a full-throttle defense of TFTP and equally strong criticism of The New York Times' decision to publish the article.

The articles alerted terrorist financiers to Treasury’s methods. More damaging, however, were the revelations about Treasury’s relationship with SWIFT, which prompted political attacks and challenges in European courts against the financial messaging service and accusations that SWIFT’s actions were illegal and violated laws on data privacy. Even those European officials who had known about TFTP claimed not to understand the extent of the program. SWIFT itself weathered the storm but was thrust into a bruising political debate.

Tensions between the U.S. and EU intensified with a February 2010 vote in the EU Parliament to block the agreement between the U.S. government, European Commission, and EU Council of Ministers permitting U.S. law enforcement access to SWIFT data. Although a new agreement was reached with the European Union later that year, the program remained under intense scrutiny and was challenged again in October 2013 when the European Parliament called for a suspension of U.S. access to SWIFT data amid concerns over the National Security Agency’s unrelated data-mining program. The program and relationship between the U.S. government and SWIFT has required constant diplomatic attention.

The Iran Playbook

Meanwhile, Iranian threats to global security and the integrity of the financial system continued to grow. Building on the administration’s work with the private sector to isolate terrorist finance, Treasury devised a new campaign to isolate Iran from the global financial system based on Iran’s illicit business and banking practices. Iran was first added to the State Department’s State Sponsors of Terrorism list in 1984 and had been under U.S. sanctions for its support for terrorism, missile proliferation, human rights abuses, and its nuclear program. These sanctions had not halted Iran’s illicit activities, so Treasury, with extensive congressional support, designed a new campaign to take financial warfare to a completely different level of impact.

In February 2006, then-Treasury Undersecretary for Terrorism and Financial Intelligence Stuart Levey formally pitched Treasury’s new idea to Secretary of State Condoleezza Rice, and, with interagency approval and coordination, the Treasury Department began its campaign to persuade the global financial market to isolate Iran.

In the first two and a half years of the effort, Levey made more than 80 visits to foreign countries to meet not

only with his government counterparts but also with the heads of more than 60 banks. Levey presented detailed information about Iran’s illicit activities and specific examples of suspicious transactions involving foreign banks. The dossiers had the effect of conditioning the environment to reject Iranian transactions. As former Treasury official Juan Zarate explained, “Levey’s job was to stage the financial assault on Iran’s banks and its financial system—in large part by demonstrating to CEOs and compliance officers around the world that the risk of doing business with Iran was too high.”

Simultaneously, utilizing Executive Orders 13224 (2001) and 13382 (2005) targeting the financing of terrorism and weapons proliferation, respectively, Treasury started to designate individual Iranian banks for their role in facilitating illicit financial activities. These two executive orders set the precedent for not only targeting the illegal trade in illicit goods but also for isolating the financial transactions that enable the movement of physical commodities. Beginning in 2007, the Treasury Department designated 23 Iranian and Iranian-allied foreign financial institutions as “proliferation supporting entities” under Executive Order 13382. Of these, at least eight banks were designated for their ties to Iran’s Islamic Revolutionary Guard Corps (IRGC) or because they were controlled by banks with IRGC links. Treasury in 2006 also sanctioned Bank Saderat as a “terrorism supporting entity” under Executive Order 13224 for facilitating fund transfers to Hezbollah, Hamas, Palestinian Islamic Jihad, and other terrorist organizations.

The State Department supported Treasury’s efforts through a diplomatic push to explain the financial campaign, as well as to increase the political pressure on Iran. Working bilaterally and within the United Nations, State sought to build international buy-in for broader sanctions against Iran. While the U.N. Security Council eventually passed four sanctions resolutions against Iran starting in 2006, each resolution required months of negotiations and significant compromises in order to get Chinese and Russian approval. It became clear that by working outside traditional international bodies like the U.N., the U.S. Treasury Department could leverage the power of the dollar and the central role that the U.S. plays in financial markets in order to cut off Iranian financial transactions. However, the U.N. resolutions provided a foundation for other countries to implement their own multilateral and unilateral sanctions. This was especially true in the case of U.N. Security Council Resolution 1929 (2010) that provided the European Union with political cover for implementing its own oil embargo. The U.N. resolutions also gave a semblance of multilateralism to what the United States was already implementing unilaterally.

Treasury’s new efforts to lead the way on a tougher and smarter sanctions regime were strengthened significantly by the bipartisan passage of multiple pieces of congressional legislation between 2010 and 2013. These congressional measures targeted Iran’s financial, energy, shipping, insurance, and defense sectors.

25. Bank Sepah (Iran); Bank Melli (Iran); Arian Bank (Iran); Bank Kargoshaee (Iran), controlled by Bank Melli; Future Bank (Bahrain), controlled by Bank Melli; Post Bank of Iran (Iran), controlled by Bank Sepah; Ansar Bank (Iran); Mehr Bank (Iran).
precious metals, and industrial trade, including a successful effort, initially opposed by the Obama administration, to squeeze Iran's economic lifeline: its crude oil exports.

In 2010, Congress passed the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 (CISADA),28 overhauling the Iran Sanctions Act, which had been on the books since 1996 but it was never effectively enforced because of resistance from European governments and companies. With Europe now moving ahead with its own sanctions against Iran's nuclear program, this resistance diminished. CISADA now provided the Obama administration with the threat of congressional action to persuade foreign companies to choose between their business ties to Iran and their access to the U.S. market.

The legislation prompted dozens of foreign companies, especially European energy firms, to terminate the provision of refined petroleum products to Iran and to cease further investments in the Iranian energy sector. It also provided a package of powerful financial measures to strengthen Treasury's financial sanctions campaign by threatening to cut off foreign financial institutions from their banking relationships in the United States, and their ability to offer U.S. banking services, including the use of the U.S. dollar, to their banking clients. Six months after the passage of CISADA, then-Undersecretary for Political Affairs Bill Burns testified before Congress that the legislation had already cost Iran between $50 and $60 billion.29

From FININT to Economic Coercion: Disconnecting Iranian Banks

During this time of escalating sanctions pressure, Iran continued to refuse to cooperate with the International Atomic Energy Agency (IAEA) or to address concerns raised in U.N. Security Council Resolutions, and rejected a proposal in October 2009 to export its 20 percent enriched uranium for reprocessing and fuel fabrication for the Tehran Research Reactor. Iran continued to support U.S.-designated terrorist groups including Hezbollah, Hamas,30 and, as Treasury revealed, even al-Qaeda.31

As Iran's nuclear program moved ahead, policymakers looked to Treasury for new innovations in tools of cyber-enabled economic warfare. Although the value of SWIFT data was recognized as a key source of financial intelligence, until early 2012, its value as a coercive instrument of economic warfare was not understood fully.

Financial institutions and multinational companies have long been responsible for knowing their customers, but SWIFT was the exception. SWIFT was treated like a simple messaging service responsible neither for the contents of the message nor for the actions of the sender or receiver.

In 2011, responding to increased international attention on more effective sanctions enforcement, SWIFT announced it had implemented a screening program to allow its customers to route messages through an application that checks the information against a


selected sanctions designation list.32 At the time, SWIFT claimed that it “manages the screening engine and is responsible for configuring and maintaining the screening algorithm.”33 However, the option of which lists to use was left to the discretion of each individual user,34 and the use of the screening system was not mandatory for SWIFT clients. The screening program was a tool for SWIFT members to do their own due diligence, but SWIFT was not responsible if its customers used its messaging system to engage in illicit financial activities.

Developments over the next six months would begin to change the way policymakers saw SWIFT’s role. After 9/11, Section 311 of the USA PATRIOT Act gave Treasury new authority to designate illicit financial actors as entities of “primary money laundering concern.” While a Section 311 regulation advises only U.S. banks to end relationships with a designated entity and requires no action by foreign banks, the effect is a stark public indictment. While the United States does not order any asset freezes, financial institutions around the world typically freeze assets and close accounts in reaction to a 311 declaration that a bank, for example, is financially radioactive.

On November 22, 2011, expanding on its designations of individual Iranian financial institutions, Treasury issued a Section 311 finding that the entire country of Iran was “a jurisdiction of primary money laundering concern,” citing Iran’s “support for terrorism,” “pursuit of weapons of mass destruction,” and “the 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 (CBI) and made it clear that the country’s entire financial system posed “illicit finance risks for the global financial system.”35

This action against the CBI built on the experience of using “the 311” as part of a full-scale, multifaceted pressure campaign against North Korea that culminated in the September 2005 finding against Banco Delta Asia (BDA), a Macao-based financial institution that enabled a range of illicit financial activities by the North Korean regime. In that case, the designation of a bank that the North Korean regime used to evade sanctions and engage in proliferation-sensitive financing, drug smuggling, money laundering, and other illicit activities spurred the private sector to dump Pyongyang like a toxic asset. Within days of BDA’s designation, North Korean accounts and transactions were frozen or blocked in banking capitals around the world—notably including Beijing.

