CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

The
Cyber Policy
Initiative

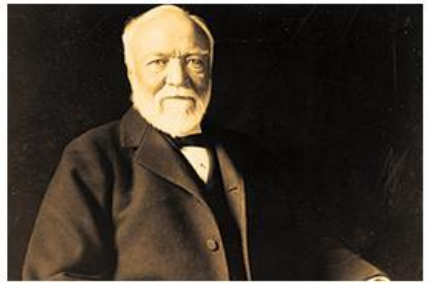
SWIFT Institute Cyber Security 3.0 – Better Together
Singapore I 18 August 2017

Proposal for an International Agreement to Protect Financial Stability Against Cyber Threats

The **Carnegie Endowment for International Peace** is a unique global network of policy research centers in Russia, China, Europe, the Middle East, India, and the United States. Our mission, dating back more than a century, is to advance the cause of peace through analysis and development of fresh policy ideas and direct engagement and collaboration with decisionmakers in government, business, and civil society. Working together, our centers bring the inestimable benefit of multiple national viewpoints to bilateral, regional, and global issues.

GLOBAL NETWORK | LEADERSHIP | HISTORY | AWARDS | SUPPORT

In 2006, Carnegie launched a revolutionary plan to build the first global think tank. Since then it has transformed a hundred-year-old American institution into



RESOURCES

Annual Report

Junior Fellows Program

Employment Opportunities

Conference Center

Library

Cyber Policy Initiative

IN THE SPOTLIGHT

ALL | PUBLICATIONS | EVENTS | ABOUT

EVENT

Launch: Toward a Global Norm Against Manipulating the Integrity of Financial Data

MICHAEL CHERTOFF, GREG RATTRAY, SIOBHAN MACDERMOTT, TIM MAURER, DUNCAN HOLLIS | JUNE 19, 2017 | WASHINGTON, DC | 中文

The G20 should commit not to manipulate the integrity of data and algorithms of financial institutions and to cooperate when such incidents occur.

OXFORD BIBLIOGRAPHIES: INTERNATIONAL RELATIONS AND CYBER SECURITY

The Carnegie Podcast

Tim Maurer, co-director of Carnegie Endowment's Cyber Policy Initiative and David Brumley, director of Carnegie Mellon's Security & Privacy Institute, sat down with Tom Carver to discuss security and cyberspace.

The Carnegie Pod... SOUNDCLOUD

The Carnegie Podcast is a regular series hosted by Tom Carver featuring commentary and analysis from Carnegie experts on critical global issues.

Sign up for

US/China agreement
(September 2015)

G20 agreement
(November 2015)

G20 agreement (November 2015)

26. We are living in an age of Internet economy that brings both opportunities and challenges to global growth. We acknowledge that threats to the security of and in the use of ICTs, risk undermining our collective ability to use the Internet to bolster economic growth and development around the world. We commit ourselves to bridge the digital divide. In the ICT environment, just as elsewhere, states have a special responsibility to promote security, stability, and economic ties with other nations. In support of that objective, we affirm that no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors. All states in ensuring the secure use of ICTs, should respect and protect the principles of freedom from unlawful and arbitrary interference of privacy, including in the context of digital communications. We also note the key role played by the United Nations in developing norms and in this context we welcome the 2015 report of the UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security, affirm that international law, and in particular the UN Charter, is applicable to state conduct in the use of ICTs and commit ourselves to the view that all states should abide by norms of responsible state behaviour in the use of ICTs in accordance with UN resolution A/C.1/70/L.45. We are committed to help ensure an environment in which all actors are able to enjoy the benefits of secure use of ICTs.

Actions speak louder than words

The New York Times | https://nyti.ms/28J9fyW

POLITICS

Chinese Curb Cyberattacks on U.S. Interests, Report Finds

By DAVID E. SANGER JUNE 20, 2016

WASHINGTON — Nine months after President Obama and President Xi Jinping of China agreed to a broad crackdown on cyberespionage aimed at curbing the theft of intellectual property, the first detailed study of Chinese hacking has found a sharp drop-off in almost daily raids on Silicon Valley firms, military contractors and other commercial targets.

But the study, conducted by the iSight intelligence unit of FireEye, a company that manages large network breaches, also concluded that the drop-off began a year before Mr. Obama and Mr. Xi announced their accord in the White House Rose Garden. In a conclusion that is largely echoed by American intelligence officials, the study said the change is part of Mr. Xi's broad effort to bring the Chinese military, which is considered one of the main sponsors of the attacks, further under his control.

As a result, the same political forces that may be alleviating the theft of data from American companies are also responsible for Mr. Xi's stunningly swift crackdown on the Chinese media, bloggers and others who could challenge the Communist Party.

"It's a mixed bag," said Kevin Mandia, the founder of Mandiant, now part of FireEye, which first detailed the activities of a People's Liberation Army cyber-arm, called Unit 61398, that had been responsible for some of the most highly publicized thefts of American technology. "We still see semiconductor companies and aerospace firms attacked."

But the daily barrage of attacks has diminished, which Mr. Mandia attributed to "public pressure" from, among others, the Justice Department's decision to indict five members of the P.L.A. unit about a year after its activities were exposed.

Carnegie’s proposal:

A cyber agreement to protect the stability of the global financial system against cyber threats

G20 Finance Ministers and Central Bank Governors

G20 Finance Ministers and Central Bank Governors

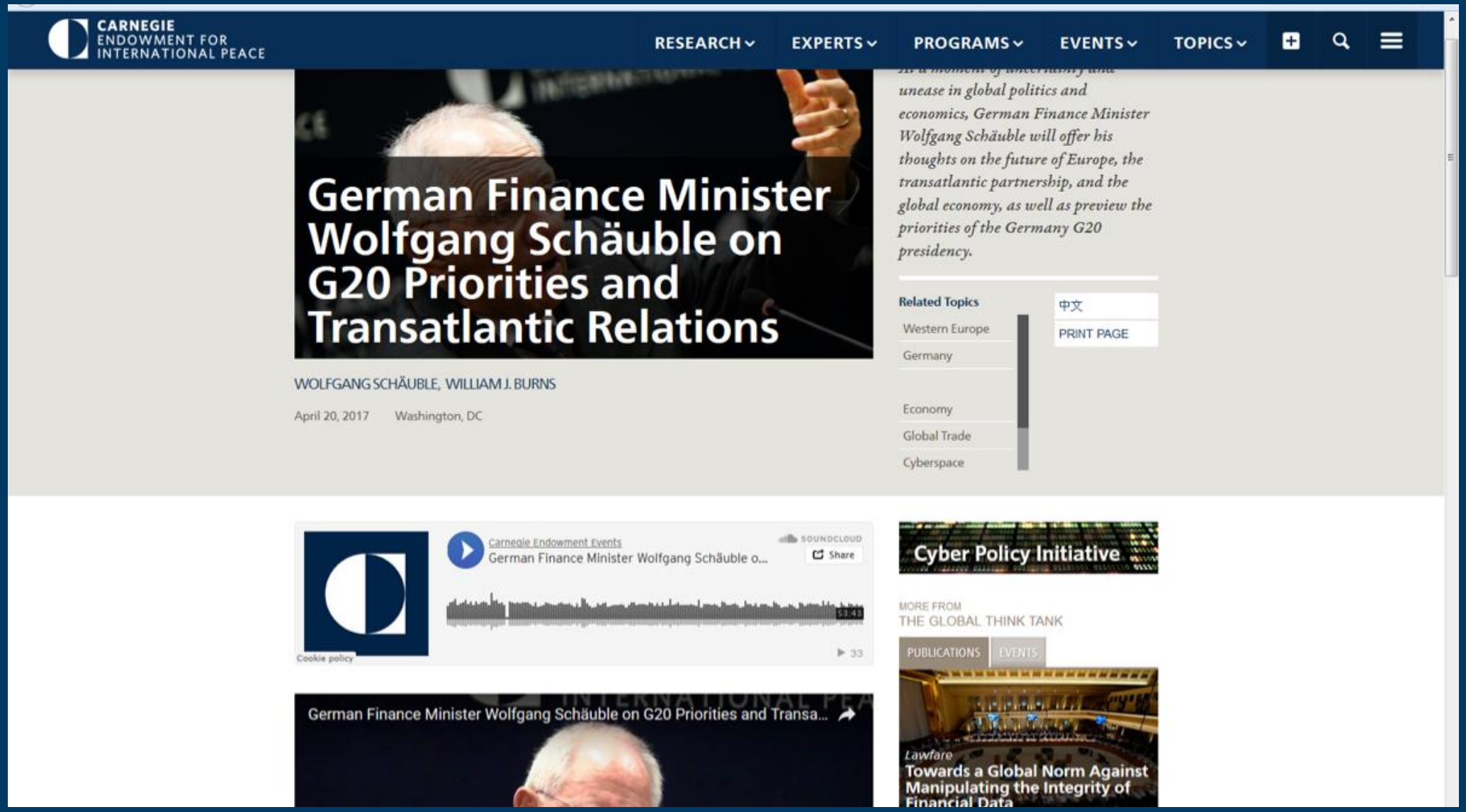
Communiqué

G20 Finance Ministers and Central Bank Governors Meeting

Baden-Baden, Germany, 17-18 March 2017

7. 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, as a first step, to perform a stock-taking of existing relevant released regulations and supervisory practices in our jurisdictions, as well as of existing international guidance, 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 stock-take report by October 2017.

many's Finance Minister speaking at Carnegie



Why focus on the financial system?

- **The financial system is different from other critical infrastructures such as the electrical grid or transportation system because of its global interdependence**

- **The source of a contagion and financial instability can be unexpected and from a single institution or other smaller players in the system**

  - Unexpected contagion effect resulting from collapse of a single financial institution: Lehman Brothers in 2007

  - Unexpected contagion effect from small player in global system: collapse of Thai baht triggering 1997 Asian financial crisis

Growing threat to countries around the world

2016 Bangladesh Central Bank heist based on credential theft

In February 2016, media reported that hackers had breached the network of the Bangladesh Central Bank and sent 35 fraudulent transfer requests to the Federal Reserve Bank of New York, totaling nearly USD 1 billion. Four of these fraudulent requests succeeded and the hackers were able to transfer USD 81 million to accounts in the Philippines, representing one of the largest bank thefts in history.

2015 malware currency manipulation through Russian bank

Russian-language hackers hacked into the computer systems of Russian-based Energobank starting in September of 2014. They were able to harvest credentials, launch their own trading software, and on February 27, 2015, they placed more than $500 million in orders at non-market rates that caused the exchange rate to swing with extreme volatility between 55 and 66 rubles per dollar for a period of 14 minutes. Energobank has claimed losses of $3.2 million due to the trades.

2013 disk-wiping attack on South Korean banks

“Dark Seoul” malware against the computer networks of three South Korean banks – Shinhan Bank, Nonghyup, and Jeju – resulting in data deletion and disruptions to ATMs and mobile payment systems. Shinhan Bank’s internet banking servers were temporarily blocked for part of the day leaving customers unable to perform online transactions, while operations at some branches of NongHyup and Jeju banks were paralyzed for two hours after the virus erased files on the infected computers.

Proposed norm
(to apply in peace and war time)

- **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.**

This principle comprises two ancillary obligations:

- **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.**

- **"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."**

Objectives

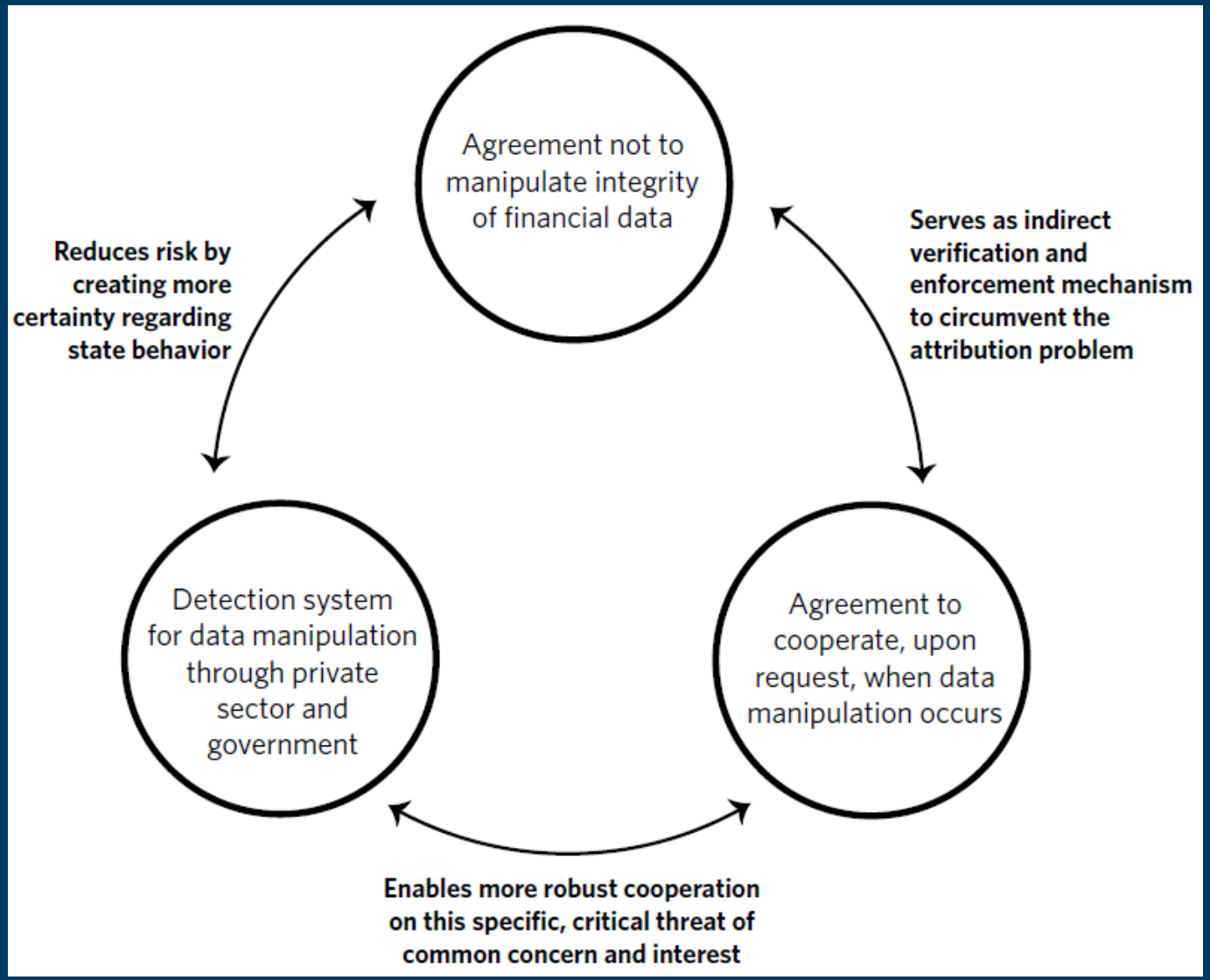
- **Send a clear signal** that the stability of the global financial system depends on preserving the integrity of financial data in peacetime and during war and that the international community considers the latter off limits;

- **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, the 2016 cyber guidance from the Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions (CPMI-IOSCO), and the 2017 stock-taking exercise by the Financial Stability Board

Three mutually reinforcing pillars



ISO 27000 definition of ‘information security’

Preservation of **availability, confidentiality**, and **integrity** of information

Open questions

- Given the potential significant effect for the system at large if certain data and systems are unavailable, how can availability be added and combined with the focus on the integrity of data in a meaningful framing and description?

- When an incident occurs involving the manipulation of the integrity of a financial institution's data, what cooperation are states expected to provide?

- What constitutes "financial institution?" Banks, stock markets, clearing houses, and/or insurers? Should all financial institutions be included or only systemically important ones at the global and national levels?

- Would the norm apply only among states who agree to accept it, or would those who accept the norm be obligated to apply its requirements and limitations even in the absence of a reciprocal commitment? How can states that are not members of the G20 become part of the agreement?

Reactions

THE HILL

Protecting financial netw cyberattacks

BY REP. PATRICK MEEHAN (R-PA.), OPINION CONTRIBUTOR - 04/04/17 01:00 PM EDT

84 SHARES

Just In...

NYT pans Michael Moore's new Broadway show
IN THE KNOW — 9M 23S AGO

OPINION | CNN's Trump shill Jeffrey Lord deserved to go, but not for that tweet
CONTRIBUTORS — 11M 11S AGO

Fancy Bear using leaked NSA tools: report
CYBERSECURITY — 21M 39S AGO

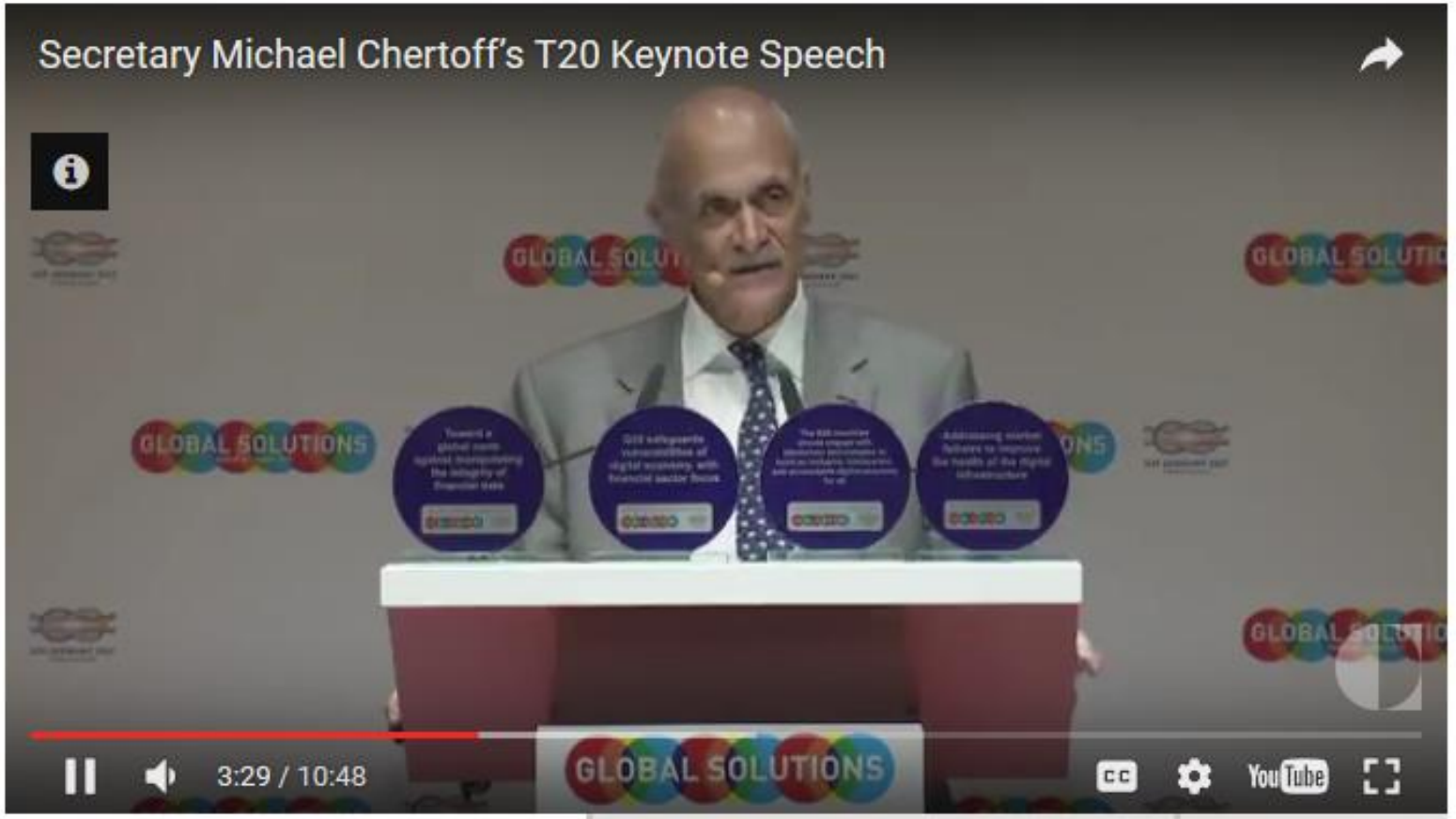
Small businesses need tax reform, not wholesale tax cuts
CONTRIBUTORS — 31M 11S AGO

Brooks seizes on Trump-McConnell feud
CAMPAIGN — 33M 5S AGO

© Getty Images

As a child, I stored my Industrial Valley Bank savings passbook in a shoebox at the foot of my bed – along with my other most treasured possessions like my Top Ten baseball cards. My savings then was the fruit of my labor shoveling snow and raking leaves. But more than that, my passbook's additions and subtractions represented something more fundamental and sacrosanct: where I stood with my financial affairs.

Reactions



Secretary Michael Chertoff's T20 Keynote Speech

Minister Schaeuble on Financial Data Integrity (Excerpt)

T20 Recomme Maurer on Dig

Key Discussion Resources

Michael Chertoff and Tim Maurer on Economic Cyber Security

Michael Chertoff, Tim Maurer | *The Carnegie Podcast*

Recording of event with Michael Chertoff, Greg Rattray, Siobhan MacDermott, Tim Maurer, and Duncan Hollis

Michael Chertoff, Greg Rattray, Siobhan MacDermott, Tim Maurer, Duncan Hollis | event

Steptoe Cyberlaw Podcast

Stewart Baker, Brian Egan, Tim Maurer, Paul Rosenzweig | *Steptoe Cyberblog*

www.protectingfinancialstability.org

Thank You

tmaurer@ceip.org