Foreign Policy Research Institute

E-Notes

A Catalyst for Ideas | *Distributed Exclusively via Fax & Email* | **September 2007**

FINANCIAL WARFARE

By Paul Bracken

The U.S. is increasingly using financial warfare to punish international actors, blocking the overseas bank accounts of North Korean, Iranian, and Russian companies involved in illicit activities such as nuclear and conventional weapons proliferation. Attacking the funding of terrorist groups is a core strategy for dealing with this threat.

Financial warfare has greater targeting accuracy than the classic economic warfare of trade sanctions, embargoes, and blockades, which have an overly diffuse impact on whole populations. For this reason, its use is likely to increase, just as precision military strikes replaced carpet bombing two decades ago.

Financial warfare also has a deep connection with information operations and network-centric warfare, which points to a new type of conflict against computing and network infrastructures in the financial sector. When these networks are cut off or compromised, money stops flowing and operations cease. The ability to do this--offensively and defensively--has enormous political consequences.

WHAT WE THINK WE KNOW

National power once meant control of natural resources, factories, and ports. Controlling or denying these was a major object of military strategy. Economic warfare--in the form of strategic embargoes, blockades, or the preemptive purchase of scarce resources to deny them to the enemy--was designed to deny access to critical resources, or to disrupt their conversion into war goods.

In the Cold War, the economic autarky of the communist bloc made it difficult to practice classic economic warfare. Outside of technology, there was little the Soviet Union wanted from the West. But with the tremendous growth of Western trade and finance, the West's attention soon shifted to whether the Soviet Union could disrupt the international order by triggering a financial panic or another kind of economic dislocation.

By the 1970s, the global economy was restructuring, with Japan's rise as the second-largest economy in the world. Trade and finance increased dramatically, and there was wide recognition of "the dollar overhang problem," or more dollars (Eurodollars) outside of the United States than there were in the U.S. economy's money supply.

Several studies and conferences held in the 1970s on the West's economic vulnerability concluded that modern capitalist economies were highly resilient; it was difficult to upset them for long.[1] Knocking out key nodes is much more difficult than it first appears because activity automatically shifts to other nodes and sectors. This framework still offers a useful vocabulary for analyzing economic warfare.

The 1980s saw a shift in attention from the economic vulnerabilities of the West to those of the Soviet Union. However, most studies concluded that the Soviets would muddle through the 1980s, with little possibility of an economic collapse. In the 2000s, attention is on the financial, as distinct from the purely economic, aspects of vulnerability. Several reasons account for this: international flows of money dwarf trade, and most of this money--over 90 percent--has nothing to do with paying for toys from China or cars from Japan. It is money seeking a better return by moving electronically from the Buenos Aires to the Russian stock market, and back again to a Connecticut hedge fund.

One measure of the astounding growth of international finance is the flow of dollars through "Chips" computers. Chips is the Clearinghouse Interbank Payments System, privately operated by large banks, to move dollars electronically from one financial institution to another. In 2007, the average daily flow of dollars through Chips is $1.5 trillion. Since Chips does not process all dollar movements and operates only in dollars, it seems reasonable to say that international money movements

[1] See, e.g., GE Tempo, *Economic Conflict and National Security Research*, Report GE-77, Feb. 22, 1977.

amount to $2.5 trillion per day.

Global finance can have important political consequences. In the "Tequila crisis" of 1994-95, the U.S. loaned $50 billion to Mexico to avoid a number of destabilizing possibilities. These included increasing the number of illegal migrants coming to the U.S. or derailing the democratic trends underway there.

Politics, likewise, can have important financial implications. In 1998, Long Term Capital Management (LTCM), a Connecticut hedge fund, lost $3 billion on Russian bonds. This caused the U.S. Federal Reserve Bank to "suggest" to the firm's limited partners that they invest more capital to avoid destabilizing the world financial system. LTCM, it turns out, was making very thin margins on their trades, and they had to bet huge amounts to generate a decent return. They got their money on loan from limited partners, Wall Street banks, and wealthy individuals. LTCM had leveraged over a trillion dollars on their bets on where the markets were going.

