September 2022

US-Singapore: Advancing Technological Collaboration and Innovation in Southeast Asia

Manoj Harjani
Andreas Kuehn, PhD
Courtney Weatherby
Natalie Pang, PhD

Edited by Mark Bryan Manantan

PACIFIC FORUM
INTERNATIONAL

September 2022

US-Singapore: Advancing Technological Collaboration and Innovation in Southeast Asia

Manoj Harjani
Andreas Kuehn, PhD
Courtney Weatherby
Natalie Pang, PhD

Edited by Mark Bryan Manantan

PACIFIC FORUM
INTERNATIONAL

About the Editor

Mark Bryan Manantan is Senior Reseearch Fellow and Director of Cybersecurity and Critical Technologies at the Pacific Forum in Honolulu, Hawaii. His current research focuses on the nexus of diplomacy, security, and governance of technology and innovation in Southeast Asia and the Indo-Pacific. He is also a non-resident fellow at the Center for Southeast Asian Studies, National Chengchi University, Taiwan, and formerly a research consultant at the Asia Society Policy Institute, Washington, DC. Prior to that, he held visiting fellowships at the Japan Foundation, the Center for Rule-Making Strategies at Tama University in Tokyo, Japan, and the East-West Center, Washington, DC.

Acknowledgements

The Pacific Forum is grateful to the many experts and practitioners for participating throughout the course of the US-Singapore Tech & Innovation Virtual Dialogue.

Our special appreciation to Crystal Pryor, PhD, Carol Li, Hannah Cole, Sholto Byrnes, Claire Tiunn (Chang), Doyeong Jung, and Jesslyn Cheong.

This project was made possible with support from the US Embassy in Singapore.

PACIFIC FORUM
INTERNATIONAL

About the Pacific Forum

Based in Honolulu, the Pacific Forum is a foreign policy research institute focused on the Asia-Pacific Region. Founded in 1975, the Pacific Forum collaborates with a broad network of research institutes from around the Pacific Rim, drawing on Asian perspectives and disseminating project findings and recommendations to global leaders, governments, and members of the public throughout the region. The Forum's programs encompass current and emerging political, security, economic, maritime, and technology policy issues, and work to help stimulate cooperative policies through rigorous research, analyses, and dialogue.

The Pacific Forum

Web: www.pacforum.org
Facebook: Pacific Forum
Twitter: @PacificForum
Instagram: @pacforum
Podcast: Indo-Pacific Current
Email: pacificforum@pacforum.org

Table of Contents

About the Authors

Manoj Harjani

Manoj Harjani is a Research Fellow in the Future Issues & Technology cluster at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University. Prior to joining RSIS, Manoj was in the Singapore Public Service, with stints at the Public Service Division, Prime Minister's Office Strategy Group, and Ministry of Trade and Industry. Manoj holds a Bachelor of Arts in Political Science from the National University of Singapore.

Andreas Kuehn, PhD

Dr. Andreas Kuehn is a Senior Fellow at the Observer Research Foundation America where he leads research on international cybersecurity cooperation within ORF America's Cyberspace Cooperation Initiative. His work focuses on the new risks and challenges in international security at the intersection of emerging technology, cybersecurity, and technology governance. Prior to joining ORF America, Dr. Kuehn was a Senior Program Associate at the EastWest Institute, where he led the development of EWI's breakthrough group efforts and worked on US-Russia and US-China cybersecurity issues. Before that, he was a Cybersecurity Fellow at Stanford University and an adjunct researcher at the RAND Corporation. He received his MSc in Information Systems from the University of Zurich and holds a PhD in Information Science and Technology from Syracuse University.

Courtney Weatherby

Courtney Weatherby is Deputy Director of the Stimson Center's Southeast Asia Program and Research Analyst with the Energy, Water, & Sustainability program. Her work focuses on infrastructure and energy development challenges in Southeast Asia and the Indo-Pacific, particularly food-water-energy nexus issues in the Greater Mekong Subregion. Weatherby was lead author on a range of technical and policy studies, including Thailand's Energy Development Pathways report in collaboration with Pact; the International Union for the Conservation of Nature (IUCN) Sekong, Sesan, Srepok Basin Energy Profile report; and the Stimson Center reports Alternative Development Pathways for Thailand's Sustainable Electricity Trade with Laos. She has authored and co-authored numerous short pieces for a range of online publications including the Bangkok Post, Nikkei Asian Review, and China Dialogue. She served as a US-Japan-Southeast Asia Fellow at the East-West Center in Washington, DC in early 2019, focusing on US-Japan collaboration on energy infrastructure. Before joining Stimson as a research associate in 2014, Weatherby worked briefly with the Center for Strategic and International Studies and the State Department. She holds an MA in Asian Studies from the School of Foreign Service at Georgetown University and a BA in East Asian Studies with honors from Dickinson College.

Natalie Pang, PhD

Dr. Natalie Pang is a Senior Lecturer and Deputy Head at the Communications and New Media Department and Principal Investigator at the Centre for Trusted Internet and Community at the National University of Singapore. She is a researcher and educator in digital citizenship and well-being, as well as digital humanities and data cultures in smart cities. She has published in various top-tier journals including New Media & Society, Computers in Human Behavior, Telematics & Informatics, and the Journal of the Association of Information Science and Technology. She also serves on a number of editorial boards, including the Asian Journal of Communication, and the International Journal of Information, Diversity, & Inclusion.

Introduction

The United States and Singapore at the Digital Crossroads

Mark Bryan Manantan

Despite the pandemic-induced economic contraction, Southeast Asia's digital economy has lately experienced a dramatic boost. A staggering 60 million consumers came online in Southeast Asia since the pandemic erupted in 2020—pumping the region's projected internet economy, which is expected to reach USD 360 billion by 2025. For better or for worse, COVID-19 has been the catalyst for the region's rapid digital transformation. Remote work has accelerated the use of cloud services, integration of Artificial Intelligence (AI) and machine learning systems, and the Internet of Things. Increased reliance on internet and mobile devices while staying at home has resulted in upward trends in e-commerce and distance learning. At least 10 percent of the adult populations in Malaysia, Vietnam, Thailand, Indonesia, and Singapore use e-wallets, making ASEAN economies global leaders in digital payments.[1] With Southeast Asia's bullish outlook on becoming a digitally enabled economy, the stage is set for the region to compete in the global tech arena. There is an increasing flow of investments in rising and homegrown unicorns like ridesharing and food delivery apps Grab and Gojek, as well as e-commerce giants Tokopedia and Lazada.[2]

As the world eases into the new normal, ASEAN is eager to leverage its digital economic gains to drive its post-pandemic recovery and spur sustainable innovation. The launch of the ASEAN Digital Masterplan (ADM) 2025 was a significant development that signals the region's growing appetite to accelerate inclusive digitalization efforts to jumpstart economic recovery and deal with climate change through the wider adoption of energy-efficient technologies that can reduce carbon emissions.[3] To reinforce ASEAN's digital initiatives in the post-pandemic era, the *Bandar Seri Begawan Roadmap: An ASEAN Digital Transformation Agenda to Accelerate ASEAN's Economic Recovery and Digital Economy Integration* was released in May 2021. It aims to conduct a preliminary study on the ASEAN Digital Economy Framework Agreement (DEFA) by 2023 and kickstart possible negotiations by 2025.