Treasury’s 311 finding against the Iranian financial sector led to the “Menendez-Kirk amendment,” congressional sanctions under Section 1245 of the National Defense Authorization Act (NDAA) of 2012, targeting foreign financial institutions conducting transactions with the Central Bank of Iran (CBI).36 The legislation blocked the assets of designated Iranian financial institutions, including the CBI. Section 1245 also prohibited the opening or maintenance of any correspondent or payable-through accounts for any foreign financial institution that the president

determined had conducted or facilitated significant financial transactions with the Central Bank of Iran or any other designated Iranian financial institution with narrow humanitarian and crude oil exceptions (that depended on a country “significantly reducing” its volume of crude oil imports). The implementation of these sanctions effectively cut off the CBI from the global financial system and reduced Iranian crude oil exports, which accounted for approximately 80 percent of Iran’s export earnings, from 2.5 million barrels per day to approximately 1 million.37

The Section 311 finding and Section 1245 of the FY2012 NDAA strengthened arguments that SWIFT should be responsible for blocking the financial messaging instructions of designated financial institutions and other related entities. The argument began to build for the expulsion of these designated entities from SWIFT’s messaging service.

By 2012, SWIFT represented one of Tehran’s last entry points into the global financial system, as the United States and the European Union had sanctioned scores of banks, energy companies, and other entities under the control of the IRGC.

Treasury was initially hesitant about the idea of using SWIFT as a tool of economic warfare. Following the backlash in response to public revelations about the Terrorist Finance Tracking Program, Treasury was particularly sensitive to the perception that SWIFT was being politicized in the dispute over Iran’s nuclear program. Treasury did not want to further complicate Washington’s relationship with SWIFT and of the value of its financial data for counterterrorism operations. There may also have been hesitation because of a concern about the loss of financial intelligence into Iranian activities that Iran’s participation in SWIFT provided.

SWIFT’s bylaws required that its “services should not be used to facilitate illegal activities,” and SWIFT was also required to prohibit access if a “user is subject to sanctions.” Moreover, senior executives of the global financial institutions that form the board of SWIFT have the power to expel a user who “has adversely affected … SWIFT’s reputation, brand, or goodwill.”40

SWIFT was also a critical financial gateway to the European Central Bank’s Trans-European Automated Real-Time Gross Settlement Express Transfer (Target2) system. Target2 is the European Central Bank’s proprietary electronic interbank payment system, equivalent to the U.S. Fedwire, and the system that settles transactions in euros through the SWIFT gateway. The ECB’s guidelines were even more specific than SWIFT’s. The guidelines explicitly barred any entity engaged in “money laundering and the financing of terrorism, proliferation-sensitive nuclear activities

and the development of nuclear weapons delivery systems.” That fit Iran to the letter.

Target2 was important to Iran because U.S. financial sanctions already had curtailed much of Iran’s dollar-denominated business. In response, Tehran relied increasingly on the euro, the world’s second largest and most liquid currency reserve holding. The regime shifted part of its foreign exchange reserves to euros and began denominating a substantial portion of its international trade contracts in euros.

In early 2012, as discussions about SWIFT’s role in enforcing sanctions intensified, SWIFT responded to challenges about its compliance with international sanctions against Iran by stating that “all decisions on the legitimacy of financial transactions under applicable regulations … rest with financial institutions and the competent international and national authorities.” However, SWIFT provides more just the “envelope and postage stamp” for a financial message and more than mere technical assistance. SWIFT provides the prerequisite codes that allow financial institutions to process a transaction.

Determined to block Iran from SWIFT, U.S. policymakers and EU regulators now focused on clarifying that financial messaging services fell under existing authorities regarding Iran sanctions. The Senate Banking Committee began working on an amendment to sanctions legislation that ultimately became the Iran Threat Reduction and Syria Human Rights Act (ITRA) of 2012. Co-authored by Senators Robert Menendez (D-NJ) and Roger Wicker (R-MI), and inspired by Senator Mark Kirk (R-IL) who was recovering from a stroke at the time, the amendment provided the administration with the authority to sanction financial communications services providers, including SWIFT, servicing European Union-designated financial institutions. The amendment was adopted into the legislation, and passed out of committee on February 2, 2012.

The Obama administration sought to persuade key legislators that it was better positioned to pursue this matter quietly rather than having Congress adopt punitive measures against a critical global financial actor like SWIFT. However, as in other cases of sanctions against Iran, congressional pressure proved to be useful leverage in persuading international companies and governments to pass and enforce their own sanctions.

Six weeks after the Senate Banking Committee’s actions, the European Union Council clarified that “no specialized financial messaging shall be provided to those persons and entities subject to an asset freeze.” EU regulators instructed SWIFT to remove specified Iranian banks from the SWIFT network. SWIFT’s chief executive Lázaro Campos announced that the consortium would remove Iranian banks from its system noting that, “disconnecting banks is an extraordinary and unprecedented step for SWIFT. It is a direct result of international and multilateral action to intensify financial sanctions against Iran.”

While the expulsion from SWIFT of most Iranian banks was ultimately a direct consequence of EU regulations, the threat of U.S. sanctions played an important role in persuading the EU to “de-SWIFT” a number of these banks.

The Impact of “De-SWIFTing” Iran

The ban from SWIFT was not total, however. The Treasury Department, in an attempt to leave open a channel for humanitarian funds to reach Iran and to avoid measures that would unduly harm the Iranian people, intentionally left a handful of Iranian banks undesignated and, therefore, not targeted for SWIFT disconnection.

Treasury officials and EU regulators assured the international community that they would keep an eye on both designated and undesignated banks and prevent illicit funds from moving through the SWIFT system.

Despite these assurances, a December 2013 corruption scandal in Turkey revealed that Iranian banks were still using SWIFT for illicit financial transactions. According to a leaked prosecutor’s report, Iran’s Pasargad Bank, Parsiyan Bank, Sarmaye Bank, Bank Tos-e-Sadarat, Karkafarin Bank, and Saman Bank allegedly processed sanctions-busting transactions for the network of Turkish-Iranian businessman Reza Zarrab, who allegedly processed more than €87 billion in illicit transactions between 2012 and 2013. The corruption scandal quickly became politicized as the probe implicated ministers, their family members including Prime Minister Recep Tayyip Erdogan’s son, and politically connected businessmen including the head of state-owned Halkbank. The AKP government responded to the allegations with a “wholesale replacement of police, prosecutors and judges.” A number of police officers who had been involved in the investigation were later arrested on charges of “attempting a coup.” Anti-corruption NGO Transparency International said the subsequent decision by the new prosecutors to drop the charges “calls into question the rule of law in Turkey.”

The Organization for Economic Co-operation and Development (OECD), an organization of 34 advanced

Following the provision in ITRA regarding SWIFT, Congress inserted a similar measure banning Iranian banks from accessing Target2 in the Nuclear Iran Prevention Act of 2013 (H.R. 850), which passed the House of Representatives in July 2013 by a vote of 400-20. The Senate companion legislation, the Nuclear Weapons Free Iran Act of 2013 (S. 1881), contained similar language. This legislation garnered the 60 co-sponsors needed for cloture and reportedly had support from a veto-proof majority of the Senate. However, the legislation stalled following the election of Iran’s new president Hassan Rouhani, the start of P5+1-Iran nuclear negotiations in Geneva, and a direct threat from President Obama to veto the legislation.

Despite implementation problems, and stalled new legislation, the expulsion of most Iranian banks from SWIFT successfully limited Iran’s ability to access the global financial system. SWIFT had become a cornerstone of international sanctions.

Meanwhile, another loophole had emerged. A year after the “de-SWIFTing,” of the Iranian banks, it was revealed that some Iranian banks were still accessing Target2. U.S. lawmakers began pressing EU regulators to block Iranian government entities and their affiliates “direct or indirect” access to Target2 in order to prevent Iran from using its “foreign-held euros.”

---

critical part of the multiyear effort to persuade scores of foreign banks to restrict Iranian access to global financial markets and further demonstrated the influence of Congress, which had successfully targeted Iran’s financial, energy, shipping, and insurance sectors and crude oil exports. These sanctions applied greater pressure on the Iranian leadership than anything in the previous decades. Iranian leaders particularly understood the damage to their economy from the SWIFT cutoff. During multiple rounds of nuclear negotiations since the fall of 2013, Iranian negotiators reportedly have demanded that SWIFT be included as one of the first Western sanctions to be reversed.65

**Contemplating Russia**

The Iranian sanctions playbook became a model for policymakers to respond to other international crises. With Russia’s annexation of Crimea and invasion of eastern Ukraine, policymakers re-opened that playbook for applicable economic warfare tools to persuade market players to voluntarily cut their business ties with Moscow.

