Building Global Digital Supply Chain Hub by Cybersecurity Commitment: Singapore's Strategic Role in the Digital Age

By Keman Huang, Stuart Madnick and Nazli Choucri - 19 October 2020

WORLD ECONOMY, TRADE AND FINANCE

Keman Huang, Stuart Madnick and Nazli Choucri argue that Singapore must lead the world in developing a global standardized cyber code for digital trade.

Salience of Digital Trading

Digital trade is growing in importance: it contributed to 10% of the global GDP in the last decade by enabling cross-border e-commerce. However, accompanied by sustained digital innovations, weak cybersecurity is becoming a growing threat to digital trading. Unfortunately, there are no global rules for managing digital trade, let alone rules to address challenges to cybersecurity issues in the domain of digital trade.

An international effort to develop a global standardized cyber code is not a luxury for digital trade. It is a necessity. Concerns surrounding cybersecurity in digital trade are global in scale and scope. The diversified circumstances and inconsistent actions that can lead to different outcomes, sometimes become a source of provocation, and even result in international conflicts. Fragmented efforts to manage various cybersecurity threats can also increase, instead of reduce cyber risks in all digital trade.

Failed Efforts

For the last decade, cyber norm discussions in the international community have focused on the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE). However, the UN GGE failed to reach a consensus in 2018 due to divergence of interests, raising the possibility that such efforts since 2010 were all for nothing. The failure of the UN GGE dialogue to achieve general cyber norms has led the international community to develop cyber norms in specific

domains that would have practical applications. Given the increasing importance of digital trade, it is time to develop cyber norms to manage cybersecurity within digital trade.

The Singapore Advantage

To develop practical cyber norms of digital trading, the international community needs a leader who is willing and capable of consistently promoting progress. Given its strategic role in the digital age and previous cybersecurity initiatives, our framework suggests that Singapore is best positioned to take such a lead. Beyond its current commitment to cybersecurity as part of its national strategy, Singapore should consolidate its institutional cybersecurity capacity to cover the digital supply chain, promote a cybersecurity innovation ecosystem, and develop practical cybersecurity norms to harmonize the digital trade policies.

From Physical Supply Chain Hub to Digital Supply Chain Hub

Digitalization has changed the determinants for national supply chain strategies' success. Digital supply chains rely on unimpeded data flows more than ever. Competitiveness is less dependent on geographic location, but the capability to connect different digital markets and guarantee cybersecurity for those connections.

As Singapore has been a hub for the physical supply chain due to its strategic location at the convergence of the main trade routes, keeping its position as a supply chain hub in the digital age is its top national priority. To that end, Singapore has dedicated significant resources to cybersecurity capability development. Since 2015, the Cyber Security Agency ("the CSA") under the Prime Minister's Office -- established for "overseeing cybersecurity strategy, operation, education, outreach, and ecosystem development" -- has become a catalyst for cybersecurity. Singapore has signed several bilateral cooperation agreements, declarations, and memorandums with different stakeholders, including the U.S., Canada, the UK., Japan, Germany, Australia, France, and Cisco and Financial Services Information Sharing and Analysis Center (FS-ISAC). In 2018, ASEAN invited Singapore "to propose a mechanism to enhance cooperation among the ASEAN countries." Singapore's commitments to cybersecurity have made it one of the most cyber-secure states and the second-best place to do business in the world. Such first-hand experience in cyber norm development has gained Singapore the strategic position to become a global digital supply chain hub.

Consolidate Institutional Capacity to Cyber Secure Digital Supply Chain

To align the long-term efforts in cybersecurity and the mission to be a digital supply chain hub, consolidating a consistent and effective institutional capacity building for national cybersecurity and incorporate the global digital supply chain is the cornerstone.

Singapore's CSA was established as a separate government agency to focus exclusively on national cybersecurity strategies, thus preventing confusion on the distribution of tasks among government agencies and providing an environment for fast decision-making. The ultimate aim is "not only to build defenses for the cyber threat of the day, but to tackle cyber threats of tomorrow." As a strong advocate of leadership in digital trade, in 2014 Singapore initiated the Smart Nation program (SNP) office to "harness the power of networks, data and information and communication technologies to improve living, create economic opportunity and build a

closer community." In September 2018, Singapore officially launched the Networked Trade Platform (NTP) as a one-stop interface to enable trading and improve operational efficiency.

Building on these capabilities, Singapore can take a step further to cover the entire digital supply chain. At a minimum, this could include establishing a working group on "cybersecurity and digital trade", tasked with developing a roadmap for a cyber-secure digital supply chain hub. Such a move will enable Singapore to consolidate a well-designed and coherent cybersecurity strategy.