ASEAN's prospects of becoming a digital economic powerhouse in the next decade are promising, although member states must overcome various challenges. The region is still grappling with a lack of infrastructure and internet connectivity, resulting in uneven digital maturity, which further exacerbates the already sobering digital divide.[4] As more technologically advanced countries like Singapore, Malaysia, Indonesia, the Philippines, Thailand, and Indonesia move in the upper-value chain of technology production and consumption, less digitally connected countries like Myanmar, Laos, and Cambodia could be left far behind.[5]

With increased technology adoption comes more attack surfaces for malicious actors.[6] If left unaddressed, the checkered allocation of cybersecurity investments and capacity gaps across ASEAN could cause the region financial and reputational damage, especially in the face of advanced persistent threats or in the event of a major cyber-attack.[7] Although the pandemic has highlighted the urgency for increased cybersecurity spending to manage hybrid work set-ups and migrate to cloud-based infrastructure, more can be done to plug existing cybersecurity gaps.[8] Similarly, the disparities underpinning the region's data governance structure may hamper its foray inestablishing a viable AI ecosystem.[9]

The United States has been working with ASEAN in close collaboration with Singapore to help bridge the persistent gaps that continue to hamstring Southeast Asia's prospects in the digital economy. Given Singapore's unique position as a vital node of innovation in the region, the US has cultivated an active approach to engage the city-state to implement regional programs to mitigate the consequences of cyber insecurity and facilitate technological partnerships through increased capacity-building. Several initiatives that seek to foster policy and technical cooperation and partnerships in the digital economy and bolster cybersecurity and resiliency across Southeast Asia include the Singapore-United States Third Country Training Program,[10] the US-Singapore Cybersecurity Technical Assistance Program for ASEAN countries,[11] as well as the Singapore-led ASEAN-Singapore Cybersecurity Centre of Excellence,[12] where the US serves as a member of the Interational Program Committee on Capacity Building. Due to the growing importance of cybersecurity within the US-Singapore strategic partnership, the two countries established the US-Singapore Cyber Dialogue in March 2022 to expand existing areas of cooperation to tackle critical technologies, international standards, and supply chain security.[13]

Over the past two years, the Pacific Forum has borne witness to the unfolding digital transformation in Southeast Asia, as well as the rapid growth in cybersecurity and tech partnerships and developments between Singapore and the US. From the height of the global health crisis to the current era of post-pandemic recovery, the Pacific Forum held two back-to-back track 1.5/track

2 virtual dialogues, starting with the US-Singapore Cyber&Tech Security Virtual Series (2020-2021) and subsequently the US-Singapore Tech & Innovation Virtual Dialogue (2021-2022). At the inaugural US-Singapore Cyber&Tech Security Virtual Series (2020-2021), discussions were oriented toward safeguarding critical national infrastructure, threat information sharing, promoting data free flow, and advancing international norms and standards in cyberspace and emerging technologies like AI. Building on the lessons learned from the inaugural US-Singapore Cyber&Tech Security Virtual Series (2020-2021), the recently concluded US-Singapore Tech & Innovation Virtual Dialogue (2021-2022) went further to dissect niche yet interrelated areas of the digital transformation trend spanning supply chains, green energy technology, smart cities, and sustainability and strategic and technological competition with various stakeholders from government, industry, academia, and civil society.

In mounting the US-Singapore Tech & Innovation Virtual Dialogue, attention was devoted to key political, security, and technological events that have had a direct impact on US-Singapore relations and the broader Indo-Pacific. We adapted our open and closed-door virtual sessions to ensure that the unprecedented war in Ukraine, as well as the drastic change in American foreign policy post-Trump—following the election of President Joe Biden in 2020—were considered, given the consequential impacts of these events in Southeast Asia and the Indo-Pacific writ large. Of course, the protracted strategic competition between the US and China and the greater call to action on climate change were also factored in during the six-part virtual discussions.

Although the Biden presidency has offered some relief in the aftermath of Trump's America First Policy, with the proactive return of the US to the political, security, and diplomatic orbit, some observers in the region argue that the ground has further tilted in favor of China in Southeast Asia. Confronted with this reality, the US must wrestle with the fact that it must compete more with China to regain influence and lost confidence among stakeholders in the region, both in political-security and economic terms. In response to such challenges, the Biden administration heralded a diplomatic comeback through various initiatives such as the reinvigoration of the US-ASEAN Summit and the launch of the Indo-Pacific Economic Framework for Prosperity (IPEF).

The confluence of these events and the insights drawn from the US-Singapore Tech & Innovation Virtual Dialogue serve as the foundation of this digital publication. Here, authors were encouraged to reflect on what stronger US and Singapore cooperation would look like in concrete policy terms in the face of the ongoing geopolitical volatility. But beyond the technical and geopolitical perspectives, the contributions in this edited volume also emphasize the importance of cross-sectoral collaboration and sustainability as the ambit of an enduring US-Singapore strategic partnership.

Leveraging their distinct expertise, select panelists from the virtual dialogue tackled niche areas of the digital economy, emerging technologies, and innovation in the context of the US and Singapore. Manoj Harjani's piece assesses the long-term implications of Singapore's sanctions against Russia. Harjani canvassed the drivers of Singapore's decision to use export controls on military and select dual-use goods that the Kremlin may use to conduct cyber operations. He also discussed Singapore's efforts to target cryptocurrency loopholes as part of the city-state's sanctions package against Russia. However, such an expansion of sanctions in the digital economy—data, digital payments, and e-commerce—could hurt Singapore and Southeast Asia in the long haul, given their exposure to global value chains and research and development amid geopolitical tensions over critical and emerging technologies. Andreas Kuehn's "Defending Supply Chain Cybersecurity: Opportunities for Singapore-United States Cooperation," examines the growing importance of supply chain cybersecurity frameworks, given the growing complexity of supply chains and the multiplicity of Information and Communications Technology (ICT) providers. Going just beyond the "Know your ICT supplier" to ensure accountability and transparency, Kuehn offers practical advice on how Singapore, as an innovation hub in Southeast Asia in cooperation with the US, can test pilot new initiatives to safeguard supply chain cybersecurity at the organizational, industry, and multilateral levels.

Courtney Weatherby investigates Southeast Asia's conundrum on how to meet its carbon emission targets amid increasing pressure on supply chain resilience and energy transitions. Weatherby explores the increasing integration of digital technologies in Southeast Asia to achieve energy sustainability, like smart meters for data analysis and predictions. Furthermore, she highlights the growing role of blockchain technologies in facilitating renewable energy certification given the growing intra-ASEAN energy trade. Reflecting on the outcomes of the US-ASEAN Summit and relatedly the IPEF, Weatherby notes the shared expertise of the US and Singapore in capacity-building to lubricate Southeast Asia's ongoing energy transition. Recognizing the region's medium to long-term prospects in the data-driven economy, Natalie Pang examines the urgency of addressing the current gaps and vulnerabilities in Southeast Asia's digital future. Pang highlights the need to fast track digital literacy to address burgeoning concerns over privacy and algorithms, as well as the increasing negative effects of electronic waste or e-waste, mainly from large data centers, that carry environmental and health risks for local communities. Pang puts forward an invitation addressed to American and Singaporean stakeholders to imagine and hopefully contribute to shaping a digital future in Southeast Asia that promotes sustainability and equity.

