CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

THE GLOBAL THINK TANK

PROTECTING FINANCIAL STABILITY AGAINST CYBER THREATS: PROPOSAL FOR AN INTERNATIONAL AGREEMENT
THE WAKE-UP CALL FOR THE GLOBAL FINANCIAL SYSTEM
2016:
THE WAKE-UP CALL FOR
THE GLOBAL FINANCIAL SYSTEM

TARGETS OF BANK HACK ATTACKS

NEW TONIGHT
REPORT LINKS NORTH KOREA TO CYBERATTACKS ON BANKS
CARNEGIE PROPOSAL:

AN INTERNATIONAL AGREEMENT TO PROTECT THE INTEGRITY AND AVAILABILITY OF DATA OF THE GLOBAL FINANCIAL SYSTEM
WHY THE FOCUS ON THE FINANCIAL SYSTEM?

- GLOBAL INTERDEPENDENCE
- TRUST IN THE SYSTEM IS PARAMOUNT
- UNEXPECTED SOURCES OF CONTAGION

---> DIFFERENT FROM MOST OTHER CRITICAL INFRASTRUCTURE
THE PROPOSAL

Agreement not to manipulate integrity of financial data
- Reduces risk by creating more certainty regarding state behavior
- Serves as indirect verification and enforcement mechanism to circumvent the attribution problem

Detection system for data manipulation through private sector and government
- Enables more robust cooperation on this specific, critical threat of common concern and interest

Agreement to cooperate, upon request, when data manipulation occurs
ISO 27000 STANDARD ‘INFORMATION SECURITY’:

PRESERVATION OF 
CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY 
OF INFORMATION
NORM INCUBATOR: G20 FINANCE MINISTERS AND CENTRAL BANK GOVERNORS
PRECEDENT:
XI/OBAMA 2015 AGREEMENT
PRECEDENT:
G20 2015 AGREEMENT
OBJECTIVES:

- SEND A CLEAR SIGNAL THAT THE GLOBAL FINANCIAL SYSTEM IS OFF LIMITS
- BUILD GREATER CONFIDENCE AMONG STATES
- CREATE FOUNDATION TO ADDRESS POTENTIAL VIOLATIONS
- ENGAGE GREATER COOPERATION TO TACKLE CRIMINAL ACTORS
- COMPLEMENT EXISTING EFFORTS FOCUSING ON RESILIENCE
G20 FINANCE MINISTERS AND CENTRAL BANK GOVERNORS MEETING MARCH 2017
COMMUNIQUE – G20 FINANCE MINISTERS AND CENTRAL BANK GOVERNORS MEETING
BADEN-BADEN, GERMANY, 17-18 MARCH 2017

“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. We will promote the resilience of financial services and institutions in G20 jurisdictions against the malicious use of ICT, including from countries outside the G20. With the aim of enhancing our cross-border cooperation, we ask the FSB [= Financial Stability Board – not Russian intelligence service], as a first step, to perform a stock-taking of existing relevant released regulations and supervisory practices in our jurisdictions, as well as existing international guidance to identify effective practices. The FSB should inform about the progress of this work by the Leaders Summit in July 2017 and deliver a stock-take report by October 2017.”
TOWARD A GLOBAL NORM AGAINST MANIPULATING THE INTEGRITY OF FINANCIAL DATA

TIM MAURER, ARIEL (ELI) LEVITE, AND GEORGE PERKOVICH | MARCH 27, 2017

INTRODUCTION

On March 18, 2017, the finance ministers and central bank governors of the world’s twenty leading economies—the G20—issued a communique highlighting that

The malicious use of Information and Communications Technology (ICT) could disrupt financial services critical to national and international financial systems, undermine security and confidence and endanger financial stability. We will promote the resilience of financial services and institutions in G20 jurisdictions against the malicious use of ICT, including from countries outside the G20. With the aim of enhancing our cross-border cooperation, we ask the FSB (Financial Stability Board), as a first step, to perform a stock-taking of existing relevant regulations and supervisory practices in our jurisdictions, as well as of existing international guidelines, including to identify effective practices. The FSB should inform about the progress of this work by the Leaders Summit in July 2017 and deliver a much-delayed report by October 2017.

The G20 finance ministers and central bank governors should be commended for urging improvements in the resilience of the global financial system. But governments should not only ask the private sector to do more; governments themselves can help reduce the risk to the financial sector. The G20 leaders of state could commit their countries explicitly to refrain from using offensive cyber tools to corrupt the integrity of data in the financial system and to cooperate when such attacks do occur.

The financial crisis that erupted in 2007 highlighted how important it 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. 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 reliance on 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​​outdated economies an explicit goal.

ABOUT THE AUTHORS

TIM MAURER is the Cyber Policy Initiative at the Carnegie Endowment for International Peace. His research focuses on cybersecurity and international law, particularly the cyber dimension of international law, human rights, and national security.

ARIEL (ELI) LEVITE is a research scholar at the Nuclear Policy Program at the Carnegie Endowment, levite was the principal deputy director general for policy at the Nuclear Weapons Group Commission from 2002 to 2005.

GEORGE PERKOVICH is vice president for studies at the Carnegie Endowment for International Peace. His research focuses on nuclear strategy and nuclear proliferation, with a concentration on South Asia, Iran, and the problems of power in the international political economy.
New paper from Carnegie on manipulation of financial data—an issue that keeps nat sec folks up at night.
WHY AM I HERE?

In their March 2017 communique, the G20 Finance Ministers and Central Bank Governors warned that “The malicious use of Information and Communication Technologies could undermine security and confidence and endanger financial stability.” That is why, the Carnegie Endowment has proposed that the G20 explicitly commit not to engage in offensive cyber operations that could undermine financial stability, namely manipulating the integrity of data of financial institutions, and to cooperate when such incidents occur. Such an agreement by the world’s leading economies would send a clear signal condemning such activity and enable future cooperation. The G20 is now discussing such a commitment by its member states.

This website is meant to serve as a hub providing more details about the G20 discussing the threat to international economic stability.

WWW.PROTECTINGFINANCIALSTABILITY.ORG