

The SWIFT System: A Potential Weapon in the Hybrid War

By [Valentin Katasonov](#)

Global Research, May 11, 2016

[Strategic Culture Foundation](#) 3 May 2016

Region: [Russia and FSU](#)

Theme: [Global Economy](#)

The economic and financial sanctions against Russia have highlighted the role of SWIFT in the US control of international monetary exchange. If Russia has already put in place, at national level, its own system, no alternatives exist yet internationally.

The acronym SWIFT (The Society for Worldwide Interbank Financial Telecommunications) has once again popped up in the global media headlines. Experts usually describe SWIFT as an international, interbank network for transmitting information about payment transactions.

Globalization would be impossible without SWIFT

The society was founded in 1973. By that time the post-war monetary system established in 1944 in Bretton Woods had virtually collapsed. The dollar as well as other currencies had been divorced from gold, and the printing presses at the US Federal Reserve and other Western central banks were furiously at work. The volume of international payments had increased sharply. The traditional systems for sharing data about payment transactions (the teletype, telegraph, and telephone) could not cope with the increased traffic.

It was necessary to draw upon the latest technology in order to centralize the isolated channels used to exchange information. Two hundred thirty-nine banks from 15 countries worked together to set up an organization devoted to solving this problem. SWIFT is a cooperative society, established under European law, with a head office in Brussels. Currently almost 11,000 institutions from over 200 countries, including 9,600 banks, are members of SWIFT. Every year 2.5 billion payment orders are transmitted through the SWIFT network, which processes billions of dollars each day.

SWIFT's advantages are its speed, low cost, and reliable data protection. As a result, the majority of the world's international settlements and payments now go through the SWIFT system. Payments are also cleared through this network even when each of the parties is under the same jurisdiction. This includes dollar and euro payments that must be handled by the banking systems of the US and European Union. During the 21st century the SWIFT system began helping money circulate throughout the entire global economy. The economic and financial globalization that began in the 1970s would have been impossible without SWIFT.

The scandal over the attack against the central bank of Bangladesh

The SWIFT system has often been targeted by hackers trying to break into databases and divert money from the accounts of the society's member banks. Several attempts at

security breaches have been documented in just the last few days.

In early March, the central bank of Bangladesh reported the disappearance of \$81 million of its foreign-exchange reserves [1]. This had gone unnoticed by the IT services at SWIFT and the central bank.

An investigation revealed that the hardware and software used to process the central bank's payment operations left much to be desired. The cyber intruders also turned out to have advanced technical skills. They did not expect the facts of the theft to come to light immediately and assumed that they would have time to either move their spoils somewhere safe or to launder the money.

The attack on the central bank of Bangladesh had been expertly planned and demonstrated a close familiarity with the inner workings of that bank. As a rule, having someone on the inside can either make or break a hacking operation conducted from outside of that organization. Thus the question arises: are there such informants inside the SWIFT headquarters in Brussels?

SWIFT: high-profile scandals from recent years



The society has suffered scandals in the past. After Sept. 11, 2001, the CIA as well as the financial-intelligence arm of the US Treasury Department gained access to SWIFT network information [2]. But the managers of the SWIFT data centers did not bring this cooperation between the society and the security agencies to their members' attention. Only a select few knew about the American «terrorist tracking» program. The information was not leaked until 2006.

In 2012 SWIFT again found itself in the headlines. At that time Washington was heavily pressuring the society to disconnect Iranian banks from the SWIFT network [3]. Of course, a society that constantly claims to «stay out of politics» was uncomfortable with this measure. Disconnecting even one bank would generate distrust of the system, lower its rating, and encourage other SWIFT members to formulate backup plans. But Washington won that battle – 14 Iranian banks were expelled from SWIFT.

But every cloud has a silver lining. Iran learned to manage without SWIFT and won valuable experience in the use of alternative systems for international payments and settlements. Washington has now graciously revoked some of the sanctions against Iran, and so once again that country is permitted to use the SWIFT network. But Tehran is in no hurry to accept the invitation. First of all, Washington's policy toward Iran is highly contradictory and

inconsistent. Second, in light of the recent scandal, Iran and other countries have increasing misgivings about SWIFT. It is unlikely that Tehran will put all its eggs into one basket. A few Iranian banks will be reconnected, but most payment transactions will continue to be made through alternative channels.