The headwinds emanating from the geopolitical volatility in Europe and across the Indo-Pacific may stifle the post-pandemic recovery in Southeast Asia. As shown throughout the US-Singapore Tech & Innovation Virtual Dialogue, black swan events like the pandemic and the unprovoked war in Ukraine are becoming more prevalent. The rate, frequency, and complexity of such crises demand more proactive responses from policymakers. Given their dependencies on global supply chains and the data-driven economy, the US and Singapore are deeply challenged by such systemic risks.

Reframing policy conversations beyond the zero-sum game of technological competition is indeed warranted. To this end, it is our hope that the distinct, yet interlinked, areas examined in this digital publication provoke some insights that Singaporean and American policymakers may consider as they stand in a digital crossroads marked by geo-technological uncertainty and disruption. Hopefully, the policy recommendations outlined here enable coherent US-Singapore bilateral cooperation to catalyze Southeast Asia's digital transformation anchored on resilience, inclusion, and sustainability.

---

[1] Giulia Ajmone Marsan, "Upskilling and reskilling MSMEs workers and entrepreneurs," Economic Research Institute for ASEAN and East Asia, February 25, 2021.
[2] Giulia Ajmone Marsan, "Artificial Intelligence in South East Asia: Upskilling and Reskilling to Narrow Emerging Digital Divides in the Post-Pandemic Recovery," Georgetown Journal of Asian Affairs, 2021.
[3] The Association of Southeast Asian Nations, ASEAN Digital Masterplan 2025.
[4] Giulia Ajmone Marsan, "Artificial Intelligence in South East Asia: Upskilling and Reskilling to Narrow Emerging Digital Divides in the Post-Pandemic Recovery," Georgetown Journal of Asian Affairs, 2021.
[5] Ibid.
[6] SOCRadar, "Most Remarkable APT Incidents That Targeted Malaysia in 2021," April 7, 2022.
https://socradar.io/most-remarkable-apt-incidents-targeted-malaysia-in-2021/
[7] Mark Manantan, "Mind the Gap: How Southeast Asia Can Make the AI Leap," The Diplomat, October 23, 2020.
https://thediplomat.com/2020/10/mind-the-gap-how-southeast-asia-can-make-the-ai-leap/
[8] Eileen Yu, "Pandemic pushes cybersecurity to top agenda in Asean boardrooms," ZDNet, March 15, 2022.
https://www.zdnet.com/article/pandemic-pushes-cybersecurity-to-top-agenda-in-asean-boardrooms/
[9] Mark Manantan, "Mind the Gap: How Southeast Asia Can Make the AI Leap," The Diplomat, October 23, 2020.
https://thediplomat.com/2020/10/mind-the-gap-how-southeast-asia-can-make-the-ai-leap/
[10] US Department of State, "Secretary Antony J. Blinken and Singaporean Foreign Minister Vivian Balakrishnan at the Signing of the Singapore-United States Third-Country Training Program (TCTP) Memorandum of Understanding Renewal," September 27, 2021.
https://www.state.gov/secretary-antony-j-blinken-and-singaporean-foreign-minister-vivian-balakrishnan-at-the-signing-of-the-singapore-united-states-third-country-training-program-tctp-memorandum-of-understanding-renewal/

[11] Cyber Security Agency of Singapore, "Singapore and the United States Sign Declaration of Intent on Cybersecurity Technical Assistance Programme," November 16, 2018.
https://www.csa.gov.sg/news/press-releases/singapore-and-the-us-sign-doi-on-cybersecurity-technical-assistance-programme#:~:text=Singapore%20and%20the%20United%20States%20signed%20a%20Decl aration%20of%20Intent,in%20regional%20cybersecurity%20capacity%20building
[12] Cyber Security Agency of Singapore, "ASEAN-Singapore Cybersecurity Centre of Excellence," October 6, 2021.
https://www.csa.gov.sg/News/Press-Releases/asean-singapore-cybersecurity-centre-of-excellence
[13] Cyber Security Agency of Singapore, "Establishment of the United States – Singapore Cyber Dialogue," March 30, 2022
https://www.csa.gov.sg/News/Press-Releases/establishment-of-the-united-states-singapore-cyber-dialogue

Singapore's sanctions against Russia: What are the long-term implications?

Manoj Harjani

On March 5, 2022, Singapore imposed sanctions on Russia in response to its invasion of Ukraine in late February. The sanctions comprised export controls on military and certain dual-use goods that could be used in offensive cyber operations, as well as financial measures against Russian banks and government fund-raising activities, including via cryptocurrencies.[1]

This move by Singapore was significant for three reasons. First, the sanctions were imposed unilaterally, rather than in compliance with UN resolutions.[2] The only other time Singapore has imposed unilateral sanctions was in 1978, following Vietnam's invasion of Cambodia.[3] Second, Singapore's position was in marked contrast to its ASEAN neighbors, many of which have close economic and political ties with Russia. For example, Myanmar went as far as endorsing Russia's actions in Ukraine, while most of the other ASEAN countries expressed concern without naming Russia as an aggressor.[4] Finally, the sanctions explicitly acknowledged the importance of cryptocurrencies as an alternative to traditional financial flows amid growing global attention toward closing this "crypto loophole."[5]

With no end to the Ukraine conflict yet in sight, it is important to understand the long-term implications of Singapore maintaining its sanctions against Russia, given their significance outlined above. This is because policymakers will need to manage enduring issues such as divergence within ASEAN, as well as more immediate and tangible concerns in relation to regulating cryptocurrencies, and more broadly, the digital economy.

Not necessarily a surprise, but largely symbolic?

Singapore's sanctions against Russia were not necessarily a surprise, given the country's steadfast support for the principles and norms enshrined in the UN Charter, which has been a cornerstone of its foreign policy since independence. In a statement to parliament on February 28, 2022, Minister for Foreign Affairs Vivian Balakrishnan said that "Russia's invasion of Ukraine is a clear and gross violation of the international norms and a completely unacceptable precedent. This is an existential issue for us… A world order based on 'might is right,' or where 'the strong do what they can and the weak suffer what they must'… would be profoundly inimical to the security and survival of small states."[6]

Nevertheless, it could be argued that Singapore's sanctions are largely symbolic, given that Russia accounted for just 0.1 percent of total exports and 0.8 percent of total imports in 2020,[7] with local banks having limited exposure to the Russian market.[8] However, as Singapore is Asia's largest oil trading hub, Russian energy giants—Gazprom, Lukoil, and Rosneft—have a presence in the country, and therefore their business activities have been disrupted by the sanctions.[9] Furthermore, prior to the Ukraine conflict, Singapore was pursuing closer trade ties with Russia through the negotiation of a free trade agreement with the Eurasian Economic Union.[10]

