G20 INSIGHTS

G20 GERMANY 2017
THINK 20 DIALOGUE

POLICY AREA:
**Digitalization**

# Toward A Global Norm Against Manipulating the Integrity of Financial Data

Tim Maurer (Carnegie Endowment for International Peace)
Steven Nyikos (Carnegie Endowment for International Peace)

April 05, 2017

## Abstract

The G20 Finance Ministers and Central Bank Governors have highlighted that cyber threats can pose a risk to financial stability. The G20 heads of state can contribute to reducing this risk by explicitly committing not to undermine the integrity of data and algorithms of financial institutions in peacetime or during war, nor to allow their nationals to do so and to cooperate when such attacks do occur.

## Challenge

The financial crisis that erupted in 2007 highlighted how important trust is for the global system and how fragile it can be. The 2016 Bangladesh central bank cyber incident exposed a new threat to financial stability and the unprecedented scale of the risk that malicious cyber actors pose to financial institutions.[i] Beyond theft, using cyber operations to manipulate the integrity of data, in particular, poses a distinct and greater set of systemic risks than other forms of financial coercion. The complex and interdependent character of the financial system and its transcendence of physical and national boundaries mean that manipulating the integrity of financial institutions' data can, intentionally and/or unintentionally, threaten financial stability and the stability of the international system. Importantly, unlike the 2007–2008 global crisis, this risk exists independent of the underlying economic fundamentals and will only increase as more and more governments make cashless economies an explicit goal.[ii] On March 18, 2017, the G20 finance ministers and central bank governors recognized this risk in their communiqué highlighting that "The malicious use of Information and Communication Technologies (ICT) could disrupt financial services crucial to both national and international financial systems, undermine security and confidence and endanger financial stability."

[i] Krishna N. Das and Jonathan Spicer, "The SWIFT hack – How the New York Fed fumbled over the Bangladesh Bank cyber-heist," *Reuters*, July 21, 2016

[ii] States' reliance on financial data and the system's interdependence is likely to increase. For example, in December 2015, the *New York Times* ran a story about the Swedish government's effort to move the country to an entirely cashless economy, and the UN is supporting countries' efforts toward cashless economies through its Better Than Cash Alliance. The Indian government is also pursuing a cashless economy.
See Liz Alderman, *In Sweden, a Cash-Free Future Nears*, N.Y.Times (April 26, 2015)
Better Than Cash Alliance (last visited April 21, 2016).
The Indian Express, "From eradicating black money to cashless economy: PM Modi's changing narrative since demonetisation" December 22, 2016.

# Proposal

**Summary**

The G20 Finance Minister and Central Bank Governors should be commended for urging improvements in the resilience of the global financial system and for highlighting the risk to financial stability through the malicious use of ICT. The 2016 Bangladesh central bank cyber incident exposed this new threat and the unprecedented scale of the risk that malicious cyber actors pose to financial institutions.[i] The economic crisis that erupted in 2007 highlighted generally how important trust is for the global system and how fragile it can be. But governments should not only ask the private sector to do more; governments themselves can help reduce the risk to financial stability. The G20 heads of state could commit their countries explicitly to refrain, in peacetime and during war, from using offensive cyber tools to corrupt the integrity of data in the financial system and to cooperate when such attacks do occur.

**Rationale**

Using cyber operations to manipulate the integrity of data, in particular, poses a distinct and greater set of risks to financial stability. Importantly, unlike the 2007–2008 global crisis, this risk exists independent of the underlying economic fundamentals and will only increase as more and more governments pursue cashless economies. An explicit agreement against manipulating the integrity of financial institutions' data would build on recent international efforts to develop rules for cyberspace and existing international law. The international community's to date is the UN Group of Governmental Experts process. Yet, the group's 2015 declaration and its G20 endorsement, thus far, lack detail and concrete steps to turn them into effective and robust security regimes.[ii] Such an agreement is therefore a particularly promising next step to operationalize what has already been agreed to and to clarify what could be considered emerging state practice.

States share a common interest due to the financial system's global interdependence. Whereas the damaging effects of an intrusion targeting the electrical grid, for example, will be mostly limited to a single country's territory or immediate neighbors, the effects of an incident targeting the data integrity of a financial institution are not necessarily bound by geography. Such effects can be hard to tailor and to predict. Indirectly, a manipulation of the integrity of an institution's data could lead to a bankruptcy that in turn could send shock waves throughout the international system. For example, the 2007 collapse of Lehman Brothers highlighted the unanticipated contagion effect the bankruptcy of even a single institution can have. The 1997 Asian financial crisis was similarly triggered by the collapse of the Thai currency and the unanticipated contagion effect across the region. Such second-order effects are also difficult to anticipate. Moreover, they may not be factored in the attacker's battle damage assessments.

Major powers, notwithstanding their fundamental differences, have recognized this in principle and deed. The U.S. government reportedly refrained from using offensive cyber operations against Saddam Hussein's financial systems as well as in hypothetical exercises simulating a conflict with China.[iii] Russia's 2011 *Draft Convention on International Information Security* explicitly suggests that "each State Party will take the measures necessary to ensure that the activity of international information systems for the management of the flow of . . . finance . . . continues without interference."[iv] China also has a vested interest in the system, reflected, among other ways, by its

successful effort to make the renminbi part of the IMF's global reserve currency basket.[v] Meanwhile, countries around the world are setting up or strengthening their CERTs specific to the financial sector, as, for example, India did in February 2017.[vi]

Of course, in the twenty-first century, a few states that are relatively detached from the global economy, and nonstate actors who may or may not be affiliated with them, have capabilities to conduct cyberattacks against financial institutions. Such hostile actors would not be expected to adhere to the proposed commitment. Yet, the states that did endorse such a norm explicitly would be more united and would have a clearer interest and basis for demanding and conducting retaliatory action against violators of the norm, be they states, terrorists, or cybercriminals.

