Economics
The Open-Access, Open-Assessment E-Journal

Discussion Paper
No. 2017-27 | June 06, 2017 | http://www.economics-ejournal.org/economics/discussionpapers/2017-27

G20 safeguards digital economy vulnerabilities with financial sector focus

Barry Carin

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.

(Submitted as G20 Policy Paper)

JEL L86 L59 L96 O38
Keywords Digital economy; cyber security; global governance

Authors
Barry Carin, ✉ Centre for International Governance Innovation (CIGI) , bcarin@uvic.ca

The ideas in the Paper represent 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). Valuable contributions were provided by Tim Maurer, Paul Twomey, Julie Maupin and Emily Taylor. The effort was generously supported by the William and Flora Hewlett Foundation.

Citation Barry Carin (2017). G20 safeguards digital economy vulnerabilities with financial sector focus. Economics Discussion Papers, No 2017-27, Kiel Institute for the World Economy. http://www.economics-ejournal.org/economics/discussionpapers/2017-27

Received June 1, 2017 **Accepted as Economics Discussion Paper** June 2, 2017 **Published** June 6, 2017

Challenge

"Why everything is hackable:
Computer security is broken from top to bottom."
Economist magazine leader[1]

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"), and 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.

On March 18, 2017, G20 finance ministers and central bank governors sounded the alarm: "*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.*"[2]

A March 27, 2017 Carnegie Endowment for International Peace Cyber Policy Initiative paper listed cyberattacks on the financial systems of a dozen countries – "…. defacement of websites, DDoS attacks, and intrusions using more sophisticated malware. The targets of the incidents were mainly banks but also one stock exchange and one payment system, and the countries whose financial sectors were hit include Belgium, Brazil, Estonia, Georgia, Lebanon, Russia, South Korea, Ukraine, and the United States."[3]

In May 2017, the "wannacry" virus attacked thousands of computers encrypting files and demanding a ransom to free the files." According to Europol, Ransomware encrypted data on at least 75,000 computers in 99 countries in one day".[4]

---

1 http://www.economist.com/news/science-and-technology/21720268-consequences-pile-up-things-are-starting-improve-computer-security

2 G20 Finance Ministers and Central Bank Governors "Communiqué", University of Toronto, http://www.g20.utoronto.ca/2017/170318-finance-en.html .

3 Tim Maurer, Ariel Levite and George Perkovich, "Toward a Global Norm against Manipulating the Integrity of Financial Data", Appendix, http://carnegieendowment.org/files/Cyber_Financial_Data_white_paper.pdf

4 http://www.bbc.com/news/world-europe-39907965

The challenge is to catalyze innovation in modes and mechanisms of international cooperation to protect the potential of the digital economy for inclusive global growth and development, to upgrade traditional industries, and facilitate structural reform, to minimize risks to the financial sector and other infrastructure, and to ensure security in a way that does not compromise creativity.

Proposal

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. Secure digital infrastructure, improved international protocol coordination and effective international cooperation are required to ensure the necessary trust in the Internet and global cyberspace. The priority should be protection of the financial sector, the foundation of the economy. The G20 should establish new norms, formal institutions and informal arrangements to enable the necessary cooperation.

Rationale

The OECD Report[5]**, "**Key Issues for Digital Transformation in the G20", listed ten policy issues:[6]

Unfortunately, with respect to its sixth policy challenge, digital security, the OECD's toothless recommendation resembled milquetoast:

---

[5] January 2017 http://www.oecd.org/G20/key-issues-for-digital-transformation-in-the-G20.pdf

[6] https://www.slideshare.net/innovationoecd/g20-digital-economy-task-force-meeting-andrew-wyckoff

> "G20 economies could explore opportunities for strengthening co-operation and international arrangements that promote greater sharing of good practice and information."

In March 2017, *with the aim of enhancing cross-border cooperation*, G20 Finance Ministers and Central Bankers asked the *Financial Stability Board* (FSB) *to perform a stock-taking of existing relevant released regulations and supervisory practices in G20 jurisdictions.*[7] *The FSB* was asked for a progress report for the Leaders Hamburg Summit in July 2017 and for a stock-taking report by October 2017.
G20 Ministers for the Digital Economy met in April 2017 in Dusseldorf. There are three paragraphs in the G20 Ministerial Declaration (out of thirty three) on "strengthening trust in the digital world"[8]. The declaration expressed fine sentiments but lacked operational or verifiable commitments.

Annexed to the G20 Ministerial Declaration is a paper called "A Roadmap for Digitalisation: Policies for a Digital Future". There are eleven issues covered in the G20 Roadmap - securing trust is number 8. I**f everything is a priority, nothing is a priority.** In a sense, while all the eleven policy challenges are equal, digital infrastructures and security are "more equal". **The G20 must focus to be relevant and effective. To be sustainable and resilient, the Internet must first be made secure and resilient.** Without trust, the immense potential of the digital economy will not be realized.

The G20 Roadmap expresses the appropriate assessment:

> "Trust and security are fundamental to the functioning of the digital economy; without them, uptake of digital technologies may be limited, undermining an important source of potential growth and social progress."

But then instead of taking concrete action, the G20 Ministers simply noted that they intend to "Exchange experiences…. Encourage the development of national privacy strategies" and discuss the issues within the forthcoming Argentine Presidency.
The dilemma is that individual nations cannot unilaterally provide the underpinnings to ensure the necessary resilience and sustainability of the digital economy. International cooperation based on international law and consensus is the only avenue. The digital economy requires modern day equivalents to standardization of railway track gauges, aircraft safety requirements, telephony 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

---

[7] G20 Finance Ministers and Central Bank Governors, Communiqué," University of Toronto, March 18, 2017, Paragraph 7 http://www.g20.utoronto.ca/2017/170318-finance-en.html

[8] **"Shaping Digitalisation for an Interconnected World"** Paragraphs 26-28 https://www.bmwi-registrierung.de/G20-Task-Force-Meeting-3/pdf/G20%20Digital%20Economy%20Ministers%20Documents_070417.pdf

stable platforms for technical coordination and innovation; and to design global norms for cyber-attacks. However, despite the potential of the Internet, there are widespread political pressures to "deglobalize"; the unfortunate result being inward-looking national solutions to address global issues.

E-commerce needs a proper regulated environment to reach its potential. A recent Internet Society survey reports that trends on data breaches "cannot be allowed to continue without significant harm to individuals' privacy and users' trust in the Internet, resulting in lower and more selective use of the Internet".[9] 45% of Americans had changed their online behaviour because of their fears[10]. According to a recent German study, consumers are concerned about the protection of their personal data on the internet.[11] 72 per cent of the people surveyed in six G20 states were concerned that too many personal data are gathered online. More than two thirds were worried that online payments might not be secure. 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 on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. It has been reported that when the Houthi rebels took over Yemen`s capital and the Internet service provider, they used Netsweeper technology, software to put in place a draconian Internet censorship regime, blocking the entire Israeli domain. Canada has many export control doesn't restrict the sale of this type of technology. Netsweeper, based in Waterloo, Ontario, sells Internet "content filtering and web threat management solutions"—to organizations and governments around the world.[12]

The risk is that a series of well-intentioned but blunt and inefficient unilateral solutions will create residual damage, possibly larger damage than the problem to be solved. A May 2017 article on the Foreign Policy website noted:

> "According to a source with knowledge of a White House meeting…. Trump's team is considering launching an investigation into a Department of Homeland Security program that shares information on cyberattacks in an effort to coordinate globally on countering digital threats, insinuating that it inappropriately opened up streams of sensitive data to Russia and other non-allies."

---

9 https://www.internetsociety.org/globalinternetreport/2016/wp-content/uploads/2016/11/ISOC_GIR_2016-v1.pdf

10 https://www.internetsociety.org/sites/default/files/bp-Trust-20170314-en.pdf

11 Study produced by the Federation of German Consumer Organizations, presented at the March 2017 G20 Consumer Summit https://www.g20.org/Content/EN/Artikel/2017/03_en/2017-03-15-g20-verbrauchergipfel_en.html?nn=2069594

12 https://www.theglobeandmail.com/report-on-business/rob-magazine/why-canadas-hacker-king-is-very-afraid/article34471769/

Cyber-sovereignty, borders and government control must be carefully handled in the framework of effective international cooperation. Otherwise the Internet could be splintered into separate networks based on incompatible technology and regulations.

International cooperation is essential to realize the Sustainable Development Goals' promise of affordable 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 Internet 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 risks and consequences 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 (ISPs) 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 consideration of potential future G20 initiatives. The Global Commission on Internet Governance recommended government agreements on targets that should be 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. In addition to the forthcoming FSB reports, the UN Group of Government Experts (UNGGE) will issue a report on norm setting for cyber espionage in June 2017.

Tim Maurer has suggested that G-20 governments could build on formulate and endorse a G20 norm regarding state-to-state cyber conflict, such as:

> "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."[13]

The G20 could establish norms around more general cyberattacks which generate physical harm. Communication channels and norms could be instituted among countries on how to collectively manage incidents at both the diplomatic and technical levels.

[13] http://carnegieendowment.org/files/Cyber_Financial_Data_white_paper.pdf

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."[14]

One approach is to insist on providing for accountability for outcomes. Legal liability for software may be inevitable – if not imminent now that IoT failures have physical consequences. With a compelling tragic event, or case law done wrong, introducing liability could destroy the software industry. "The industry will fight any attempt to impose liability absolutely tooth and nail".[15] Industry will raise the spectre of delays analogous to the introduction of new drugs due to regulation of the pharmaceutical industry. Done right, legal liability is in the interest of the public good and public safety, and could even be stimulative to catalyzing appropriate 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 existing 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

What can be expected of the G20? We must remember that the G20 is only a forum for dialogue – the "premier forum for our international economic cooperation"[16]. The G20 does not take "decisions". It was never intended to usurp the mandates of existing international organizations. The G20 is an informal arrangement, without treaty-basis, charter, constitution

---

[14] 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. https://www.schneier.com/essays/archives/2016/11/testimony_at_the_us_.html

[15] http://www.economist.com/news/science-and-technology/21720268-consequences-pile-up-things-are-starting-improve-computer-security

[16] Paragraph 11 http://www.g20.utoronto.ca/analysis/commitments-09-pittsburgh.html

or binding bylaws. **However, t**here are several kinds of constructive outcomes that can emerge from a meeting of G20 Leaders.[17]

G20 Leaders can:

- commit themselves to specific actions in their individual countries;
- invite their own portfolio ministers or working groups of officials and experts to undertake specific actions;
- establish a High Level Panel or expert group with specific terms of reference;
- request international organizations to pursue specific tasks;
- initiate the creation of entirely new international organizations or informal arrangements.

There are six practical avenues for G20 initiatives to address vulnerabilities in the digital economy:

1) Each G20 government could commit to take specific steps to secure its financial sectors by regulations for ISPs and network operators:
    - Require ISPs to 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 (MANRS)[18];
    - Engage ISPs to encourage better device deployment processes and operational decisions, utilizing publicly available data on network risk indicators, such as provided by the non-profit CyberGreen Institute[19].

2) The G20 presidency could invite the U.S., China and Germany to prepare a joint report on means of international 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) G20 Leaders could request G20 Ministers and regulators with Internet responsibility to report on options to modernize and "vaccinate" the Internet:
    - 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;

---

[17] Carin and Shorr, "The G20 as a Lever for Progress", CIGI G20 Papers, No. 7, February 2013, https://www.cigionline.org/sites/default/files/g20no7_0.pdf

[18] https://www.manrs.org

[19] http://www.cybergreen.net/

- 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.

4) G20 Leaders could task their Energy Ministers to improve cyber resilience at power facilities, focused on removing malware and fielding better defenses;

5) G20 Leaders could invite their Development Ministers to report on 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 could appoint a High Level Advisory Panel and upgrade the G20 Task Force on the Digital Economy into a formal G20 Working Group. Illustrative options for their terms of reference and work program are provided in Annex 1.

Annex:

High-Level Advisory Panel / formal G20 Working Group on the Digital Economy Proposed Remit

- Follow up the G20 Finance Ministers and Central Bank Governors March 2017 request to the FSB on the resilience of the financial sector against the malicious use of ICT;
- Propose concrete international cooperation, beyond the commitment to exchange experiences encourage the development of national privacy strategies and discuss issues of the April 2017 **G20 Digital Economy Ministerial Declaration;**
- Follow up with the BIS on the options for international cooperation, based 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 cooperation among Community Emergency Response Teams in developing countries and initiatives for capacity building of their law enforcement agencies;
- Examine prospects for regulating surveillance software like arms and dual use technologies;
- Advise on how to take work on cyber-espionage forward.

Useful References

1. http://nymag.com/selectall/2017/01/the-internet-of-things-dangerous-future-bruce-schneier.html
2. "The Internet of Things Is Wildly Insecure—And Often Unpatchable",Wired, January 6, 2014 https://www.schneier.com/essays/archives/2014/01/the_internet_of_thin.html
3. Constance De Leusse http://www.huffingtonpost.com/entry/critical-decisions-for-the-internets-future-at-this_us_5880787ce4b0fb40bf6c46d4
4. Internet Society, Global Internet Report 2016 "The Economics of Building Trust Online: Preventing Data Breaches" https://www.internetsociety.org/globalinternetreport/2016/
5. Internet Society, "Mutually Agreed Norms for Routing Security" https://www.routingmanifesto.org/
6. Center for international and Strategic Studies "Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime", 2014 https://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf
7. Tim Maurer, "UN Body Considers International Cyber Norms", IHS Jane's Intelligence Review, 25 October 2016 http://www.janes.com/article/64878/un-body-considers-international-cyber-norms
8. Committee on Payments and Market Infrastructures & International Organization of Securities Commissions, "Guidance on cyber resilience for financial market infrastructures". https://www.bis.org/cpmi/publ/d146.pdf
9. Mattias Schwartzian "Cyberwar for Sale", NYT Jan 4, 2017 https://www.nytimes.com/2017/01/04/magazine/cyberwar-for-sale.html?_r=2
10. https://www.g20.org/Webs/G20/EN/G20/Calendar/calendar_node.html
11. https://www.g20.org/Content/EN/Artikel/2017/03_en/2017-03-15-g20-verbrauchergipfel_en.html - consumer meeting