Recent events will have undoubtedly cast a shadow over these areas of economic connectivity and cooperation, but even an end to Russia's invasion may not bring about an immediate restoration of the pre-conflict status quo. This is because Russia has demonstrated a willingness to respond to sanctions "tit-for-tat," which is likely to entrench the breakdown of economic ties caused by the Ukraine conflict. For instance, in April 2022, state-owned Gazprom exited its German unit which is responsible for gas supplies to Europe.[11] Russia subsequently imposed sanctions on subsidiaries of Gazprom Germania, renamed Securing Energy for Europe GmbH by the German government, located in countries that had censured the invasion of Ukraine, including one based in Singapore.[12]

Divergence within ASEAN over Ukraine

Beyond the potential loss of economic connectivity and cooperation, Singapore will also have to manage challenges arising from a regional neighborhood marked by increasingly diverse and fragmented interests. The Ukraine conflict has arguably added to a growing list of issues where ASEAN is facing difficulty in achieving consensus beyond the lowest common denominator. Indeed, ASEAN's initial joint statement[13] following Russia's invasion of Ukraine was criticized for its perceived softness in tone, which reflected the regional grouping's divisions over the issue.[14]

However, as the conflict intensified, ASEAN called for a ceasefire,[15] and most of its member states supported a strongly worded resolution tabled at the UN General Assembly in early March condemning Russia's actions and calling for a withdrawal of its forces.[16]

Singapore nevertheless remains the only ASEAN member state to have imposed sanctions on Russia, with the remaining countries largely continuing with business as usual. However, attention is now focusing on key meetings due to be held later this year—such as those associated with the East Asia Summit—where Russia will be invited to attend given its status as an ASEAN Dialogue Partner.[17] Russia's presence at these meetings could provoke a response similar to that seen at the G20 summit held in July, when Western countries staged a walkout in protest at Russia's attendance.[18]

Beyond such symbolic gestures, it is unlikely that the Ukraine conflict will cause any substantive disruptions to ongoing ASEAN business, although it will continue to bring to the surface difficult questions regarding ASEAN's future relevance and effectiveness. This is primarily due to the open challenge posed by Russia's actions in Ukraine to the principles and norms that guide ASEAN. The difficulty ahead for Singapore, therefore, has less to do with potential censure by its neighbors for sustaining sanctions than it does with fostering consensus in the current geopolitical climate in the region.

Plugging the "crypto loophole"

Compared to the challenges it faces with ASEAN, Singapore's attempt to plug the "crypto loophole" in its sanctions on Russia presents more tangible concerns to be addressed. The "loophole" here refers to the possibility of financial sanctions being circumvented through transactions carried out using cryptocurrencies, which are less tightly regulated than traditional finance and banking. To address this, Singapore included specific language prohibiting the use of cryptocurrencies to circumvent the financial measures it imposed on Russia in the official announcement of its sanctions, and the Monetary Authority of Singapore (MAS) subsequently issued a notice regarding the sanctions to all financial institutions in the city-state.[19]

However, the burden of implementing the sanctions falls squarely on financial institutions and service providers, with any breach of MAS regulations liable for a fine of up to SGD one million (USD 720,000).[20] The challenge with this regulatory approach is that it does not account for whether financial institutions have the resources and capabilities to comply. There is a similar uncertainty over MAS's own ability to enforce regulations. Furthermore, service providers often

operate across borders, and may not have clear incentives to comply with MAS regulations unless they are headquartered in Singapore or have key personnel based in the country.

Cryptocurrency advocates have also pointed out that Russia may not necessarily be able to use cryptocurrencies to evade sanctions on a large scale due to limited liquidity; any evasion would likely occur on a smaller scale, similar to that involved with money laundering.[21] This would also make it much harder to detect, raising the question of whether there is sufficient gain for governments in trying to plug the "crypto loophole." Without any publicly available information on MAS's enforcement actions regarding the sanctions, it will be difficult to gauge how effective Singapore's approach has been thus far.

The challenge ahead for Singapore to sustain these financial measures related to cryptocurrencies will be to find suitable ways to measure and account for compliance costs. The sanctions also come at a time when chaos in cryptocurrency markets has led to calls for greater regulatory oversight,[22] raising the stakes for the approach that policymakers will eventually decide on. Fortunately, Singapore has taken steps in the right direction, with the Payment Services Act 2019 providing a base for MAS to license service providers and manage their activities.

The road ahead: more unilateral sanctions?

The fact that Singapore has imposed sanctions unilaterally just once prior to the current sanctions on Russia should sound a note of caution when gauging the likelihood of more unilateral sanctions in the future. Superpowers are likely to use all available means at their disposal to gain a strategic advantage, so pressure on Singapore and other ASEAN countries to take a side by adopting future sanctions will remain a possibility. However, judging by how Southeast Asia has reacted to the conflict in Ukraine thus far, pragmatism will continue to be the order of the day, although this will exert pressure on ASEAN's unity as a regional grouping.

What we can expect in future with a greater degree of certainty—and we therefore should emphasize appropriate preparations for—is the continued expansion of sanctions and other tools of economic coercion to encompass digital economy activities, as well as control over critical and emerging technologies.

This expansion of sanctions into the digital realm follows on from recent efforts to regulate flows of data, digital payments, and e-commerce activities. Singapore is itself leading multiple efforts to sign digital economy agreements with like-minded countries,[23] and has also been a

driving force behind model contractual clauses recently developed by ASEAN for cross-border data transfers.[24] Furthermore, as countries strive to secure and gain a strategic advantage from the control of critical and emerging technologies, we can expect more announcements of export controls and investment screening by superpowers, which will impact Singapore and other countries in Southeast Asia due to their participation in global value chains and R&D. As competition intensifies over these technologies, so too will efforts to impose limits on their proliferation.

---

[1] Ministry of Foreign Affairs (Singapore), "Sanctions and Restrictions Against Russia in Response to its Invasion of Ukraine," press release, March 5, 2022
https://www.mfa.gov.sg/Newsroom/Press-Statements-Transcripts-and-Photos/2022/03/20220305-sanctions
[2] Bhavan Jaipragas, "Ukraine invasion: Singapore to impose unilateral sanctions on Russia in 'almost unprecedented' move," South China Morning Post, February 28, 2022
https://www.scmp.com/week-asia/politics/article/3168648/ukraine-invasion-singapore-impose-unilateral-sanctions-russia
[3] Sebastian Strangio, "Singapore Announces Sanctions on Russia Over Ukraine Invasion," March 1, 2022
https://thediplomat.com/2022/03/singapore-announces-sanctions-on-russia-over-ukraine-invasion/
[4] Ian Storey and William Choong, "Russia's Invasion of Ukraine: Southeast Asian Responses and Why the Conflict Matters to the Region," ISEAS Perspective no. 24 (March 9, 2022)
https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2022-24-russias-invasion-of-ukraine-southeast-asian-responses-and-why-the-conflict-matters-to-the-region-by-ian-storey-and-william-choong/
[5] Keita Sekiguchi, "US, Japan and EU rush to close crypto loophole in Russia sanctions," Nikkei Asia, March 4. 2022,
https://asia.nikkei.com/Politics/Ukraine-war/U.S.-Japan-and-EU-rush-to-close-crypto-loophole-in-Russia-sanctions
[6] Ministry of Foreign Affairs (Singapore), "Minister for Foreign Affairs Dr Vivian Balakrishnan's Ministerial Statement on the Situation in Ukraine and its Implications," press release, February 28, 2022
https://www.mfa.gov.sg/Newsroom/Press-Statements-Transcripts-and-Photos/2022/02/20220228-Ministerial-Statement
[7] Nabilah Awang, "Explainer: Will Singapore's sanctions against Russia have any impact?" Today, March 2, 2022
https://www.todayonline.com/singapore/explainer-will-singapores-sanctions-against-russia-have-any-impact-1833386
[8] Hwee Min Ang, "Singapore banks have limited exposure to Russia; MAS sends reminder to manage risks amid Ukraine crisis," CNA, March 1, 2022
https://www.channelnewsasia.com/singapore/singapore-banks-limited-exposure-russia-dbs-uob-ocbc-mas-2528091
[9] Uma Devi, "How big are Russia's oil majors in Singapore?" The Business Times, March 4, 2022
https://www.businesstimes.com.sg/companies-markets/how-big-are-russias-oil-majors-in-singapore
Noreen Jazul and Vann Villegas, "Russian oil vessels facing 'difficulties' bunkering in Singapore," Singapore Business Review, March 4, 2022
https://sbr.com.sg/exclusive/exclusive-russian-oil-vessels-facing-difficulties-bunkering-in-singapore
[10] "Eurasian Economic Union-Singapore FTA will make 'positive contribution' to economic relations: Russia, Singapore," CNA, December 17, 2021
https://www.channelnewsasia.com/singapore/eaeu-singapore-fta-positive-contribution-economic-relations-russia-singapore-2387171.

[11] "Gazprom Exits German Unit Without Disclosing New Ownership," Bloomberg, April 1, 2022, https://www.bloomberg.com/news/articles/2022-04-01/russia-s-gazprom-exits-german-unit-new-owner-isn-t-disclosed.
[12] "Russia puts sanctions on Gazprom units in Europe and U.S., part owner of pipeline," Reuters, May 12, 2022, https://www.reuters.com/business/russia-sanctions-gazprom-germania-units-owner-polish-part-yamal-europe-pipeline-2022-05-11/.
[13] Association of Southeast Asian Nations, "ASEAN Foreign Ministers' Statement on the Situation in Ukraine," press release, February 26, 2022 https://asean.org/wp-content/uploads/2022/02/ASEAN-FM-Statement-on-Ukraine-Crisis-26-Feb-Final.pdf
[14] Thi Ha Hoang, "Ukraine invasion: Asean should have called out Russia's attack but it chose to stay mute," South China Morning Post, March 1, 2022 https://www.scmp.com/week-asia/opinion/article/3168789/ukraine-invasion-asean-should-have-called-out-russias-attack-it.
[15] Association of Southeast Asian Nations, "ASEAN Foreign Ministers' Statement Calling for a Ceasefire in Ukraine," March 3, 2022, https://asean.org/wp-content/uploads/2022/03/ASEAN-Foreign-Ministers-Statement-calling-for-Ceasefire-in-Ukraine-EN.pdf.
[16] United Nations General Assembly, Aggression against Ukraine, A/RES/ES-11/1 (March 2, 2022), https://digitallibrary.un.org/record/3965290.
[17] "Cambodia invites Russian foreign minister to ASEAN meetings," Nikkei Asia, July 7, 2022, https://asia.nikkei.com/Politics/International-relations/Cambodia-invites-Russian-foreign-minister-to-ASEAN-meetings.
[18] Stefan Wolff, "Ukraine war: Russia's G20 walkout heightens tensions at fractious summit as China's rise continues," The Conversation, July 12, 2022 https://theconversation.com/ukraine-war-russias-g20-walkout-heightens-tensions-at-fractious-summit-as-chinas-rise-continues-186650.
[19] Monetary Authority of Singapore, Financial Measures in Relation to Russia, MAS Notice SNR-N01 (March 14, 2022), https://www.mas.gov.sg/-/media/MAS-Media-Library/regulation/anti-money-laundering/targeted-financial-sanctions/MAS-Notice-SNRN01-14-Mar-2022final.pdf.
[20] Monetary Authority of Singapore, "Targeted Financial Sanctions," n.d., https://www.mas.gov.sg/regulation/anti-money-laundering/targeted-financial-sanctions.
[21] "Cryptocurrency Markets Aren't Liquid Enough for Mass Russian Sanctions Evasion," Chainalysis, April 13, 2022, https://blog.chainalysis.com/reports/cryptocurrency-liquidity-russia-sanctions/.
[22] Monetary Authority of Singapore, "Reply to Parliamentary Question on restrictions on cryptocurrency trading platforms to protect members of public," press release, July 4, 2022, https://www.mas.gov.sg/news/parliamentary-replies/2022/reply-to-parliamentary-question-on-restrictions-on-cryptocurrency-trading-platforms-to-protect-members-of-public.
[23] Ministry of Trade and Industry (Singapore), "Digital Economy Agreements," n.d., https://www.mti.gov.sg/Trade/Digital-Economy-Agreements.
[24] ASEAN Model Contractual Clauses for Cross Border Data Flows (Association of Southeast Asian Nations, 2021), https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf.

Defending Supply Chain Cybersecurity: Opportunities for Singapore–United States Cooperation

Andreas Kuehn, PhD

The cybersecurity threat and risk landscapes have significantly changed in recent years, with a growing number of cyber incidents targeting or affecting supply chains in information and communications technology (ICT) as well as other industry sectors.[1] Today's digital transformation and innovative use of ICT and data have expanded the attack vector and created new interdependencies that have become attractive targets for malicious criminal and state actors. This development is a particular concern for advanced digital economies that increasingly rely on secure and trusted digital infrastructure for their industries and their nation's economic prosperity. Supply chain breakdowns and disruptions through cyber or other means can have significant regional and global effects.

Singapore's Smart Nation strategy, for example, relies on secure connected products, as well as the assurance that the supply chain of those devices and their components meets certain security requirements and that their suppliers and service providers can be trusted.[2] The same applies to US efforts to make cities smarter, rollout 5G communications networks, secure future defense capabilities, and future-proof advanced manufacturing through Industry 4.0 technologies.[3]

Technical and Geopolitical Aspects of Supply Chain Cybersecurity

There are two prevailing, yet intertwined ways to think about supply chain cybersecurity—on both a technical and a geopolitical level. Supply chain security from a technical perspective focuses on the risk and the use of third-party products and services and the subsequent need to apply technical and organizational measures to mitigate such risks. A shift in perspective

toward geopolitical considerations of supply chains has occurred in recent years, highlighted by the growing political tensions between China and the United States as major state powers and ICT providers. This reflects the recognition that ICT, and especially critical and emerging digital technology, including 5G, artificial intelligence, semiconductors, and the Internet of Things (IoT), are of critical, strategic value for the economy, national security, and defense.[4]

Governments and industries recognize that dependence on foreign ICT suppliers, and the potential for adversaries to exploit such reliance, exposes them to greater and continual risks. This reality has been compounded by the COVID-19 pandemic and Russia's invasion of Ukraine, which have highlighted the importance of resilience in global production and distribution networks to ensure a functioning economy.

The United States and Singapore have undertaken various efforts to strengthen supply chain cybersecurity and manage third-party ICT risk. Without attempting to be comprehensive, key efforts by the United States include the inclusion of supply chain security in the updated National Institute of Standards and Technology (NIST) Cybersecurity Framework in 2018 and a recent 2022 update of the NIST Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations to enhance software supply chain security.[5] The White House issued a series of executive orders to secure supply chains, including cybersecurity, over the past several years, and directed several US Departments to conduct a seminal supply chain review concerning emerging and critical and emerging technologies. The Departments of Homeland Security, Defense, Commerce, and State, as well as the Cybersecurity and Infrastructure Security Agency, have led a number of efforts to secure civilian and defense ICT supply chains, including work related to 5G deployments domestically and abroad and certification of defense industrial base suppliers under the Cybersecurity Maturity Model Certification (CMMC) framework.[6] Furthermore, Congress has undertaken numerous efforts to strengthen supply chain resilience and security, including cybersecurity. The National Security Commission on AI and the Cyberspace Solarium Commission have also dedicated some of their work to supply chains and US dependence on foreign suppliers, which led to calls to relocate production domestically, build technology alliances among like-minded states, and decouple technological and economic systems from adversarial competitors.

Singapore has engaged in similar efforts, albeit on a smaller scale, to protect supply chains and the nation's role as a regional innovation hub. Its updated Cybersecurity Strategy 2021 references supply chain risks, which are managed through the Critical Information Infrastructure (CII) Supply Chain program. This aims to enhance the visibility and management of cyber supply chain risks and establish structures for relevant stakeholders to mitigate those risks.[7]

To this point, the United States and Singapore have initiated cybersecurity cooperation in the form of three memorandums of understanding and agreed to establish the United States-Singapore Cyber Dialogue in March 2022.[8]

The Challenges and Pitfalls of Securing Global Supply Chains

Securing global supply chains has become increasingly challenging. This applies particularly to supply chains of ICT products and services, but also holds true for other industry sectors, especially as globalization and the digital transformation have fundamentally transformed how goods and services are developed, manufactured, and delivered, while the management of supply chains relies heavily on ICT and data. Recent calls to strengthen the resilience of supply chains may result in shifting supply networks toward like-minded regional and local partners and alliances, but the net effects of these changes on security remain uncertain. The following four factors describe why securing supply chains will persist in being a significant challenge in the years to come:

First, supply chains are complex and difficult to secure, due to their distributed and global nature. Apple, for instance, has more than 200 suppliers in 43 countries on six continents, each with its own supply chains and multiple subcontractors. Monitoring and securing supply chains is a complex and expensive management task. Supply chains are only as strong and secure as their weakest link.

Second, cybersecurity is hard and remains a foundational problem. Even ICT developed by trusted entities contains unintentional, exploitable security flaws. Frequent software updates only exacerbate the ICT security challenge.

Third, ICT is a strategic asset for economic prosperity and military power, thus putting technology at the core of geopolitical tensions and making ICT an attractive target for exploitation.

Fourth, accountability for bad behavior is limited as malicious criminal and state actors are difficult to deter or hold accountable.[9]

In response to these challenges, some governments have enacted or are considering restrictive measures to manage the growing cybersecurity risks to supply chains and digital technology. These include technical, organizational, and political measures that help strengthen national and economic security. In some instances, however, measures are solely politically motivated,

such as when government policies or actions favor ICT products and services from domestic producers (or companies incorporated in friendly states) over those produced and distributed by companies headquartered in states seen as adversarial competitors. Such an approach can undermine competitiveness, innovation, and cybersecurity rather than improve supply chain security or help generate market value. Restrictive government measures that fall under the rubric of technology nationalism may also include subjecting foreign companies to enhanced security requirements, such as mandatory source code inspection; requiring foreign companies to partner with domestic entities to gain market access; banning products or services from foreign vendors; and requiring companies to localize data domestically. While such measures may be justified on national security grounds, there are commercial and economic trade-offs that have to be considered.

Working Towards Trust: The What, the Who, the When, the Where, and the How of Supply Chain Security

Supply chain cybersecurity should be risk-informed, objective, and quantifiable with the goal of ensuring ICT security and trustworthiness through a combination of measures that foster assurance, transparency, and accountability.

The What, the Who, the When, the Where, and the How are fundamental pillars of supply chain security. Concerning the question of *What* should be done, a single measure alone does not create sufficient security or trustworthiness, but in combination a set of measures can raise confidence and reduce residual risk to an acceptable level. Trust must be earned and achieved on the basis of continuous, ongoing verification through such measures. The key to building trust is that stakeholders have to agree to abide by shared rules and requirements for secure ICT and establish mechanisms to effectively discourage violators.

Concerning the question of *Who* is responsible, supply chain security is a team sport—a shared responsibility among vendors, operators, and buyers. A secure connected device built by a manufacturer, but deployed by a customer with a faulty configuration, exposes the security, safety, and privacy of its users. Who owns and operates the ICT changes the answer to the question of who is best positioned to take action. Finally, governments have a role to play through coordination, regulations, and other means, particularly in circumstances in which industries are ill-equipped to do so, such as in the presence of information asymmetries and externalities that cybersecurity markets have failed to resolve. To that end, smart regulatory actions may include baseline security requirements. Joint efforts and coordination across all stakeholders, the

private sector, government, and civil society to ensure security and resilience across the value chain and throughout the ICT life cycle are needed now and into the future, which answers the question of *When*.

The response to *Where* to take action to improve digital and supply chain security lies at three levels:

First, at the *organizational level*, ICT buyers would be well served to determine their risk-informed procurement requirements. This includes requiring vendors to follow international standards for secure software and ICT development, to ensure that services and software are delivered by default with a secure configuration, and to use best practices for security vulnerability reporting and disclosure.

Second, at the *industry level*, ICT buyers and vendors should determine requirements for their respective industries. By leveraging their collective purchasing power, ICT buyers are in a position to influence requirements for their respective industries and can establish best practices that require ICT vendors to provide statements of supply chain risk management. They can also strive to establish ICT security assessment consortia for their industry sectors. In parallel, ICT vendors should push for vendor-led assurance and transparency requirements, including participating in international standards and norms setting to improve ICT and supply chain security, committing to coordinated vulnerability disclosure as an industry, adopting technology-specific evaluation and accreditation schemes, and establishing industry-wide oversight boards.

Third, at the broader *ecosystem level*, relevant stakeholders can play a role by establishing regional transparency centers that allow for code review and testing, building global conformance programs, such as the European Union's certification framework and cybersecurity schemes, and adopting United Nations cyber norms and other normative efforts relevant to protect ICT supply chains.

Demonstrating that an organization takes sufficient actions based on measures and controls is a matter of reporting and speaks to the question of *How*. This may include dedicated reporting, controlling, and auditing of supply chain security and trustworthiness at all levels, from subcontractors and suppliers to ICT integrators, and ICT manufacturers and vendors to governments and regulators. There is a growing debate about reporting and verifiable controls for supply chain cybersecurity to calculate risk and vendors' trustworthiness. As such, both self and third-party certification are likely to become integral parts of future reporting practices to demonstrate an organization's cybersecurity posture.

Opportunities for Singapore–United States Cooperation to Advance Supply Chain Cybersecurity

There are a number of areas in which joint efforts could leverage the measures and agreements adopted by Singapore and the United States to enhance supply chain cybersecurity. As a recognized leader in digital transformation and cybersecurity within ASEAN and the wider region, Singapore is well positioned to spearhead technical and policy innovations to advance supply chain cybersecurity that directly benefits the resilience of supply chains. Four areas seem particularly relevant and deserve attention in the near term:

First, building on existing cooperation, Singapore and the United States are ideally placed to strengthen cybersecurity information sharing, especially threat and vulnerability information pertinent to the security and integrity of supply chains, and to foster operational cybersecurity cooperation to respond to cyber incidents that undermine supply chain security and resilience.[10] Information sharing increases visibility and situational awareness, which provides a basis for taking protective actions.

Second, a large number of standards, best practices, and frameworks that address digital and supply chain cybersecurity has emerged—both in general, as well as pertaining to specific industry verticals.[11] This is a welcome result of a long process that sought to define supply chain cybersecurity, and signals that governments and industries have taken steps in the right direction over the last five years. To date, fragmented efforts reinforce the concept that countries and industries should work in greater concert to bring about organizational and institutional changes to implement standards, best practices, and frameworks. In this context, rather than expanding the existing repertoire, Singapore and the United States should together take the lead on demonstrating the value of focusing on the implementation of standards and frameworks; leading pilot programs together with selected partners in key industries to test adoption and effectiveness; and share the findings with the wider ICT ecosystem. Special attention should be paid to the incorporation of supply chain cybersecurity requirements in government contracting and the needs of small and medium-sized contractors and vendors who face difficulties in adopting adequate cybersecurity measures. Dedicated, government supported programs should also support capacity-building and professional development for supply chain cybersecurity in digitally less developed nations in Southeast Asia and beyond. Simple, yet effective, easy-to-implement solutions are the first step toward the overall objective.

Third, Singapore and the United States should consider joint engagements with manufacturers and service providers in Southeast Asia, particularly those that focus on industrial and consumer IoT, to lead the conversation about supply chain cybersecurity accountability. Addressing digital and supply chain security at the source of the world's manufacturing hub, before digital products, components, and services are delivered across the region and the globe, could have significant positive effects on cybersecurity overall. Such an effort could be coordinated with private ICT certification providers that are working closely with local manufacturers and regional retailers. Singapore may even consider leveraging its own certification and labeling capabilities, such as its Cybersecurity Certification Centre and its Cybersecurity Labelling Scheme, to that end.

Fourth, joint efforts to enhance supply chain cybersecurity should inform and be aligned with other initiatives underway, such as the Quadrilateral Security Dialogue and its relevant working groups on critical and emerging technologies, and the Indo-Pacific Economic Framework for Prosperity. Relatedly, the United States and Singapore would benefit by continuing to support the implementation of United Nations norms of responsible state behavior in cyberspace, specifically regarding supply chain security, and by coordinating the development of relevant international standards in technical bodies.

Amid US efforts to manage technology competition through alliances with partners that emphasize shared values, cooperation with Singapore could be a stepping stone, albeit a difficult one, to expand the aforementioned alliances on the basis of similar forms of cooperation, to strengthen supply chain resilience, and even to seek convergence on cybersecurity and other digital and technology policy issues in the region.

---

[1] Leon Spencer, "Singapore's cyber agency flags threat surge," Channel Asia, July 9, 2021. https://www.channelasia.tech/article/689683/singapore-cyber-agency-flags-threat-surge/; CISA, Defending Against Software Supply Chain Attacks, 2021, https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf; and ENISA, Understanding the increase in Supply Chain Security Attacks. July 29, 2021 https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks

[2] Smart Nation Singapore, https://www.smartnation.gov.sg/

[3] E.g., National advanced manufacturing portal, https://www.manufacturing.gov/

[4] Critical and Emerging Technologies List Update, White House, February 2022, https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf

[5] NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 2018, https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf; and NIST, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, SP 800-161r1, May 2022 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf

[6] E.g., ICT Supply Chain Assessment Fact Sheet, US Department of Commerce, February 24, 2022, https://www.commerce.gov/news/fact-sheets/2022/02/ict-supply-chain-assessment-fact-sheet

[7] CSA, Keeping Our Digital Spaces Safe, 2021, https://www.csa.gov.sg/-/media/csa/documents/cos/2021/csa-cos-2021-factsheet---keeping-our-digital-spaces-safe.pdf

[8] CSA, Establishment of the United States-Singapore Cyber Dialogue, March 30, 2022 https://www.csa.gov.sg/News/Press-Releases/establishment-of-the-united-states-singapore-cyber-dialogue

[9] Andreas Kuehn, Bruce McConnell, "Weathering TechNationalism: A Security and Trustworthiness Framework to Manage Cyber Supply Chain Risk," Policy Report, EastWest Institute, New York, NY, 2020, https://www.eastwest.ngo/technationalism

[10] CISA, United States and Singapore Expand Cooperation on Cybersecurity, August 23, 2021 https://www.cisa.gov/news/2021/08/23/united-states-and-singapore-expand-cooperation-cybersecurity

[11] Paris Call for Trust and Security in Cyberspace, Working Group 6. Report: Securing ICT supply chains. November 2021, https://pariscall.international/assets/files/2021-11-12-Paris-Call-Working-Group6-Report-SecuringICTSupplyChain.pdf

Digitalization and Sustainable Energy in ASEAN

Courtney Weatherby

Southeast Asia's energy demand is expected to rise rapidly in the coming decades: a survey of national plans by the International Energy Agency (IEA) anticipates a cumulative energy demand growth of 60 percent for the region through 2040.[1] Electricity demand growth alone rises about four percent annually, which is nearly double that of the rest of the world.[2] Some Southeast Asian countries like Cambodia and Vietnam experience double digit electricity demand growth from one year to the next. This rapid growth requires a massive expansion of power generation infrastructure, even as pressures on the energy market from climate change considerations and global supply chain resilience require a transition of both energy supply and energy system management. Digitalization of the energy sector will be key to support the clean energy transition, and there are opportunities for the United States and Singapore to expand collaboration on technical capacity-building in this space.

