CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

BRIEF

MARCH 2017

TOWARD A GLOBAL NORM AGAINST MANIPULATING THE INTEGRITY OF FINANCIAL DATA

TIM MAURER, ARIEL (ELI) LEVITE, AND GEORGE PERKOVICH

On March 18, 2017, the G20 finance ministers and central bank governors issued a 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." The 2016 Bangladesh central bank cyber incident exposed this new threat to financial stability and the unprecedented scale of the risk that malicious hackers pose to financial institutions.

While the UN Group of Governmental Experts (UNGGE) and the G20 have suggested broad norms against attacks on critical civilian infrastructure in peacetime, we propose that states go further and explicitly commit not to undermine the integrity of financial institutions' data, in peacetime and during war, or allow their nationals to do so, and to cooperate when such attacks do occur.

There is now an opportunity for the G20 heads of state to promulgate such a commitment and to ask the Financial Stability Board to implement its details, together with the relevant standard-setting bodies, the private sector, law enforcement, and Computer Emergency Response Team (CERT) communities. The G20 could also request a report exploring whether and how data availability could be addressed and included in the proposed agreement.

States have already demonstrated significant restraint from using cyber means against the integrity of financial institutions' data. By making such restraint explicit, they could:

- 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, the 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).

ABOUT THE AUTHORS

Tim Maurer *co-directs the Cyber Policy Initiative at the Carnegie Endowment for International Peace. He focuses on cyberspace and international affairs, namely cybersecurity, human rights online, and Internet governance.*

Ariel (Eli) Levite *is a nonresident senior fellow at the Carnegie Endowment. He was the principal deputy director general for policy at the Israeli Atomic Energy Commission from 2002 to 2007 and deputy national security adviser for defense policy.*

George Perkovich *is vice president for studies at the Carnegie Endowment for International Peace. He works primarily on nuclear strategy and nonproliferation issues, and on South Asian security.*

***

The Carnegie white paper "Toward a Global Norm Against Manipulating the Integrity of Financial Data" outlines this proposal in further detail, including a list of open questions.

Using cyber operations to manipulate the integrity of data, in particular, poses a distinct set of systemic risks. 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. Moreover, 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.

Major powers, notwithstanding their fundamental differences, have recognized these risks in principle and deed. In fact, they already exercise significant restraint and refrain from manipulating the integrity of financial institutions' data. That is why, 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 risk.

The proposed agreement would therefore commit states

- Not to 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, to 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

The elements of this proposed agreement are mutually reinforcing. The commitment by states to provide assistance and information, upon request, shifts the burden of attribution from the victim of attack to states that profess interest in helping to respond to and ultimately prevent such attacks. Linking an agreement on state restraint with expectations for the private sector to implement due diligence standards addresses potential moral hazard problems. Finally, such an agreement would build on recent international efforts to develop rules for cyberspace and on existing international law. This includes the 2015 report of the UN Group of Governmental Experts stating that "States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts."

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, could conduct cyberattacks against financial institutions. Yet, the states that did endorse such a norm explicitly would be more united and would have a clearer interest and basis for demanding an end and potential retaliatory action against violators of the norm, be they states, terrorists, or cybercriminals.

The G20 heads of state could powerfully advance this norm by articulating it when they meet next, on July 7–8, 2017, building on the mid-March finance ministers' statement.

CONTACT
Steven Nyikos
Research Analyst,
Cyber Policy Initiative
+1 202 939 2236
snyikos@ceip.org