An interesting feature of this crisis is how poorly LTCM assessed political risk. The Russian bond default that triggered LTCM's collapse did not arise because Moscow was unable to pay back the bondholders. Rather, the problem was a political split inside the Russian government. One faction simply refused to pay.

More recently, terrorist attacks beginning with 9/11 have had little economic or financial impact. After 9/11, the NYSE was closed for only four days. Within a year, the job market on Wall Street (and the New York City real estate market) was again booming. Even the New York firms hardest hit showed extraordinary resilience. Cantor Fitzgerald, Aon, and Marsh & McLennan lost hundreds of employees in the WTC attacks. Yet they all came back, most in weeks, some in months. The resilience of markets and business is not to be underestimated.

FINANCIAL AND ECONOMIC SYSTEMS

It is important to distinguish between financial and economic systems. This distinction is central to understanding the growing opportunities for financial warfare, as distinct from classic economic warfare. The economic system deals with the hard and soft outputs of the economy--that is, goods and services. The financial system deals with money and credit. In the modern financial system these can be very complicated. Bank credit, money transfers, stocks, bonds, and derivatives are the “stuff” of the financial system. It is a system built on confidence. There is trust that loans will be paid, that money transferred to an account will actually get there, and that money once placed in an account will not suddenly “disappear.”

The difficult question is the relationship between these two systems. After the 500-point drop in the Dow Jones Industrial Average on October 19, 1987, the Dow recovered to its pre-crash levels by the second half of 1989. The huge one-day hit in 1987 had little lasting effect on the real economy. At times the real economy can slow down, measured by GDP decline and increased unemployment, while financial markets boom. At other times, the underlying economics can be good, but finance bad--as in 1987.

Distinguishing between the two systems is important. Financial shocks tend to be more immediate and concentrated in time. They can also be more targeted, affecting particular groups. Economic shocks usually affect broad segments of the population; unemployment goes up or goods are in short supply. Financial shocks are usually more concentrated. For example, when Enron collapsed in 2000, those most affected were not the average citizen, or even the average stockholder. It was the employees and share-owners who disproportionately suffered loss.

FINANCIAL WARFARE

Financial warfare is an expanding arena of conflict. Understanding financial vulnerabilities requires thinking across departments that have not historically been well coordinated--e.g., Defense, Treasury, and the intelligence community. Since money in the modern era can be instantly moved electronically, even the appearance of a threat to accounts can lead to large outflows into safer banks in safer countries. This is how the Eurodollar market began back in the early 1950s. The Soviet Union sold gold for dollars, but was afraid to keep the dollars in an account in New York, where they might be blocked for Cold War reasons. Moscow started a dollar-denominated account in an Italian bank known as "Eurobank," where it felt safer from seizure.

In the 1956 Suez crisis, when Britain and France landed forces on the Suez Canal to prevent its nationalization by Egypt, President Dwight Eisenhower looked for ways to pressure London to call off the attack. Clearly, Washington could not take direct military action against NATO allies. Eisenhower turned instead to financial warfare. He ordered the Treasury Department to dump British Sterling on the international market. This depressed the value of the British pound, causing a shortage of reserves needed to pay for imports. If this financial situation had continued for much longer, it would have also increased British inflation. The message quickly got through to London, which, along with Paris, soon pulled out of the Canal.

In the aftermath of Iran's seizure of U.S. hostages in 1979, President Jimmy Carter ordered Iranian government bank accounts frozen in the U.S. and the UK. Recently, the U.S. has acted to block North Korean bank accounts linked to illegal activities and the financing of its nuclear program. The U.S. Treasury Department blocked $25 million in accounts held in Banco Delta Asia in Macao. This Department also pressured other banks to stop dealing with the banks of Iran and Syria, as well as those of certain Russian companies involved in the arms trade. This pressure has made it more difficult for them to use the global financial system for letters of credit, trade finance, and remittances from their overseas citizens. It also has increased the risk premium and interest rates on any financing they are able to secure from other sources.