To date, U.S. and EU governments have cautiously imposed calibrated sanctions to inflict steadily increasing costs while signaling to Russia and market players that there is more to come. With its closer integration into the global economy and greater scope for retaliatory measures, Russia however was a much larger and more difficult target than Iran. As a result, the U.S. and EU have been slow to impose broad, sector-based sanctions on Russian oil and gas, block Russian access to the global banking sector, or target Russian arms exports. There is genuine concern that Russia could retaliate by cutting off natural gas exports to Europe, freezing or appropriating the assets of Western businesses operating in Russia, or launching cyberattacks against Western business interests. Russia could also expand import bans on EU and U.S. goods, restrict commercial air traffic over Siberia, suspend U.S. and NATO access to the Northern Distribution Network to Afghanistan, and serve as a financial outlet or supplier to rogue regimes, with the potential use of Russian banks by Iran and North Korea. Russia could deliver advanced weapons systems, like the anti-aircraft S-300s, to Iran and Syria, weapons systems for which these countries previously had contracts.66 Moscow could also respond to U.S. and EU sanctions by undermining the P5+1 nuclear negotiations with Iran through Russian support for Tehran’s negotiating positions or sanctions-busting Russian-Iranian economic deals.

Obama administration officials have maintained that the crisis in Ukraine and the Iranian negotiations with the P5+1 are completely separate and that they are not concerned that Russia will undermine the nuclear negotiations and the international sanctions regime. However, reports of a $20 billion oil-for-goods deal between Moscow and Tehran indicate that both Russia and Iran are keeping their options open.67 Russia also built and supplies the fuel for Iran’s Bushehr Nuclear Power Plant after German company Siemens abandoned the project following the 1979 Revolution.68 Moscow has outstanding contracts with Iran to provide surface-to-air defense missiles and other military goods and is providing diplomatic, economic, and military support


to Bashar Assad in Syria. Russia has also repeatedly provided diplomatic cover for the Assad regime at the United Nations and prevented the passage of multiple U.N. Security Council Resolutions. Indeed, following the passage of U.S. legislation authorizing additional sanctions and the provision of lethal aid to Ukraine and the announcement of designations of Russian human rights violators at the end of December 2014, the Russian Foreign Ministry spokesman warned that sanctions “are putting in doubt prospects for bilateral cooperation on solving the situation around the Iranian nuclear program, the Syrian crisis and other acute international problems.”

Starting in March 2014, following Russia’s invasion of the Crimean peninsula, the United States and European Union began implementing measures to pressure Russia politically and economically. Efforts began by designating individuals directly involved in the invasion of Crimea, and later those directly involved in the rebellion in eastern Ukraine including separatist leaders, officials of the Russian intelligence and government, and oligarchs closely connected to President Vladimir Putin. These individuals were subject to asset freezes and visa bans. The United States issued three executive orders in March 2014 (and a fourth in December) outlining these restrictions. At the same time, the Group of Seven (G-7) countries announced that they would not attend the planned G-8 summit in Sochi but instead would hold meetings as the G-7 in Brussels. The announcement effectively kicked Russia out of the group.

On March 20, the United States sanctioned the first Russian bank, Bank Rossiya, under Ukraine-related sanctions. The “deeply obscure but hugely powerful” bank is reportedly “the personal bank for senior officials of the Russian Federation” and its “shareholders include members of Putin’s inner circle.”

Over the next several months and especially following the downing of Malaysia Airlines Flight MH17, which killed 298 people, the European Union and United States began restricting exports of dual-use goods, and certain technologies for Russia’s oil sector related to deep-water, arctic offshore, and shale exploration and

production operations. Initially, these restrictions, however, excluded natural gas and applied only to future military sales, not existing contracts.

As the situation continued to deteriorate—and following a de facto Russian invasion of Ukraine—Western countries began looking for additional ways to pressure Putin to respect Ukraine’s sovereignty and territorial integrity. On September 12, 2014, the United States and Europe announced additional sanctions targeting Russia’s financial, defense, and energy sectors. The U.S. Treasury expanded sanctions on Russia’s financial institutions, including Russia’s largest bank Sberbank, on Russia’s energy sector, and on the Russian defense sector. The measures restrict the ability of designated Russian banks to obtain credit, and the energy-sector related measures apply not only to future contracts but also to existing business, providing U.S. firms only two weeks to cease relevant business interactions. These sanctions built on debt and equity restrictions that the United States began implementing over the summer, and addressed the gap between designations by the United States and those by Europe, which had designated Sberbank in July. The sanctions will affect Russia’s access to Western technology and services that are needed to develop Moscow’s medium- to long-term oil exploration and production capacity.

However, notably absent from U.S. and EU designations has been Russia’s state-owned arms exporter, Rosoboronexport, which plays a leading role in Russian weapons provisions to Ukrainian rebels, the Assad regime in Syria, and the government of Iran. The Bush administration had previously sanctioned Rosoboronexport in 2006 for assisting Iran’s nuclear program, but all sanctions on the company expired in May 2010. Despite pressure from Congress to sanction Rosoboronexport, the Treasury Department has not taken steps against the company in large part because of existing Defense Department contracts to provide helicopters to the Afghan military.

Were U.S. officials to contemplate mirroring the Iran sanctions architecture, a next step in the sanctions escalation might be the issuing of a Section 311 finding against a Russian bank found to be financing the...


government’s support for the rebels in the illegal invasion of eastern Ukraine, Russia’s support for and weapons exports to President Assad in Syria (which violates U.S. and EU sanctions against Damascus), or other examples of illicit financial activity including money laundering and proliferation-sensitive financing in contravention of U.S. law. In accompanying statements, U.S. officials could indicate that other Russian banks are being investigated for similar conduct and that there are concerns that the entire Russian financial sector might be a jurisdiction of primary laundering concern.

U.S. officials could then partner with their EU counterparts and other members of the Financial Action Task Force (FATF), a financial standards body comprised of 34 members plus the European Commission and the Gulf Co-operation Council, to issue warning notices to foreign financial institutions about Russian money laundering concerns. As both international economic sanctions and global financial standards gained prominence, this international body, whose focus on combating the classic money laundering schemes of drug cartels and organized crime, was retooled to build international standards surrounding terrorist financing and proliferation. If Moscow’s financial sector failed to implement anti-corruption and anti-money laundering measures, FATF could decide to issue a notice adding Russia to the “gray list” of countries with money laundering and terror finance deficiencies. Unlike Iran, however, Russia is a member of one of the “FATF-Style Regional Bodies,” and thus this may need to be factored into the strategy vis-à-vis any FATF statements on Russia.

Meanwhile, Congress could begin—and, indeed, already has begun—discussing financial and sector-based sanctions like those found in CISADA. This legislation would ban investments in key sectors of the Russian economy and would designate foreign financial institutions doing business with blacklisted Russian companies. Senator Mark Kirk (R-IL) has drafted legislation mirroring some of the measures imposed on Iran, including sanctions targeting the Russian central bank and Russian access to SWIFT. His involvement this draft legislation is especially notable as he is the co-author of many of the most stringent sanctions against Iran.

While EU governments have not yet considered measures like those contained in Senator Kirk’s draft legislation, there are reports that they may be looking at SWIFT as a possible alternative tool. The British government reportedly has been pressing its EU partners to remove Russian banks from the SWIFT system and tabled the issue at an EU ministers meeting at the end of August 2014. Other members of the EU, however, have been more hesitant to the support punitive measures against Russia, and the bloc has not yet taken action to remove Russian financial institutions from the SWIFT system.

“De-SWIFTing” even one Russian bank would have far reaching consequences for the Russian economy. Coupled with removal from the Target2 euro clearing system, the exclusion of a small number of already

designated Russian banks from SWIFT would have painful consequences for Moscow. If implemented, this could be legitimized as an essential regulatory step to protect the integrity of the financial system from Russian banks whose illicit financial activities explicitly contravene the bylaws of both SWIFT and Target2. However, the use of SWIFT as a financial sanctions tool carries certain risks that will be discussed in more depth in the next section.