Russia needs an alternative to SWIFT

There are about 800 banks in Russia today, approximately 600 of which are connected to the SWIFT system. Russia is home to the second-highest number of SWIFT member institutions (after the US), but it doesn't even crack the top ten in terms of volume of transactions (last year Moscow was in 15th place). By the early 2000s at least 90% of Russia's foreign payments were processed through SWIFT. The system was also utilized for many domestic transactions.

When the West first introduced economic sanctions against Russia in 2014, British Prime Minister David Cameron demanded that Russia be disconnected from the SWIFT system. The only reason they have not made good on this threat is because the West is afraid of the potential consequences. After all, disconnecting Russia from SWIFT isn't like disconnecting Iran - only 14 banks were cut off there, while 600 would need to be unplugged in the Russian Federation.

But if the hybrid war against Russia becomes a full-blown conflict, it will not be possible to rule out the chance that Russian bank operations will be completely barred from SWIFT. Preparations for that war can't wait until the last minute, and some measures are already in place. For example, by late 2014 Russian companies and organizations were already making payments and settling accounts with one another without resorting to SWIFT as an intermediary. A national system had been set up to handle domestic payments between Russian banks [4].

International payments are more complicated. Back in 2014, talk began of creating a direct-payment system (that would also communicate information about payments) between China and the Russian Federation. The system needs to be autonomous - fully independent of any payment systems controlled by the United States and European Union (specifically the trans-European TARGET system). And this autonomy is only possible by transitioning to the use of national currencies - a premise that was built into the original design.



In addition to the agreement signed at the BRICS summit in Brazil in July 2014 to establish the BRICS Development Bank, it was also agreed that the central banks of the BRICS countries would open mutual lines of credit in one another's national currencies. Perhaps that was when the idea of creating a bilateral payment system for Russia and China was transformed into the idea of a multilateral BRICS payment system. Naturally, that would also involve transactions in the national currencies of those five countries.

Russia has shown the most interest in this BRICS payment network. Last October Beijing reported that a system for processing international payments in yuan was already operational, which it called the Chinese alternative to SWIFT. Only a modest number of transactions are as yet using this Chinese platform, but it is possible that this acorn could grow into a mighty oak of a system, in time becoming an alternative to SWIFT.

Some non-BRICS countries, such as Iran and Kazakhstan, have shown an interest in taking part in the project to create an alternative network for multilateral payments. The latest SWIFT scandal (the theft of the money from the central bank of Bangladesh) is yet another reason why Russia and its international partners should pick up the pace and get this project to create an alternative international payment system up and running.

Notes:

[1] [“The Incredible Story Of How Hackers Stole \\$100 Million From The New York Fed”](#), Tyler Durden, *Zero Hedge*, March 10, 2016.

[2] [“Bank Data Is Sifted by U.S. in Secret to Block Terror”](#), Eric Lichtblau & James Risen, *The New York Times*, June 23rd, 2006. «[La CIA a contrôlé les transactions financières du monde entier via la société SWIFT](#) », par Grégoire Seither, *Réseau Voltaire*, 26 juin 2006.

[3] [“Iran Praises Nuclear Talks With Team From U.N.”](#), Rick Gladstone, *The New York Times*, January 31st, 2012.

[4] [“Russia precipitates the abandonment of SWIFT among the BRICS”](#), by Ariel Noyola Rodríguez, Translation Jordan Bishop, *Russia Today (Russia)*, *Voltaire Network*, 6 October 2015.

The original source of this article is [Strategic Culture Foundation](#)
Copyright © [Valentin Katasonov](#), [Strategic Culture Foundation](#), 2016

[Comment on Global Research Articles on our Facebook page](#)

[Become a Member of Global Research](#)

Articles by: **[Valentin Katasonov](#)**

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca