G20 INSIGHTS

G20 GERMANY 2017
THINK 20 DIALOGUE

POLICY AREA:
Digitalization

G20 safeguards vulnerabilities of digital economy, with financial sector focus

Barry Carin (Centre for International Governance Innovation (CIGI))

April 05, 2017

Abstract

The G20 can ensure a secure, resilient, sustainable and responsible digital economy, especially in the financial sector, by removing vulnerabilities in Internet infrastructure, encouraging cross-border cooperation, providing guidance to telecommunications regulators and implementing norms regarding cyber-attacks[1] [2].

Challenge

The digital economy faces a significant, perhaps existential, challenge that could compromise G20 plans to promote inclusive growth. Given Internet vulnerabilities and inadequate security, actions by criminal or terrorist actors can immediately have cross border consequences. There have been many costly instances of denial of service, ransomware and hacking of financial institutions. Breaches in the financial sector and in private sector records are widely reported. Cyber operations targeting the availability or integrity of data of financial institutions could undermine the stability and trust in the financial system. Credential theft, malware currency manipulation, disk-wiping attacks ("Dark Seoul" and "man in the browser"), distributed denial of service attacks have required banks to take defensive and remedial measures costing millions. As more devices and more services being connected to the Internet, they are increasingly susceptible to mischief and cyberattacks which diminish trust and could ultimately cripple the Internet.

The challenge is to catalyze innovation and international cooperation to exploit the potential of the digital economy for inclusive global growth and development, to upgrade traditional industries, and facilitate the structural reform, to minimize risks to the financial sector and other infrastructure, and to ensure security in a way that promotes creativity.

[1] This Policy Brief represents the result of the discussions by the **T20 Task Force on Digitalization**. The Task Force was chaired by Fen Osler Hampson (CIGI), He Fan (RDCY), Samir Saran (ORF) and Dennis Görlich (Kiel Institute).
[2] References specific to the financial sector are based on the research and proposal developed by Tim Maurer and the Cyber Policy Initiative of the Carnegie Endowment of international Peace.

Proposal

Summary

The German G20 presidency has set the themes for 2017 as "Resilience, Sustainability and Responsibility". Digitalization (infrastructure and standards and norms) is highlighted as a priority focus. The Internet, the global cyberspace, and the digital economy have great potential to increase growth and productivity. Innovation in data and digital tech can transform the manufacturing, transportation, energy, and financial sectors. But the potential is threatened by weaknesses in the digital infrastructure, the instability of international protocol coordination and the lack of effective cross-border cooperation. There is inadequate international coordination on crime and security to establish norms to deal with cyber threats. To ensure the necessary trust in the Internet and global cyberspace, international cooperation is required. A priority is protection of the financial sector, the foundation of the economy.

The G20 can catalyze the necessary initiatives by invitations to G20 Ministers responsible for the Internet and global cyberspace, to the Financial Stability Board and others and to establish a G20 Working Group on the Digital Economy.

Rationale

Individual nations cannot provide for the necessary resilience and sustainability of the digital economy. International cooperation based on existing international law is the only avenue. We need modern day equivalents to standard railway track gauges, aircraft safety requirements, telephone standards, and the 1929 International Convention for the Suppression of Counterfeiting Currency. Leadership is required to improve network operator practices, to cope with the developing "Internet of Things", to provide support for globally stable platforms for technical coordination and innovation, and to design global norms for cyber-attacks. However, despite the potential of the Internet, there are political pressures to "deglobalize", the result being inward-looking national solutions to address global issues.

Focus on cyber-sovereignty, borders and government control should also be carefully handled in the framework of effective international cooperation so that it will not threaten to splinter the Internet into separate networks based on incompatible technology and regulations. E commerce needs a proper environment to reach its potential. A recent Internet Society survey reports that 45% of Americans had changed their online behaviour because of their fears. A 2014 Report estimated cyber-attacks cost the global economy $445 billion annually. The surveillance software industry appears to have "turned email theft into a terrifying — and lucrative — political weapon". There have been calls for a software analogue to the 41 country Wassenaar Arrangement. The risk is a series of blunt and inefficient unilateral solutions that create residual damage, possibly larger damage than the problem to be solved.

International cooperation is essential to realize the Sustainable Development Goals' promise of access for the global population. International collaboration is indispensable to generate and maintain trust in both digital security and in privacy risk management. There is considerable room for improvement in network risk indicators and Service Providers' (ISPs) security provisions and device deployment processes. But there is a market failure – ISPs do not have sufficient incentive to address the

problems. The financial sector and its customers are bearing the risk of the failure of ISPs to maintain best practice management. Specific issues are adoption of the Internet Engineering Task Force's Best Current Practice of network operators to diminish "spoofing" (fake IP addresses disguising or masquerading identity) and requiring Internet service providers to regularly scan internally for inventory identification and mapping and to identify and rectify vulnerable Operating System/service versions.

There is a substantial basis for future G20 initiatives. The Global Commission on Internet Governance recommended government agreements on targets that are off limits to cyberattack, with a mutual-assistance pact to deter cyber intruders. The OSCE has worked on confidence building measures. There is a bilateral China US agreement on cyber espionage. The Bank for International Settlements (BIS) and the International Organization of Securities Commissions released a report in December 2016 on guidance on cyber resilience for financial market structures The UN Group of Government Experts (UNGGE) will issue a report on norm setting for cyber espionage in June 2017.

It has been suggested that G-20 governments build on existing work on norms regarding state-to-state cyber conflict. It could establish norms around more general cyber-attacks which generate physical harm. Communication channels and norms could be instituted among countries on hot to collectively manage incidents at both the diplomatic and technical levels.

The Internet of Things (IoT) opens a new source of vulnerability. Bruce Schneier has argued that the market has prioritized devices features and cost over security; devices built by teams that don't have security expertise; devices without security updates, or a way to be patched. He points out that when it comes to internet regulation, "there's no government structure to tackle this at a systemic level. Instead, there's a fundamental mismatch between the way governments work and the way this technology works that makes dealing with this problem impossible at the moment."

One approach is to insist on providing for accountability for outcomes. Software Liability may be inevitable – if not imminent now that IoT failures have physical consequences. With a compelling event or case law, done wrong, introducing liability could destroy the software industry. Done right, it is economic, in the interest of the public good and public safety, and could even be simulative to catalyzing real and measured cyber insurance.

There are many gaps in governance of the digital economy which require international collaboration to fill. One suggestion is to promote transparency in labeling to reveal distinctions among market alternatives and to permit evaluation of costs and risks. An internationally consistent IoT/Software Bill of Materials would ideally include ingredients from any 3rd party and open source software parts used in products. Listing known vulnerabilities would require justification. Product standards could be updated to require that IoT devices be patchable.

Vendors and/or ISPs could be legally required to offer life-long security updates.

There have been calls for a single regulatory agency to house required new expertise, because its applications cut across several preexisting agencies. There have been proposals for a U.S. National Institutes of Health along for cybersecurity, a Federal Robotics Commission, or a Department of Technology Policy.

Means to Implement

There are several avenues for G20 initiatives':

1. Commit that each G20 government will take specific steps to secure key aspects of their financial sectors under their control, as a first step to creating international norms:

   ◦Require that internet service providers give early warning of new infections and help their customers find and fix vulnerabilities.

   ◦Encourage the adoption by network operators of the Internet Society's Mutually Agreed Norms for Routing Security, or MANRS (https://www.manrs.org).

   ◦Utilize publicly available data on network risk indicators[3], to engage ISPs to encourage better device deployment processes and operational decisions.

2. Invite the U.S., China and Germany to prepare a joint report on means of cooperation to deploy better cyber defenses, to use payment-pattern controls to identify suspicious behavior, and to introduce certification requirements for third-party vendors to limit illicit activity.

3. Task G20 Energy Ministers to improve cyber resilience at power facilities, focused on removing malware and fielding better defenses.

4. Request G20 Ministers and regulators with Internet responsibility to report on options to:

   ◦Develop network risk indicators and review ISPs' security provisions and device deployment processes.

   ◦Require that IoT devices be patchable in a reasonable time frame, because future vulnerabilities are inevitable.

   ◦Legally require vendors and/or ISPs to offer life-long security updates.

   ◦Fund and coordination of research and development of tools and methodologies to build flawless systems from their conception.

   ◦Promote public education on cyber-hygiene and IoT labeling initiatives while ensuring broad public access to the Internet.

   ◦Update standards on data protection, privacy and the use of algorithms.

   ◦Incentivize competition to make the Internet and its devices accessible to all.

5. Request G20 Development Ministers for options to scale up existing effective initiatives, introduce innovative ideas, or expand the mandate of existing international institutions and arrangements to promote Internet accessibility, affordability and appropriate infrastructure.

6. The G20 agree to establish a G20 Working Group on the Digital Economy[4].

[3] Such as provided by the non-profit CyberGreen Institute.

Annex 1: G20 Working Group on the Digital Economy

◦Terms of reference could include to:

◦Follow up with the BIS on its recent report on cyber resilience of the finance sector.

◦Provide metrics and measure progress re the trustworthiness and security of the financial ecosystem.

◦Advise on national campaigns (like Y2K programs) to reduce the number of compromised computers.

◦Re IoT, report whether to establish an Internet Underwriters Laboratory, akin to the product- testing and certification system used for electrical appliances, to ensure internet-connected devices meet minimum security levels before commercial release.

◦Evaluate where accountability should fit into the software/IoT value chain.

◦Recommend means to provide affordable access to cybersecurity products;

◦Initiate a G20 conversation on securing digital supply chains.

◦Propose CERT to CERT cooperation and initiatives for capacity building of law enforcement agencies in developing countries.

◦Examine prospects for regulating surveillance software like arms and dual use technologies.

◦Advise on how to take work on cyber-espionage forward.

References

Bruce Schneier, "Testimony at the U.S. House of Representatives Joint Hearing "Understanding the Role of Connected Devices in Recent Cyber Attacks", November 16, 2016

http://nymag.com/selectall/2017/01/the-internet-of-things-dangerous-future-bruce-schneier.html

"The Internet of Things Is Wildly Insecure—And Often Unpatchable",Wired, January 6, 2014

Constance De Leusse
http://www.huffingtonpost.com/entry/critical-decisions-for-the-internets- future-at-this_us_5880787ce4b0fb40bf6c46d4

Internet Society, Global Internet Report 2016 "The Economics of Building Trust Online: Preventing Data Breaches"

Internet Society, "Mutually Agreed Norms for Routing Security"

Center for international and Strategic Studies "Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime" 2014

[4] Upgrading the G20 Task Force on the Digital Economy; terms of reference with illustrative options for their work program are provided in Annex 1.

Tim Maurer, "UN Body Considers International Cyber Norms", IHS Jane's Intelligence Review, 25 October 2016

Committee on Payments and Market Infrastructures & International Organization of Securities Commissions, "Guidance on cyber resilience for financial market infrastructures".

Mattias Schwartzian "Cyberwar for Sale", NYT Jan 4, 2017