A U.S. crackdown on Iran's Bank Sederat involved getting foreign banks including some of the world's largest banks--UBS and Credit Suisse of Switzerland and ABN Amro of the Netherlands--to agree not to conduct business with this bank or risk being cut off from the U.S. financial system. U.S. actions have involved both official sanctions undertaken by the Treasury Department's Office of Foreign Assets Control, and informal actions intended to sap business confidence in dealing with Iran.

Most major banks fear "headline risk." Having their names in major media for dealing with Iran's atomic programs, for example, is likely to scare off their regular corporate customers. Informal pressure has proven to be a partial solution to hidden dealings, in that a bank has to consider the costs of dealing with a company or bank linked to Iran or North Korea. In the 1990s, many foreign banks easily bypassed oil sanctions against Iraq which were incorrectly thought to be governed by strict UN supervision of Baghdad's accounts. The 2005 Volcker Report concluded that Saddam Hussein, using surcharges and kickbacks, diverted $1.8 billion involving more than 2,000 companies that engaged in illicit activities.

U.S. VULNERABILITY TO FINANCIAL ATTACKS

How would the U.S. financial system react to a WMD attack on a major hub, such as New York? Is enough being done to harden and back up financial systems so that a cascading set of failures would not spread to other markets, with dire political implications?

One reason Wall Street responded so quickly after 9/11 was that planning for a possible attack had been undertaken earlier. In 1997, a war game of a Wall Street attack was played. Leaders from the White House, Treasury, the Federal Reserve, the Pentagon, and the intelligence community came together with leaders of Wall Street's largest financial institutions to simulate a terrorist attack designed to disrupt the U.S. economy. The game was played in the WTC's north tower, and some of the actual players were working there on 9/11 and were killed in the attack. The terrorist scenario was nothing like what actually happened on 9/11. The war game attacks focused on key nodes, like computer clearing houses and telephone switching centers, whereas on 9/11 a primitive yet highly effective attack was launched. Nonetheless, the lessons drawn from this game included the need to disperse key facilities away from lower Manhattan, as well as to back up important data at remote locations. All of this proved highly useful to the quick restoration of Wall Street on 9/11.

Since 9/11 the concern to reduce the U.S. financial system's vulnerability to terrorist attacks has greatly increased. Virtually every major U.S. bank and financial institution has thought through its vulnerabilities. In addition, the Treasury Department has taken major steps to ensure that financial systems are more redundant and hardened and that back-up alternates are ready to take over in case of disaster. Sarbanes-Oxley and other legislation require financial institutions to monitor carefully their internal processes. Basle II, from the Bank for International Settlements in Basle Switzerland, reinforces this trend by requiring banks to reserve capital against so-called operational risks, i.e. internal process breakdowns such as those from cyber attacks or inside theft.

In addition, the pattern in the New York financial industry is to disperse back office operations to New Jersey and elsewhere. The hedge fund business is concentrated in nearby Fairfield County, Connecticut. The pattern from San Francisco to Miami is to shed high-cost downtown locations as much as possible. These trends have the combined effect of reducing the U.S. financial system's vulnerability to terrorist attack. However, interdependencies among the financial system and other complementing systems remain. The electrical and telephone grids, in particular, are essential for the smooth operation of the financial system. One of the peculiar features of the New York financial market is that 40 percent of the workforce uses mass transit to get to work. In the event of a bio-attack in New York, this might be a major vulnerability. But in sum, the U.S. financial system is getting much harder to take down.

TERRORIST NETWORKS

The chief problems of denying funding to terrorist groups are that the amount of money they use is small, and the networks they rely on are mass market in character, and thus difficult to monitor without specific intelligence. Terrorist cells are unlikely to use large international networks for international funds transfer. Reports are that the Tamil Tigers in Sri Lanka have used on-line e-Bay and PayPal accounts for money laundering, arms trafficking, and other activities. Such small accounts are very difficult to monitor .