Promote Cybersecurity Innovation to Cyber Secure Digital Supply Chain Hub

Currently, countries are adopting different and sometimes conflicting policies for data localization and privacy policies. Public policy barriers to digital trade now replace physical frontiers. Supporting cybersecurity innovation and technological development as a national policy to serve as the cyber-secure "third-country" to connect different digital markets and enable cross-border data flow worldwide is a critical feature of a digital supply chain hub.

The commitment to cybersecurity has succeeded in drawing business to Singapore. The Singapore government is among the world's best for digital capabilities and achievements. World tech companies' moving to Singapore reinforces Singapore's position as a regional hub in innovation and technological development. Complementing the previous efforts, Singapore could develop a policy toolkit to promote cybersecurity innovations further. For example, Singapore should strengthen its ability to support innovations, such as privacy-supported distributed ledger technology, to bridge and secure the cross-border data flow among fragmented digital markets. Singapore should also encourage and incubate services related to cybersecurity testing and auditing and promote a trusted global cybersecurity certification center. Cybersecurity testing and auditing are becoming best practice vehicles within the global digital supply chain, as mechanisms to build trust among different stakeholders, including government and industry. Given that testing and auditing procedures may require the disclosure of sensitive intellectual property and trade secrets, Singapore can serve as a reliable and impartial global actor and leader to ensure that the industry adopts best practices for any cybersecurity certification scheme.

Develop Practical Cyber Norms within Digital Trading

Developing robust normative contents to support institutionalization and capacity building is the key to sustained cybersecurity efforts. All efforts to date -- such as the annual Singapore International Cyber Week, the ASEAN Ministerial Conference on Cybersecurity, the cybersecurity leadership among ASEAN countries, and the bilateral cooperation agreements, declarations, and memoranda supported by many stakeholders -- have handed Singapore a global platform to develop cyber norms for digital trade. This is a specific domain with specific dilemmas. For example, Singapore could use its leadership in ASEAN to harmonize cybersecurity responses to digital trade policy within ASEAN countries and then expand the discussion to ongoing global dialogues. Using its experience in creating cybersecurity initiatives and its existing practices in the digital supply chain, Singapore could bring different stakeholders together to develop and promote the cyber norms for digital trade.

Just as the Computer Emergency Response Teams Coordination Center (CERT/CC) was designed to improve software and Internet security broadly, a global process focusing on

cybersecurity capacity building for digital trade can be established and help other states to develop or strengthen required institutional capacities. Singapore can be the initiator and leader for such global processes, support its partners to build the cybersecurity capability, and frame practical cyber norms for digital trading.

Building the Digital Supply Chain Hub Supported by Cybersecurity Capability

Building a global, open, and cyber-secure digital trade is a strategic mission for the worldwide community in the digital age. Implementing a global cyber norm platform to develop specific and practical cyber norms for the digital supply chain can create synergy and forge the necessary momentum.

Singapore's commitments to and efforts supporting cybersecurity have been paying off, making it a leader on these issues. Singapore could further enhance their cyber effectiveness and push the adoption of cybersecurity norms globally to build a global digital supply chain hub. This is a mission with a vision that Singapore can offer the world – and lead in its realization. It is incumbent upon Singapore to take on this challenge, as it is for the global community to accept the challenge and both mission and vision.

Authors' note: The research reported herein was supported in part by the MIT Internet Research Policy Initiative funded by the Hewlett Foundation, Cybersecurity at MIT Sloan, which is funded by a consortium of organizations, and MIT Policy Lab at the Center for International Studies.

Dr. Keman Huang is a research scientist at the MIT Sloan School of Management, where he works on cybersecurity management and policy, innovation ecosystems, and big data analysis.

Prof. Stuart Madnick is the John Norris Maguire (1960) Professor of Information Technologies in the MIT Sloan School of Management, Professor of Engineering Systems in the MIT School of Engineering, and Director of Cybersecurity at MIT Sloan (CAMS): the Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity. He has been active in the cybersecurity field since co-authoring the book Computer Security in 1979.

Prof. Nazli Choucri is the Professor of Political Science, Faculty Affiliate at MIT Institute for Science and Data (IDSS) and Senior Faculty at the Center or International Studies (CIS). Her research focuses on international relations, with special attention to growth and expansion– in "real" and cyber systems.

Photo by Negative Space from Pexels / FacebookTwitterShare