As Russia’s economy has dramatically declined in recent months, its leadership and central bank have intervened not only to try to stem inflation but also to provide a mechanism for companies—including designated entities—to refinance their foreign debt. The Russian leadership understands the significance that such a de-SWIFTing would have for the economy and Russia’s ability to transact with global markets. Andrei Kostin, head of Russia’s state-owned VTB Bank, warned that de-SWIFTing Russian banks would be tantamount to a declaration of war. “In my personal opinion it would mean war—if this type of sanction will be introduced… If Russian banks’ access to SWIFT will be prohibited, the US ambassador to Moscow should leave the same day. Diplomatic relations must be finished. Banking is the most vulnerable part of the Russian economy because the system is based so strongly on the dollar and the euro,” he said. Russian experts believe that this statement likely reflected President Putin’s perspective as well given Kostin’s close relationship with the Russian leader. Reportedly, Kostin is Putin’s close friend, a member of the board of Rosneft, and Putin’s second-most consulted adviser.

The U.S. Treasury also added VTB Bank to its Sectoral Sanctions Identification list prohibiting U.S. persons from transacting in debt of longer than 90 days maturity with VTB Bank.

It is debatable whether sanctions will affect Moscow’s political calculations or have been a key driver of Russia’s current economic difficulties. While the ruble lost half of its value in 2014 and the Russian central bank projects that the economy could shrink by 4.7 percent next year, Russia has yet to reverse its policies on Ukraine. It is also not clear how much of the crisis in the Russian economy is a result of the sanctions, structural problems in the Russian economy, or the drop in oil prices from $110 in July 2014 to under $60 per barrel in January 2015. As former U.S. Ambassador to Russia Michael McFaul noted, “Sanctions raise uncertainty about the Russian economy. Their own minister of economic development said today that the ruble is falling faster than the macroeconomic indicators would suggest it should.” Russia’s Finance Minister Anton Siluanov, however, has said that sanctions are costing Russia $40 billion per year and that the drop in oil prices is costing between $90 and $100 billion per year.


The impact of the price of oil on the Russian economy raises questions—beyond the scope of this study—about the extent to which U.S. policymakers can influence market prices as well as restricting Russian market access through sanctions. While some experts believe that Saudi Arabia convinced OPEC not to reduce production, even as oil prices fell, in order not to lose market share to U.S. shale-oil companies and other non-OPEC producers, others speculate that Riyadh's real target was Iran, with whom the kingdom finds itself at odds throughout the Middle East, from Syria to Yemen. Future economic coercion might include a more active role by the U.S. government in influencing markets; however, such policies could move the government away from a focus on conduct-based economic measures towards the politicization of markets with negative consequences for America's role as a global arbiter of economic activity.

Unlike the sanctions against Iran, sanctions on Russia were crafted in a way to protect specific economic and financial trade flows that the U.S. government deemed essential and areas in which the U.S. government saw specific risks of retaliation. The U.S. government identified a different kind of financial vulnerability, namely the dependence of Russian banks and corporations on external financing. The application of economic tools against a larger, more complex, and more globally integrated economy like Russia's required innovations in sanctions and not just a wholesale application of the Iran sanctions playbook. The complexity of dealing with a target like Russia reinforces the need for the development of a doctrine of economic warfare and the importance of a forward-leaning policy planning process to identify financial vulnerabilities and design appropriate tools to be used against a range of targets. A further discussion of the importance of developing a doctrine of economic warfare is included in Part 3.

The use of economic coercion to achieve national security goals provides the United States with an important policy tool for changing the policy calculations of other countries. However, economic measures should supplement but not replace the use of other coercive measures. To affect not only the Russian economy but also Moscow's political calculations, Western economic warfare must be combined with other means of coercion—from tough diplomacy to covert action to the credible threat of military force or the provision of meaningful military aid to Ukrainians and other Eastern Europeans prepared to fight for their freedom. Offensive economic warfare also must have a defensive component that strengthens Western resiliency against Russian responses.

---

Russian officials have reportedly discussed a SWIFT alternative with their Chinese counterparts. However, it is not clear how quickly such a system could be created and whether major banks outside Russia would be willing to use this alternative system if it exposed them to reputational damage or legal sanction from the U.S. and EU.

Banking experts believe, however, that the creation of an alternative system could have a significant impact on international trade including by making global payments less efficient. If Russia and China created a SWIFT-competitor, the system likely would place less of a priority on monitoring and blocking illicit financial activities and might enable Iran and other rogue financial actors to operate freely.

The elaborate scheme revealed in the Turkish prosecutor’s report, through which Iran moved tens of billions of dollars in illicit funds between Turkey and Iran, also allegedly involved numerous sanctions-busting techniques including “over-invoicing.” This is one of the many classic money laundering techniques, which “allows illegal organizations the opportunity to earn, move, and store proceeds disguised as legitimate trade.” In the Turkish example, a luxury yacht company sold the Iranian Pasargad Bank 5.2 tons of brown sugar for a massively inflated price of about $240 per pound. EU regulators had permitted the Iranian bank, which electronically transferred the illicit funds, to remain on SWIFT to provide a humanitarian channel for Iran’s people. Iran abused this.

In other attempts to skirt sanctions, Iran has reflagged numerous vessels from Islamic Republic of Iran Shipping Lines (IRISL) and NITC (formerly the National Iranian Tanker Company) to places like Tuvalu and Tanzania, and renamed ships repeatedly with non-Farsi names. The objective was to evade international sanctions following the U.S. Treasury Department’s designation of IRISL in 2008 under Executive Order 13382 for “facilitat[ing] shipments of military-related cargo destined for [Iran’s Ministry of Defense] MODAFL and its subordinate entities.” At the time, Treasury noted that IRISL “has deliberately misled maritime authorities through the use of deception techniques” to transport military-related goods and other banned items.

As noted above, sanctions on Iran’s crude oil exports were aimed at reducing government revenue for Iran’s nuclear program and support for terrorism and pressuring the government to cease its illicit activities. As these sanctions were increasing, Iran engaged in


another sanctions-busting scheme. Using ship-to-ship transfers in order to disguise the origin of its crude oil, NITC tankers would move the Iranian crude oil into foreign-owned ships to be sold in Southeast Asia. There were also instances of Iranian crude being blended with other crudes or held in mislabeled barrels.109

These and numerous other sanctions evasion schemes run by Iran and other rogue actors are well documented.110 As a result, the U.S. Treasury Department has created a “Foreign Sanctions Evaders” list as a complement to its Specially Designated Nationals (SDN) list.111

But the U.S. government is always playing catch-up as new schemes emerge and new players willing to take the risks for large profits enter the market. As those unwilling to take risks leave the market, the remaining players exercise their increased market power by negotiating deep discounts, steep premiums, or high commissions to help rogue actors evade sanctions.

The birth of cyber-enabled tools and financial mechanisms present new sanctions-busting opportunities for criminal organizations, terrorists, weapons proliferators, and rogue states.112 Nontraditional, digital, virtual, or peer-to-peer currency that is issued based on a computer algorithm rather than from a national bank—for example, are not subject to the same regulations and reporting requirements (although this is beginning to change) as the traditional financial sector and thus may provide a space for illicit financial activities to flourish.113

New, alternative technologies do not yet pose a realistic, large-scale alternative to traditional financial channels—the commodities market is not pricing barrels of oil in bitcoin nor are companies financing their debt in “Linden” dollars from the popular virtual world Second Life or “Ven,” a digital currency from the social networking site Hub Culture, which focuses on the virtual and physical exchange of goods and services. However, the continued development of new cyber-enabled tools requires proactive engagement with the creators of these financial mechanisms and in-depth policy planning across multiple agencies of the U.S. government to properly assess vulnerabilities. This topic will be explored in Part 3.

Future Threats: The Use of Cyber-Enabled Economic Warfare Against the United States and U.S. Allies

While sanctions evasion threatens the efficacy of economic coercion and requires constant vigilance by enforcement authorities, cyber-enabled economic warfare against the U.S. and its allies is a much greater threat to national and economic security. In the past decade, the United States has been at the forefront of...
using economic warfare against rogue actors, but it can only be a matter of time before adversaries and enemies turn the tables on the U.S. and its allies. Developing an arsenal of defensive tools for America and its allies has become an urgent task.

In an indication of challenges ahead, on October 6, 2014, SWIFT announced that pro-Palestinian organizations had petitioned SWIFT to disconnect Israeli financial institutions and the entire country from its financial messaging system.\(^\text{114}\) SWIFT made the following statement:

> “SWIFT regrets the pressure, as well as the surrounding media speculation, both of which risk undermining the systemic character of the services that SWIFT provides its customers around the world. As a utility with a systemic global character, it has no authority to make sanctions decisions. SWIFT will not respond to individual calls and pressure to disconnect financial institutions from its network.”\(^\text{115}\)

Although SWIFT rejected the pressure and explained that it would not take action without direction from EU regulators, SWIFT would presumably comply, as it did in the Iran case, if the EU designated Israeli financial institutions because they operate in the West Bank and issued orders requiring that SWIFT expel these institutions from its system.