Terrorist funding is hard to disrupt, but even partial successes can have significant payoffs. One of the major lessons learned from cracking down on terrorist funding after 9/11 was the critical importance of the timing of financial attacks. Freezing suspects' bank accounts requires worldwide coordination, since the seizures must come down nearly simultaneously.

FINANCIAL WARFARE AS A STRATEGY

One criticism of U.S. offensive financial warfare is that it is unlikely to be effective. Iran in 2007, for example, earns about $300 million a day in oil and gas exports. This money flow is not the object of financial actions because it is tied to the legitimate sale of oil and gas to customers around the world. The amount of money blocked in bank accounts held in the name of Iranian Revolutionary Guards, for example, is small compared to these larger flows of money coming from the energy exports.

But this view fails to put financial warfare in a strategic context. Blocking bank accounts of key groups and individuals puts the spotlight on them and thereby increases the risks to any company or government doing business with them. Financial sanctions legitimize additional actions, both financial and non-financial, which can ratchet up more pressure. This is where

financial warfare and military strategy converge. Most people think of financial warfare as a substitute for military action, which it is, up to a point. But after a point it becomes a complement rather than a substitute.

The most intense kinds of financial warfare, such as blocking all monetary transactions and flows to and from a country and its citizens, may only make sense under conditions of war. But there is a large spectrum of intermediate cases between small financial sanctions which substitute for kinetic attacks and "all out" financial warfare complementing military attack. And it is this spectrum that gives us the key insight that financial warfare as a strategy is best viewed in an escalation framework. It has two separate effects. The first is the direct pain it causes to individuals and companies whose accounts are blocked or confiscated. The second impact comes from its place as a "next-step" action which is considered reasonable and justifiable. The next step builds on a sequence of actions which raise the bar of what are seen to be sensible and legitimate measures to right some wrong or to force a change in behavior. If the current step does not do this, the next step might. Placing financial warfare in an escalation framework has several important aspects. It is more focused than traditional economic warfare. It is, therefore, more likely to be considered acceptable in a political sense. It was the Iraqi people who suffered most from the embargo placed on Iraq from 1991-2003; Saddam and his cronies bypassed the embargo.

Blocking bank accounts and disrupting money flows is a sharp instrument that goes after those in power who are calling the shots. In many respects, conventional economic warfare is like carpet bombing; financial warfare is like precision strike. Neither one guarantees success, but the latter approach is usually more attractive. Another aspect of placing financial warfare in an escalation framework is that it doesn't just play the game, it reshapes it. The U.S.'s use of informal financial pressures is a case in point. Over 40 major global banks and financial institutions have cut off or sharply reduced their dealings with the Iranian government and businesses at the urging of U.S. Treasury and State Department officials. This is action that goes beyond official UN sanctions intended to deal with Iran's nuclear program. Consider a bank that serves as a financial intermediary for Iran or North Korea. It now has to evaluate the reputation risks to its entire portfolio in dealing with such "hot" clients. Again, credit is confidence. If other banks in the Interbank market (banks making short-term loans to other banks) view it as taking major risks by its dealings with Iran or North Korea, they are likely to be cut off.

Seen this way, financial warfare is a consensus-building device. It sets up a coalition made up of allies and those sitting on the fence who will have to decide whether to honor the sanctions. Financial warfare has an element of risk communication as well, both for the target and others in the network. According to Stuart Levey, Undersecretary of the Treasury for Terrorism and Financial Intelligence, "All the banks we've talked to are reducing significantly their exposure to Iranian business. It's been a universal response. They all recognize the risks--some because of what we've told them and some on their own. You don't have to be Sherlock Holmes to see the dangers."