In other words, most states have already demonstrated significant restraint from using cyber means against the integrity of data of financial institutions. Such an agreement would therefore be making explicit what could be considered emerging state practice in order to:

- send a clear signal that the stability of the global financial system depends on preserving the integrity of financial data in peacetime and during war and that the international community considers the latter off limits;
- build confidence among states that already practice restraint in this domain, and thereby increase their leverage to mobilize the international community in case the norm is violated;
- create political momentum for greater collaboration to tackle nonstate actors who target financial institutions with cyber-enabled means; and
- complement and enhance existing agreements and efforts, namely the 2015 G20 statement, 2015 UNGGE report, and the 2016 cyber guidance from the Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions (CPMI-IOSCO).

While the March 18 G20 Finance Ministers and Central Bank Governors communiqué does not define 'malicious use of ICT', it is reasonable to think that it particularly focuses on the integrity and availability of financial data as the source of the most significant systemic risk. We therefore propose the following language for a G20 heads of state agreement, of course inviting debate and refinement:

A State must not conduct or knowingly support any activity that intentionally manipulates the integrity of financial institutions' data and algorithms wherever they are stored or when in transit.

To the extent permitted by law, a State must respond promptly to appropriate requests by another State to mitigate activities manipulating the integrity of financial institutions' data and algorithms when such activities are passing through or emanating from its territory or perpetrated by its citizens.

In order to achieve effective reciprocal adherence and be widely accepted among UN member states, the agreement should not be limited to a subset of financial institutions. The envisioned prohibition would be conveyed from states to states. If and when key states subscribe to something like the agreement proposed here, future work could seek to broaden it in terms of actors and sanctuaried targets. Defining whether and how data availability could be addressed and included in the proposed agreement requires broader expert consultation and advice. The G20 could task the Financial Stability

Board to work with relevant standard-setting bodies and experts to report on this issue for further consideration. Finally, we acknowledge that other sectors, such as telecommunications and energy, and the integrity of data of other systems are critical for the financial system. However, any agreements covering these sectors are even more complicated to negotiate and to implement effectively. We therefore offer this proposal as the start for what is likely going to be a prolonged process until an effective comprehensive security regime can be put in place.

## Proposed implementation

1. The G20 finance track discusses the language proposed here (or otherwise improved) for inclusion in the communiqué of the G20 heads of state meeting in July 2017;

2. The G20 agree to establish a G20 Working Group on the malicious use of ICT and financial stability;

3. The G20 finance track discusses language asking the Financial Stability Board to

    - implement and promulgate the agreement with the relevant standard-setting bodies and private sector institutions including CPMI, IOSCO, and the Basel Committee (this would include exploring some of the questions such as whether the availability of certain data and systems ought to be included and whether all types of data or specific types of data would fall under the agreement, such as transaction-based data, operations data, and ledger/ownership data);

    - develop a report to be submitted to the next G20 meeting outlining the progress made and a road map for further implementation.

---

[i] Krishna N. Das and Jonathan Spicer, "The SWIFT hack - How the New York Fed fumbled over the Bangladesh Bank cyber-heist," *Reuters*, July 21, 2016,

[ii] United Nations, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" July 22, 2015, UN Doc. A/70/174; G20 Leaders' Communiqué Antalya Summit, 15-16 November 2015

[iii] John Markoff and Thom Shanker, "Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk," *The New York Times*, August 1, 2009; Richard Clarke and Robert Knake (2010) Cyber War: 202-203

[iv] The Ministry of Foreign Affairs of Russia, "Convention on International Information Security (Concept)" 9 September 2011.

[v] Mark Fahey & Nicholas Wells, *Charts: Who loses when the renminbi joins the IMF basekt?*, CNBC (Dec. 2, 2015),

[vi] Sandhya Dangwal, "Budget 2017: Computer Emergency Response Team to be set up to check cyber frauds," India, February 1, 2017,

# References

Krishna N. Das and Jonathan Spicer, "The SWIFT hack - How the New York Fed fumbled over the Bangladesh Bank cyber-heist," Reuters, July 21, 2016

States' reliance on financial data and the system's interdependence is likely to increase. For example, in December 2015, the New York Times ran a story about the Swedish government's effort to move the country to an entirely cashless economy, and the UN is supporting countries' efforts toward cashless economies through its Better Than Cash Alliance. The Indian government is also pursuing a cashless economy.
See Liz Alderman, In Sweden, a Cash-Free Future Nears, N.Y.TIMES (April 26, 2015);
BETTER THAN CASH ALLIANCE (last visited April 21, 2016).

The Indian Express, "From eradicating black money to cashless economy: PM Modi's changing narrative since demonetisation" December 22, 2016

Krishna N. Das and Jonathan Spicer, "The SWIFT hack - How the New York Fed fumbled over the Bangladesh Bank cyber-heist," Reuters, July 21, 2016

United Nations, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" July 22, 2015, UN Doc. A/70/174; G20 Leaders' Communiqué Antalya Summit, 15-16 November 2015

John Markoff and Thom Shanker, "Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk," The New York Times, August 1, 2009

The Ministry of Foreign Affairs of Russia, "Convention on International Information Security (Concept)" 9 September 2011

Mark Fahey & Nicholas Wells, Charts: Who loses when the renminbi joins the IMF basekt? CNBC (Dec. 2, 2015)

Sandhya Dangwal, "Budget 2017: Computer Emergency Response Team to be set up to check cyber frauds," India, February 1, 2017