Israel, of course, has been long been a target of economic warfare. Israeli Chamber of Commerce estimates that the Arab boycott, which began more than 40 years ago, has cost the country $45 billion.\(^\text{116}\) On a global scale, the Arab oil embargo of 1973 is estimated to have caused a 4.7 percent decline in America’s GDP and a 7 percent and 2.5 percent decline in Japan’s and Europe’s GDP, respectively.\(^\text{117}\)

Ten years ago, an anti-Israel “Boycott, Divestment and Sanctions” (BDS) campaign began to coalesce.\(^\text{118}\) The United States should view this movement in its broader economic warfare context: The campaign is attempting to persuade corporations and financial institutions to discriminate against the State of Israel, its corporate entities, and its citizens.

The BDS movement and the idea of using tools of economic warfare against Israel appear to be gaining some ground in Europe. In 2012, the EU’s consuls general in East Jerusalem and Ramallah issued a Heads of Mission report recommending sanctions on Israeli settlements,\(^\text{119}\) and in January 2014, PGGM, a large Dutch pension fund, withdrew its investments from Israel’s five largest banks because they have branches in the West Bank.\(^\text{120}\) In November 2014, an internal EU document was leaked to the press. The document included an assessment of what economic sanctions against Israel could possibly include.\(^\text{121}\)

Although the BDS movement and similar efforts are directed against Israel today, such strategies could be employed against other American allies—and the United


\(^{118}\) “Palestinian Civil Society Call for BDS,” *BDS Movement Website*, July 9, 2005. (http://www.bdsmovement.net/call).


States itself—down the road. The strategic assessment and institutional reforms necessary to protect the United States and its allies from economic coercion (discussed in Part 3) should include an understanding of the BDS movement as a manifestation of economic warfare.

In the following scenario, we lay out an unlikely but entirely plausible situation through which SWIFT could become a political football in a regional conflict and a dangerous tool employed by America’s global competitors. This scenario is entirely hypothetical, and the authors have no reason to believe that countries are contemplating the steps outlined below. However, there is also nothing preventing such a scenario.

Hypothetical: SWIFT and the Crisis in the South China Sea

In the South China Sea, the Paracel and Spratly Islands are hotly contested, in part, because of estimates of their significant oil and gas reserves. Although the area has been under-explored due to territorial disputes among China, Vietnam, the Philippines, and others, there may be up to 11 billion barrels of oil reserves and 190 trillion cubic feet of natural gas reserves in the South China Sea.

In recent years, China, Vietnam, and Malaysia have been dredging and enlarging islands and building large structures on newly reclaimed land. China, in particular, is aggressively building up reefs, and the state-owned China National Offshore Oil Corporation (CNOOC) placed its first oil rig in the Paracels in May 2014, sparking anti-Chinese protests in Vietnam and a rare statement from the United States calling China’s actions “provocative and unhelpful to the maintenance of peace and stability in the region.” Although China removed the rig in July 2014 reportedly because it completed the task, additional oil rigs are expected to appear in the South China Sea in the coming years. When China places its next oil rig, increased tensions are likely.

Imagine the following hypothetical scenario:

After typhoon season, China returns its oil rig to the Paracel Islands, announcing its intention to install additional rigs in the coming year. In response, anti-Chinese protests again erupt in Vietnam. To contain the growing unrest and prevent a recurrence of the May 2014 protests that escalated to include other domestic grievances, the Vietnamese government pledges an aggressive response to China’s encroachment on its sovereignty. Hanoi urges the international community to condemn China’s actions and emphasizes its desire for increased cooperation with the United States as part of the “comprehensive partnership.” Meanwhile, Chinese state media is filled with propaganda and negative stories about Vietnam, encouraging already negative populist sentiment about China’s neighbors.

The two nations step up their naval presence around the Paracels and engage in a dangerous game of chicken—coming within 200 yards of each other's vessels and shooting off flares. The Vietnamese government announces that it intends to hold another live-fire drill in the South China Sea, a repeat of its June 2011 exercise. Tensions reach levels not seen since the 1988 Johnson South Reef crisis when 64 Vietnamese border guards were killed in a Chinese naval attack.¹²⁹

Meanwhile, in the Spratly Islands, there has been a dangerous accident aboard the Filipino ship, the *Sierra Madre*. The formerly American, World War II-era ship was scuttled in 1999 by the Filipino navy and has been an important outpost marking Filipino claims to the nearby reef.¹³⁰ Two members of the crew of Filipino marines were seriously injured while attempting to reinforce an area of the ship's near rusted-through hull that had become structurally unsound.

Although the two marines are in stable condition, the decision is made that they require greater medical attention than the crew can provide onboard the ship. The Philippines sends another naval vessel to retrieve and relieve the two injured men, but China repeatedly blocks the ship's attempts to reach the *Sierra Madre*, claiming that the Filipino vessel is carrying military supplies. Although China has previously blocked vessels from resupplying the *Sierra Madre*,¹³¹ tensions on the Paracel Islands prompt a more aggressive response from Chinese vessels, which come dangerously close to ramming the Filipino ship.

The government of the Philippines and its citizens are outraged and request U.S. diplomatic intervention to pressure China to allow the rescue of the injured men. Following private meetings with U.S. officials, Beijing announces that it will send one of its coast guard ships to evacuate the injured marines but on the condition that the rest of the crew also board the Chinese vessel for safe transport back to the Chinese mainland, followed by a flight to Manila. The Philippines refuses China's offer, recognizing that once the marines are off the *Sierra Madre*, China could sabotage the ship, making the marines' return impossible and removing the barrier to Chinese expansion.

The United States continues to try to negotiate a compromise between China and the Philippines, but the Chinese, Vietnamese, and Filipinos become more entrenched as the international press begins to cover the escalating conflict. Although its bilateral Enhanced Defense Cooperation Agreement with the Philippines does not explicitly require a U.S. response to disputes in the South China Sea,¹³² the U.S. administration feels increasing domestic pressure from a wave of press articles and congressional statements about a rising, aggressive China to engage diplomatically to support its ally and stand up to Chinese intimidation. The U.S. administration begins to take a more outspoken approach to the tensions, publicly condemning China's unilateral attempts to change the status quo in the contested region. The United States announces that it is prepared to airlift the injured marines out of the region and that China and the Philippines, and the other nations with claims in the South China Sea, should submit to binding, international arbitration to resolve the territorial disputes and map the lines of each nation's Exclusive Economic Zone.

Outraged by U.S. interference in China's backyard, Beijing reverses its hesitation about using economic


sanctions for geopolitical goals (despite its public opposition to sanctions, China banned exports of rare earth minerals to Japan in 2010\textsuperscript{133} and used economic and diplomatic pressure in the past to challenge international recognition of Taiwan). China has previously been cautious about the use of economic coercion against Washington, recognizing its mutual dependence on the United States. In 2008, China rejected a Russian proposal to jointly sell each of their holdings in Fannie Mae and Freddie Mac, which would have forced a U.S. government defense of the two institutions and dramatically exacerbated the already serious financial crisis.\textsuperscript{134}

Recognizing that direct action against the United State might put its export relationship at risk or cause repercussions for its own economic growth, Beijing decides to employ an indirect approach modeled on the escalation of sanctions on Iran. A direct assault on the U.S. financial system is likely to be unsuccessful given the dollar’s preeminence and would likely also prompt a forceful response from the United States. Instead, China decides to target U.S. allies in efforts to convince Washington to remove itself from the South China Sea conflict and concede to Beijing’s territorial ambitions.

After first announcing a ban on Chinese energy exploration technology provided to the Philippines, Beijing then declares that it is imposing sanctions on the Philippines and secondary sanctions against those foreign companies and banks doing business with designated Filipino entities.

Markets are initially skeptical of this announcement of “CISADA-like” sanctions, but China begins a full-court press urging European companies to cease their business relationships with Manila. China then identifies a few instances of sub-par reporting of suspicious activity by Filipino banks and urges European banks to close euro-denominated accounts for Filipino customers and correspondent accounts for select Filipino banks at which the suspicious activity occurred. China begins simultaneously to exert diplomatic pressure on other members of FATF’s Asia/Pacific Group on Money Laundering\textsuperscript{135} to begin a formal review of the Philippines.

At each stage, the United States and U.S. companies serve as a backstop against a severe impact on the Filipino economy. Initially U.S. companies back-fill those contracts that EU firms relinquish while extracting more favorable terms given the risk premium of doing business in the Philippines. Beijing issues statements warning U.S. firms against these relationships and threatens to ban U.S. firms from the Chinese market if they provide goods and services related to the Philippine’s oil exploration. China does not impose secondary sanctions on American companies, concerned that this step could provoke direct retaliation, and satisfied that the replacement contracts alone are costing Manila.

When European banks begin closing correspondent accounts, Filipino non-dollar trade converts to dollars, and foreign businesses use banks in New York to transact. However, China soon begins pressuring private American banks to close their correspondent accounts or risk losing access to the Chinese financial system. U.S. banks soon comply, acknowledging the vast difference in the economic scale of China versus the Philippines.

As they become more isolated, Filipino leaders appeal to the United States government to intervene and protect their country’s access to international financial markets.


The State Department begins pressing federal bank regulators to find a solution to the current situation. In the past, when foreign embassies were having difficulty accessing banking services because banks were concerned about reputational risk associated with any transactions with certain countries, the State Department intervened and urged banks to accept the accounts. In that case, banking regulators also issued guidance alerting banks that they could accept these accounts and still comply with anti-money laundering regulations. However, in this scenario with China and the Philippines, private banks make their own risk assessments and begin closing accounts. The Fed responds by creating a special mechanism at a Federal Reserve bank through which trade can continue in dollars.

Beijing then turns its attention back to the EU and begins urging EU regulators to issue guidance to SWIFT and to the European Central Bank’s Target2 euro-clearing system to remove designated Filipino banks from the financial messaging systems. When EU regulators initially respond that the behavior of the banks does not reach a threshold to pose a threat to the financial system and warrant removal from the systems, China slows the renewal of select contracts with EU businesses. These companies interpret this initial move as a warning that Beijing may reduce select imports from the European Union, China’s largest trading partner. Meanwhile, strategically placed Chinese ministers and economic advisers raise questions about whether China’s purchase of eurozone junk bonds, particularly those bonds issued by Greece and Italy, are responsible investments. Well-respected economic analysts in Europe and the United States issue reports that a large-scale sale of these bonds would cripple Greece’s fragile economy, damage Italy’s, and undermine the EU economic recovery.

EU regulators assess that the de-SWIFTing of Filipino banks would be a significant inconvenience for Manila but would not have the devastating impact it had on Iran. At the time of Iran’s de-SWIFTing, the country had few remaining access points to international markets. As long as trade can be conducted in dollars, the impact on the Filipino economy would not be profound. Thus unwilling to sacrifice its own economy to save Manila from what is likely to be no more than a costly annoyance, the European Union begins to seriously consider China’s request. Acknowledging that China and other BRICS have taken steps to create an alternative international development bank, EU regulators also assess that China may move forward with an alternative messaging system in direct competition with SWIFT if China’s geopolitical demands in the South China Sea are not met. SWIFT itself expresses strong reservations to the de-SWIFTing but ultimately must adhere to EU sanctions regulations.

The EU pressures Washington to reconsider its support for the Philippines, Vietnam, and other countries

with competing claims over the South China Sea. EU policymakers make it clear to their America counterparts that, in order to protect their bilateral trade interests with Beijing, they may have to consider heightened sanctions against Filipino banks and persons operating in the European Union or European persons operating in the Philippines. Washington is put on notice: If China escalates its economic warfare campaign, the U.S. will have to find a political resolution to the South China Crisis even if it means agreeing to Beijing’s demands.

Although the United States has prevented the worst of the economic impact on its ally, it has paid a high political price—increasing tensions not only with China but also with European leaders. SWIFT has indeed become the political football that the U.S. Treasury Department had feared, and the traditional mechanisms of global financial markets are being called into question.

Is Washington prepared to deal with scenarios, like the SWIFT and the South China Sea crisis, where the tools of economic coercion are turned against the U.S. and its allies? While the scenario described above is a hypothetical and, perhaps, a low-probability scenario, it is useful for understanding the challenges that the United States might face. Could Washington implement “whole-of-government” systems and tools to head off other potential economic warfare scenarios and avoid responding to crises in an ad-hoc and ultimately ineffectual way? What economic and policy planning mechanisms ought we have in place to anticipate and manage such a scenario? How can Washington coordinate with the U.S. and international business and financial community to effectively defend American interests and the interests of our allies? The following section offers recommendations to help develop a better whole-of-government approach to defensive economic warfare.

PART 3: RECOMMENDATIONS

Introduction

The offensive and defensive tools of American economic coercion depend on the power of the U.S. dollar. As long as global finance is structured as it is—with the dominance of the U.S. dollar as the currency of choice for global trade and foreign exchange reserves, and with the U.S. Treasury bill seen as the safest investment even during financial crises—the United States enjoys a strong economic advantage. Despite analysts’ predictions over the past decade and especially after the 2008 financial crisis that the dollar would lose its preeminence, the overwhelming majority, 87 percent,141 of international trade is still conducted in U.S. dollars, 43 percent of international financial transactions are denominated in dollars,142 and about 61 percent of total allocated global foreign exchange reserves is denominated in U.S. dollars.143 Yet, countries are looking at non-dollar options. For example, Chinese UnionPay has taken over nearly half of the global credit card market, with 45 percent of the credit and debit cards in circulation, accepted in 135 countries, and representing 25 percent of transaction volume for the second half of 2012.144

debit cards are delinked from New York, providing an alternative for countries facing U.S. sanctions. When MasterCard and Visa froze accounts in Russia in response to U.S. sanctions, designated Russian banks turned to UnionPay as an alternative. Washington and its allies might be exposed to economic coercion and America’s own financial warfare tools would be blunted if systems that avoid the dollar grow in prominence. Moreover, the International Monetary Fund is working to establish an alternative global-reserve asset, known as Special Drawing Rights, linked to a basket of currencies that would reduce the weight of the greenback and increase the weight of the yuan, explains global-finance expert James Rickards in his book “The Death of Money.” China is beginning to allow an open financial market which might enable the yuan to become a reserve currency, although at the end of 2014 less than two percent of foreign exchange reserves were in yuan. If China is willing to allow greater yuan trade and greater foreign investment in Chinese stocks, the yuan could in the future become a competitor to the dollar and undermine U.S. financial leverage. The combination of a Chinese global credit card, an alternative SWIFT system backed by Russia and China, Chinese and Russian banks willing to defy the global financial order, and foreign trade and exchange reserves denominated in yuan might create that perfect storm.

Another challenge to the U.S.-led global financial order is the BRICS nations’ creation of an alternative development bank and the Chinese-led Asian Infrastructure Investment Bank (AIIB). The latter was conceived as a competitor to the World Bank and was reportedly opposed by the United States. In March, however, U.S. allies including the U.K., France, Germany, and Italy announced their intention to become founding members of AIIB. South Korea and Australia also joined as founding members, along with Sweden, Poland, and Israel, as well as Egypt and Saudi Arabia. Canada is reportedly considering joining the group which includes 16 of the world’s 20 largest economies. The exclusion of Taiwan despite its desire to join indicates that China recognizes the political significance participation in this new club.

For that reason, it is especially noteworthy from an American perspective that Iran has been accepted as a founding member even as it continues to face financial sanctions for illicit financial activities. Russia, with whom the United States increasingly finds itself at odds, is also a member. The inclusion of these two nations ought to raise concerns in Washington about whether China may be able to loosen the financial pressure the United States has worked to construct.

It may be too early to judge the impact of AIIB, but U.S. Secretary of the Treasury Jack Lew noted that, “new players are challenging U.S. leadership in the multilateral system.” He and his colleagues at the Treasury have also repeated emphasized the need for new institutions to adhere to international standards “regarding governance and environmental and social safeguards.”

International anti-money laundering and counter threat finance standards should also be of paramount concern. Thus, the development of alternative multilateral development banks and other international financial institutions ought to demand serious study to determine the possible effects on U.S. economic power projection and to devise possible countermeasures by the United States to mitigate undesirable consequences.

Based on our discussions with government officials and private sector experts, neither the U.S. government nor the private sector has engaged in serious planning about how to protect America and its allies against economic warfare. As the hypothetical scenario in Part 2 indicates, although other countries may not have the ability to affect the macroeconomic landscape in as profound a way as the United States, Washington can still be forced to make difficult political and economic choices when confronting the use of economic warfare against its interests.

New thinking and new structures are needed to effectively engage in defensive economic warfare. In response to the development of offensive missiles and then missile defense shields, the United States created a Space and Missile Defense Command. In response to the proliferation of cyberattacks, both by the U.S. against its adversaries and by its adversaries against the U.S. and its allies, Washington created a U.S. Cyber Command, crafted a Department of Defense “Strategy of Operating in Cyberspace,” and is expanding CYBERCOM even as the Pentagon, like the rest of the federal government, is facing budget cuts. The evolving power of economic warfare, including cyber-enabled economic warfare, and the willingness of countries like Russia, China, and Iran to devote significant state resources to their offensive

cyber capabilities mean that America’s adversaries could one day bring down a country’s financial system or disrupt millions of miles of critical infrastructure. As it develops cyber command capabilities and defenses, the U.S. government ought to be developing defensive and offensive economic warfare capabilities now rather than waiting for a crisis to occur.

First Phase: Organizational Rearrangement

In our consultations with U.S. government experts, we have identified three initial changes in organizational structure and legal authorizations for the U.S. to more effectively engage in strategic planning on economic warfare. As part of this initial phase, baseline assessments of U.S. vulnerabilities and existing institutional structures should be undertaken immediately within existing institutional structures without waiting for institutional reform.

These initial changes, and the broader reorganization discussed in the fourth recommendation below, are primarily, although not exclusively, focused on questions of the use of financial sanctions but are also likely to have an impact on broader policy and doctrinal discussions on the broader use of economic warfare strategies. This larger conversation within the U.S. government about the full range of offensive and defensive economic warfare capabilities may yield additional institutional reforms, which are beyond the scope of these recommendations.

1. Create an Office of Policy Planning at the U.S. Department of the Treasury

Unlike the State Department and the Pentagon, the Treasury Department does not have an office responsible for policy planning. The priorities of the policy planning office at the State Department are focused elsewhere. Additionally, as with many bureaucracies, the State Department must balance regional and subject matter experts, career civil servants and political appointees. Those with economic expertise have historically not played leadership roles in the State Department. Instead, Treasury should have its own policy planning office to examine economic statecraft, economic warfare, and other challenges. The office should report directly to the Secretary of the Treasury. The Treasury has the resources and expertise to take the lead in this area.

This new Office of Policy Planning would emphasize creativity in the development and deployment of new economic tools. It would assemble experts from different offices throughout the department who can bring different expertise and assets to the table, including specialists from the Office of Foreign Assets Control (OFAC)—the office in charge of U.S. sanctions programs—to examine technical regulations and financial sanctions enforcement; experts from the Office of Terrorism and Financial Intelligence (TFI), including those from the Office of Terrorist Financing and Financial Crimes (TFFC) to focus on illicit finance; those from the Office of Intelligence and Analysis (OIA) to share financial intelligence; and the financial crimes experts from the Financial Crimes Enforcement Network (FinCEN); as well as professionals from Treasury’s International Affairs office to consider economic warfare and its impact on global markets, financial trading, and other macroeconomic systems. As we have seen in the application of sanctions on Russia, the intra-agency exchange can create valuable innovations in economic warfare tools. For example, Treasury economists working in international affairs understood the dependence of Russian corporations on external financing while Treasury’s sanctions experts knew how to leverage the existing legal authorities to develop new targeted sanctions. The Office of Policy Planning would also build and expand on Treasury’s relationship with Congress, which has been a key driver behind the secondary sanctions on Iran. The Office of Policy Planning would also work closely with economic and
finance officials in Europe—who developed some of the most creative ideas regarding Russia sanctions because of their countries’ own exposure and vulnerabilities—and with foreign ministries around the world.

In the creation of the Iran sanctions architecture, the private sector also played a vital role. The power of “smart sanctions” derived from deep cooperation and interaction between the government and private financial institutions. While TFI would continue to drive the implementation of tools of economic warfare, and its relationships in foreign banking capitals would remain paramount, the new Office of Policy Planning should develop long-range strategies on how to incentivize the private sector to build on the already extensive and effective collaboration and deepen its cooperation with the U.S. government. Treasury’s tax, domestic finance, and trade experts, for example, have a valuable role to play in thinking through these strategies.

In today’s environment, the creation of a new office would face budgetary challenges. However, Congress’ willingness to provide funding for the Treasury Department, specifically TFI, is an exception. In the past, Congress played an important role by authorizing the formation of OIA and driving the creation of TFI, even ahead of White House wishes. In April 2014, at the Senate Appropriations Financial Services Subcommittee hearing on TFI’s budget, it was striking how many senators, from both sides of the aisle, asked Undersecretary David Cohen what other resources they could provide. Building on that support, Treasury and Congress should work together to find the necessary budgetary flexibility and funding to create this new office. To create an Office of Policy Planning at Treasury, Congress again should be relied on to do some of the heavy lifting.

2. Set Up an Economic Coercion Directorate at the National Security Council

In addition to more resources within the Treasury Department, U.S. officials have told us that the White House itself needs more staff members who have in-depth understanding of economic tools and view economic coercion as a central component of national security policy making. As the institution that calls, sets the agenda for, and invites participants to inter-agency meetings, the National Security Council needs to play a role in strategic planning around the use of economic warfare tools. The NSC has a directorate of international economics, and thus from this directorate—as a subcomponent or as a reconfiguration of its priorities—a directorate of economic coercion ought to be created. This directorate would also need to interact and coordinate with the National Economic Council (NEC) within the White House because of the important role that the NEC plays in providing advice on domestic and global economic policies.

It is vital that Treasury officials are detailed to, and play a leading role in, this new directorate to ensure that Treasury’s resources and expertise on economic suasion are used effectively in inter-agency settings. This directorate would focus broadly on economic coercion and would need to cooperate and perhaps have a permanent cross-directorate mechanism with other experts in the NSC to address specific cyber-enabled offensive and defensive economic warfare.

In addition to budgetary challenges, as we understand from our conversations with U.S. government officials, this new directorate may run up against the orthodoxy within the government that is pro-trade, pro-investment, pro-development, and pro-business. The U.S. government has traditionally been more...
focused on how open markets can create political opportunity than on how countries should be isolated from the global economy. For example, rather than thinking about tools of economic coercion that might dissuade Russian aggression toward Ukraine, the U.S. government has focused on what support the International Monetary Fund might provide to Ukraine to help Kiev balance its budget. Despite the leading role that sanctions are playing in today’s national security policy—Treasury is reportedly President Obama’s “favorite noncombatant command”165—we are told that there remains a groupthink within the U.S. government that sanctions don’t work and that they hurt innocent people. Tools that restrict economic and financial flows are dismissed and are traditionally sidelined in favor of tools that aid economic growth. A restructuring of the NSC directorate to also include those who have expertise in economic coercion may begin to change this way of thinking.

3. Create a Doctrine on the Use of Economic Coercion

Thus far, sanctions have merely been a tool. Economic coercion has not taken a central role in economic policy planning from an offensive or defensive position. While this is changing with the increasing profile of TFI’s role in addressing national security crises,166 we are told that too few officials outside TFI and select members of the NSC, State, Commerce, and threat finance specialists at the Defense Department truly understand these tools.

The new Office of Policy Planning and Economic Sanctions Directorate should develop and articulate a doctrine on the use of economic coercion. This doctrine could provide a framework for strategic evaluation of when, and how, economic coercion can be effective in policy relevant timeframes. The Defense Department has well-developed doctrines on the use of military force, and it is creating a cyberwarfare 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 warfare. The Pentagon has created clear rules of engagement on the use of the tools at its disposal, and so should the Treasury Department and NSC.

For at least the first three years after the creation of CYBERCOM, the Command was reportedly still heavily focused on the development of policy and legal frameworks.167 Although the Pentagon had issued its Strategy for Operating in Cyberspace in 2011, the 2010 National Security Strategy had stated that cyber threats are “one of the most serious national security, public safety, and economic challenges,”168 and the 2010 Quadrennial Defense Review had noted that cyberspace is “as relevant a domain for DoD activities as” traditional arenas,169 the creation of offensive and defensive doctrines of cyberwarfare was still a multiyear process. In 2012, President Obama signed “Presidential Policy Directive 20,” establishing secret


guidelines for offensive and defensive cyber action, however statements from U.S. officials including President Obama in response to the North Korean hacking of Sony Pictures, reveals that there is not a clear definitions of cyberwarfare, cyberterrorism, or “cybervandalism.”

Recognizing that the creation (let alone implementation) of government-wide doctrines requires significant resources, coordination, and time, it is important that the process to develop a “Doctrine on the Use of Economic Coercion” begins immediately, as a precursor to the creation of an Economic Warfare Command, as discussed below.

The development of a doctrine may also help the United States in broader, international discussions about the application and legitimacy of economic warfare and to defend against the use of these tools in unacceptable ways by America’s adversaries. In developing a system of rules and norms to govern the use of economic warfare, as it has for the use of force and is developing in the cyber realm, the U.S. can bolster its defenses against the unacceptable use of economic coercion.

Second Phase: The Creation of an Economic Warfare Command

In addition to mechanisms to address the use of economic warfare, a more system-wide change should be considered to develop an Economic Warfare Command, ECONCOM. This Command would become the locus for developing and leveraging offensive coercion and incentive tools and for devising and building proactive strategies of economic defense. Housed at the Treasury Department and led by TFI with close coordination with the Treasury Office of Policy Planning, this new command would coordinate and draw assets from within Treasury and across the federal government. Placing ECONCOM at Treasury would be unique as even CYBERCOM, which is led by the director of the National Security Agency, is housed within the Department of Defense.

More so than perhaps any of the other commands, ECONCOM would depend on the participation of a wide range of officials, who would be detailed to the Command from throughout the government. ECONCOM would also depend on its ability to requisition additional assets from agencies and therefore must be given the authority to requisition assets. We recommend housing ECONCOM at the Treasury Department not because Treasury has exclusive expertise on tools of economic coercion but because the U.S. Treasury’s mission includes protecting the integrity of the global financial system. The international community’s, and specifically foreign financial institutions’, understanding and acceptance of this particular component of Treasury’s mission has been important for isolating illicit financial activity and rogue actors identified by Treasury. Building on Treasury’s reputation will likely be important for ECONCOM’s success.

With Treasury in the lead, ECONCOM would require the coordination of a number of key assets. The Commerce Department’s Bureau of Industry and Security would provide expertise on export control issues and the U.S. Trade Representative on issues of U.S. trade relationships. Homeland Security Investigations (HSI) would provide assets related to illicit procurement and customs enforcement, and the Drug Enforcement Agency (DEA) would bring its significant investigatory and intelligence skills into illicit
build a close working relationship with the DOJ as well as closely coordinate with the Superintendent of Financial Services (New York’s financial regulator), who has prosecuted banks for sanctions violations, and the Manhattan District Attorney’s Office and the office of the U.S. Attorney for the Southern District of New York, which have also played leading roles in terrorism and sanctions-related cases.

The Economic Warfare Command would also require a large intelligence component, drawing on assets from across the intelligence community. Treasury’s OIA has traditionally been a consumer and analyst rather than a collector of intelligence although it plays a leading role in the intelligence community’s counter-threat finance efforts. While OIA would continue to play a leading role in the analysis of FININT, the Director of National Intelligence would need to coordinate across the CIA, DIA, and other intelligence agencies to ensure that their agents and analysts are collecting FININT and other useful intelligence for analysis by OIA and others. Conversations with former U.S. government officials in unclassified settings indicate that this coordination is already ongoing and effective.

In addition to offensive financial sanctions like those we have seen from Treasury in the past decade, the new Command would address the broad scope of U.S. economic persuasion and coercion—both offensive and defensive measures and tools of both isolation and inclusion. Coordination between financial and economic experts from Treasury with cyberwarfare experts at CYBERCOM would likely be necessary for the development and implementation of offensive and defensive cyber-enabled economic warfare tools. The two very different perspectives that these experts would bring to policy discussions would likely be a force multiplier of what each could develop and implement separately. Discussions about CYBERCOM’s relationship with the


private sector—as well as Treasury’s experience working with SWIFT to create the Terrorist Finance Tracking Program—can also help inform ECONCOM’s development of relationships with the private sector.

U.S. Cyber Command was initially created as a sub-command of the U.S. Strategic Command and is scheduled to become a full, unified command by the beginning of 2015.174 Explaining the importance of this step, then-NSA Director and head of CYBERCOM Gen. Keith Alexander testified before a House Armed Services Committee hearing that the main reason is “command and control, directly from the President and the Secretary [of Defense], directly to that commander.”175 A similar lesson should be applied to ECONCOM—that it should be a full, unified command so that the leadership has direct chain of command to the president.

Unlike CYBERCOM, which was—in part at least—built on more than a decade of military engagement with cyber and information warfare against the United States,176 ECONCOM has less precedent from which to draw; economic warfare has been overwhelmingly offensive not defensive.177 The creation of this command, however, depends on creativity and innovation on the part of policymakers to analyze and prepare for over-the-horizon threats.

CONCLUSION

Cyber-enabled economic warfare tools like the SWIFT financial messaging system have reshaped the mechanisms and levers of global statecraft. Economic sanctions had been dismissed for decades as ineffective until the debate shifted following the implementation of smart sanctions against Iran as a result of its illicit financial activities in support of its nuclear program and international terrorism. The ever-tightening financial isolation of Iran, including the first-ever expulsion of a country’s banks from SWIFT, changed Tehran’s tactics from nuclear defiance to international negotiations (whether or not this economic pressure however will change Iran’s objective of a nuclear weapons capability still remains to be seen178). The use of sanctions against Iran, Russia, Syria, and non-state actors such as al-Qaed, the Islamic State, Hezbollah, Hamas, and others demonstrated that economic warfare can be an important tool but cannot work in isolation; it is one instrument to be wielded in conjunction with the full range of national power to address national security threats.

Over the past decade, the United States government—led by the U.S. Treasury with vital input and pressure from Congress—has developed its economic warfare offensive capabilities but neglected defensive planning. With the challenge by states such as China and Russia to the U.S.-led international order, including to the preeminence of the U.S. dollar, economic warfare against the United States and its allies is a growing threat. While U.S. legislators and British officials

177. During World War II, the United States and Britain had offices of economic warfare. Exploring lessons from this period as they apply in the modern context would likely provide fertile ground for additional analysis.
contemplate de-SWIFTing Russian banks, Russian officials are considering creating an alternative SWIFT system with Chinese cooperation, to create a financial network that is unlikely to meet high standards of financial integrity. Meanwhile, Palestinian activists are pressuring SWIFT, so far unsuccessfully, to expel Israeli banks, raising concerns that SWIFT may become a political football.

A whole-of-government approach to hardening defenses against economic warfare is required to protect America and its allies. If we can envision a hypothetical scenario involving the use of SWIFT in a crisis in the South China Sea, in which economic warfare becomes a threat to U.S. interests and allies, our enemies no doubt can as well.
Acknowledgments

This report is included in the monograph, “Cyber-Enabled Economic Warfare: An Evolving Challenge,” edited by Dr. Samantha Ravich and published by the Hudson Institute. We are grateful to Samantha for her vision in leading a project on the future challenges, threats, and opportunities associated with cyber-enabled economic warfare. Without her leadership, we may never have been inspired to write this paper.

We would also like to thank her for assembling a top-notch team of experts to provide comments and discussion on each of the chapters in the monograph. The roundtable conversations that she facilitated were extremely constructive. In particular, we would like to thank chief respondent Michael Shrage and Doug Feith, who served as the respondent on our chapter.

The paper was also greatly enhanced by conversations with distinguished scholars and practitioners. We owe a debt of gratitude to FDD’s Center on Sanctions and Illicit Finance Chairman and Senior Counselor Juan Zarate, the first ever assistant secretary of the treasury for terrorist financing and financial crimes; Peter Harrell, former deputy assistant secretary of state for counter threat finance and sanctions in the Obama administration; Leonard Schrank, former CEO of SWIFT; Jonathan Schanzer, FDD Vice President for Research and former Treasury terrorism finance analyst; and Emanuele Ottolenghi, an expert in Iran sanctions. They each provided invaluable insights and suggestions throughout the process. The final report is stronger as a result of their contributions. We would also like to thank the U.S. government interlocutors who shared their expertise and perspective on these important issues. These conversations informed the overall direction of the report. While each of these experts helped us to refine the paper, any remaining errors of fact or judgment are exclusively our own.

Finally, we are grateful for our colleagues at the Foundation of Defense of Democracies. We would like to single out Laura Grossman for her invaluable editing and research skills and Erin Blumenthal for the design and production of this report.
About The Authors

**Mark Dubowitz** is executive director of the Foundation for Defense of Democracies, a Washington, D.C.-based nonpartisan policy institute, where he leads projects on Iran, sanctions, and nonproliferation.

Mark is an expert on sanctions and has testified before Congress and advised the U.S. administration, Congress, and numerous foreign governments on Iran and sanctions issues.

Mark heads FDD’s Center on Sanctions and Illicit Finance and is the co-author of more than a dozen studies on economic sanctions against Iran. He also is co-chair of the Project on U.S. Middle East Nonproliferation Strategy.

Mark is a lecturer and senior research fellow at the Munk School of Global Affairs at the University of Toronto where he teaches and conducts research on international negotiations, sanctions, and Iran’s nuclear program.

**Annie Fixler** is a policy analyst at the Foundation for Defense of Democracies’ Center on Sanctions and Illicit Finance (CSIF).

She contributes to CSIF’s work on offensive and defensive tools of economic coercion and the application of financial sanctions. She also works closely with FDD’s government relations team and executive leadership on a range of issues including Iran sanctions.
About FDD’s Center on Sanctions and Illicit Finance (CSIF)

The Foundation for Defense of Democracies’ Center on Sanctions and Illicit Finance (CSIF) expands upon FDD’s success as a leading think tank 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 activities 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.