Viewed as a "next step" in a dynamic escalation, financial warfare may be much more effective in building pressure than is commonly believed. A good case can be made that North Korea decided to test its atom bomb when it did, in October 2006, because of the asset freeze placed on accounts Banco Delta Asia in Macao by Chinese authorities, at U.S. urging. Financial warfare could produce explosive effects, quite literally. This is another reason for looking at financial warfare as an escalation process: the failure to estimate and analyze its potential effects can lead to serious mistakes and big surprises. It can only be appreciated with a thorough understanding of it as a dynamic process.

INFORMATION OPERATIONS AND ELITE TARGETING

Financial warfare complements military operations as well as information operations. When combined with advances in social network mapping, it can give a highly detailed picture of an elite's communication and financial structure that can be used for targeting. Communication and software tools now exist to analyze connections in vast networks of heterogeneous information, such as financial transactions, mobile telephone calls, e-mail, and air travel. This gigantic information pool can be a source of knowledge about a nation's elite, where they stash their money, who they talk to, and their position in a social hierarchy. The key to doing this lies in constructing overlays of these datasets to visualize the various connections.

Watching how money flows out of a country in a crisis can be an important tip-off to who is in the know and who is at least partially responsible for national decisions. Carried to the next step, this can be combined with precise military attacks to go after a nation's elite. For example, tracking mobile telephone calls can reveal things like where the elite live, their vacation homes, and their travel patterns. Financial tracking of their bank accounts can reveal where they keep their money and who has access to their accounts. This creates the conditions for potentially ruinous attacks with far-reaching social implications on the national leadership. Were a national elite's overseas bank accounts frozen and their homes targeted with cruise missiles, simultaneously, a hyper-decapitation attack could destroy a nation's leadership. Clearly, this represents a large escalation. But there are many possibilities which fall short of this, and these constitute an important type of strategy: counter-elite targeting. Counter elite targeting has been considered in the past, both in the Cold War, with nuclear weapons, and more recently in conflicts in Kosovo and Iraq. But the 21st century is likely to see considerably more applications of it.

Spoofing--sending false signals of increased military and financial pressure--could be used to map out the crisis response patterns of a national elite, who they call, and where they send their money. This could be an intelligence treasure-trove of information. It could also be an input to information operations designed to make certain individuals, groups, or companies "suspect" in the eyes of a leader. This could undermine confidence in the regime. Seen as an escalation process, this focuses attention on actions which fall short of all-out attacks. These lower-level or intermediate actions are likely to provide U.S. decision-makers with a range of options between doing nothing and all-out attacks.

Developments in technology, intelligence, and finance are converging, creating more favorable conditions for financial warfare. More systematic thought should be given to this important subject.

COMMAND AND CONTROL

Financial warfare blurs the military and civilian spheres of conflict. It should entail cooperation among the armed services, State, Defense, Treasury, DHS, and the intelligence community. Organizational issues over authority and tasking may prove to be one of the greatest barriers to getting a coherent intellectual framework for what is going on. The challenges are difficult, but ignoring them only makes it likely that improvisation and over-compartmentalization could produce serious mistakes.

War games, appropriately designed, could go a long way to revealing some of the tensions and stresses in command and control. The Wall Street Security Exercise cited earlier had this effect. It put attention on the sensitive interface among different government agencies and was an important, if small, step in understanding the vulnerabilities of the U.S. financial system.

CONCLUSIONS

Financial warfare is likely to be an increasing form of conflict because it lies at the intersection of powerful long-term trends in technology, networks, and finance. The precise targeting feature of financial warfare, relative to conventional economic warfare, marks a significant change in the nature of conflict. This topic calls out for more thought about what is likely to be a growing use of a tactic that calls for a strategic framework to understand it.

Paul Bracken is Professor of Management and Political Science at Yale University. This enote is based on his article in the Fall 2007 issue of **Orbis.**

FPRI, 1528 Walnut Street, Suite 610, Philadelphia, PA 19102-3684.
For information, contact Alan Luxenberg at 215-732-3774, ext. 105 or email fpri@fpri.org or visit us at www.fpri.org.