Expanding Renewable Energy

Globally, investment in renewable energy surpassed investment in fossil fuels by the early 2010s. Starting in 2015 the amount of new power generation brought online each year from solar and wind began to outpace fossil fuel power generation.[3] However, most annual investment in ASEAN in the short-to-medium term is still targeted toward fossil fuels. Despite a shared target to ensure 23 percent of the region's power sector investments are renewable by 2025, ASEAN is not on track for renewables to outpace fossil fuels until 2034.[4] At the same time, countries around the region are responding to global pressures to move toward net zero carbon emissions and manage climate risk. In 2020 Laos and Singapore pledged to move toward net zero, and in 2021 Malaysia, Thailand, and Vietnam followed suit.[5] The other five ASEAN members have varying targets and commitments to reduce emissions.

Meeting these targets while expanding electricity supply will require a major transition in the region's energy mix, changes to energy system management to effectively integrate variable solar and wind, and greater demand for management to endorse energy efficiency. The initial challenge in the renewable energy transition has been to adjust regulations, national plans, and policies to support alternative energy projects. With the exception of Thailand, most countries in Southeast Asia had negligible solar and wind capacity installed until 2017. However, as countries like Cambodia and Vietnam have begun to integrate higher amounts of variable renewable energy, they have also begun to run into challenges of grid integration. Digitalization of the energy sector will be a key factor in Southeast Asia's ability to make this transition successfully.

Renewable energy technologies like solar and wind operate very differently from traditional power plants—they produce electricity intermittently based on when the sun is shining or the wind is blowing, and that leads to greater demands on the utility companies as they work to ensure grid stability. The decentralization of the energy supply through the deployment of rooftop solar panels also leads to exceptional growth in the number of grid connections. For instance, Vietnam has 378 operational commercial-scale power plants, but as of mid-2022 there were more than 100,000 individual solar rooftop units connected to the grid.[6]

Digitalization and Renewable Energy Integration

Effective use of variable renewable energy requires more data, more immediate data processing, and more rapid operational shifts than working with traditional fuel-based plants, which can be ramped up or down depending on need. Digital data collection, data analysis, forecasting, and improved connectivity and information sharing can all enhance efficient operation of electricity systems. This requires investments in physical infrastructure such as smart meters to track second-to-second changes in electricity production and demand. Better data can better predict when electricity demand may peak, allowing for better load forecasting on the part of utilities. Improved weather forecasting can predict when a cloud will move in front of the sun or the wind will stop blowing and disrupt energy production. If utilities can plan for such disruptions, they will be able to improve overall use of solar or wind power when it's available and prepare utilities to adjust effectively when it is not.

While many countries have identified pathways to adopt digital solutions on the supply side, improving efficiency and management on the demand side is the next key area of opportunity for digitalization. Detailed and remote data collection at the individual household or business level through the use of smart meters can help provide personalized recommendations on

how to save energy. Malaysia has been doing this through one of its utilities, with great success.[7] Digitalizing and automating management of building features such as lighting or air conditioning can reduce overall electricity demand. The latter consideration is particularly important for Southeast Asia, as IEA projections indicate that air conditioning could make up 30 percent of peak electricity demand by 2040.[8]

And finally, the use of blockchain technology can play a role in renewable energy certification (REC), which is increasingly important in ASEAN given its place in the global manufacturing supply chain. Multinational corporations are increasingly under pressure from both consumers and shareholders to ensure that their operations are sustainable. Many companies have established their own renewable energy and net zero targets, and these are often more ambitious in terms of timeline than those of ASEAN countries. Cambodia is a particularly good example of this: Cambodia's government has plans to expand coal production in the coming years, but global manufacturing brands have expressed concern about what that means for their ability to maintain operations in the country.[9]

Blockchain can be a key technology to support REC programs, allowing companies to buy power through the grid with guarantees that they are truly supporting renewable energy production. RECs can ensure that when an end user—say, a financing institute in Singapore which has a commitment to use 100 percent renewable energy—purchases electricity from national utilities, they can have confidence that they are truly supporting renewable energy use instead of a coal plant.

Some ASEAN countries are already developing REC standards domestically: the Electricity Generating Authority of Thailand (EGAT) is certified by the International REC Standard Foundation to issue renewable energy certificates. In October 2021, Singapore's Energy Market Authority instituted a standard process for renewable energy certificates domestically.[10] And in 2018, the Bangkok Metropolitan Electricity Authority in Thailand began a pilot project using blockchain to support direct peer-to-peer renewable energy trade.[11] This was followed by a larger feasibility study by EGAT in 2020 to explore whether this could be scaled up.

The use of blockchain and renewable energy certification processes could be exceptionally useful as ASEAN moves toward a more integrated power grid, through which countries like Singapore aim to purchase renewable energy from countries like Laos and Malaysia in order to meet national carbon emissions reductions pledges. Regional electricity trade is already underway: in 2022-2023, Singapore has committed to purchasing 100 MW of hydropower

from Laos via Thailand and Malaysia as a power integration trial. Singapore currently plans to expand electricity imports by up to 4,000 MW by 2035 as it moves to reduce dependence on natural gas.[12] As electricity trade picks up, it is important to standardize not only the regulations for electricity trade but the definitions of what counts as renewable and approaches for renewable energy certification.

All of these improvements to the energy system are enabled by greater adoption of digital technologies, as well as capacity-building and training for new operational procedures. There are direct opportunities for the United States and Singapore as leaders in innovation and digitalization to jointly support technical training programs that would help less developed countries like Laos better prepare to apply digital technologies to integrate renewable energy and improve efficiency.

Of all the priority topics discussed in the recent ASEAN–US Special Summit Joint Vision Statement, energy was mentioned most often after health, more often even than security, peace, and even the economy.[13] Recently announced US initiatives in this space include the USAID Southeast Asia's Smart Power Program to catalyze blended finance to meet clean energy needs and support regional energy trade; the US–ASEAN Climate Solutions Hub, which will provide technical assistance for ASEAN countries in meeting their nationally determined contributions; as well as additional efforts by the US Trade and Development Agency and the Department of Commerce to support clean energy.[14]

Opportunities for Collaboration

As these initiatives develop, there are real opportunities for the United States to partner with Singapore in providing support on clean energy. The United States and Singapore already partner on the Third Country Training Program (TCTP), which has long provided regionally based capacity-building and technical training to neighboring countries on issues like cybersecurity, health, smart cities, and intellectual property rights. In August 2021, the US and Singapore announced an effort to green the TCTP efforts through the inclusion of courses on climate change and environmental sustainability.[15] Future programs through the TCTP should emphasize training on clean energy, which would take advantage of expertise and innovation in both the United States and Singapore to support improved system management and lay the groundwork for more sustainable power trade.

Prioritizing digital solutions to integrate renewable energy and supporting regional dialogue and training on REC would not only address immediate needs in ASEAN and help fulfill US commitments to the region's clean energy transition, but could also support Singapore's need to ensure future electricity purchases from ASEAN neighbors provide sustainable renewable energy.

[1] International Energy Agency (IEA), Southeast Asia Energy Outlook 2019, October 2019, page 10.
[2] Ibid, page 15.
[3] IRENA, World Energy Transitions Outlook: 1.5' C Pathway, 2021, IRENA, Abu Dhabi, page 42.
[4] Wood Mackenzie, "Coal is still king in Southeast Asia's power market," September 25, 2019, at https://www.woodmac.com/press-releases/coal-is-still-king-in-southeast-asias-power-market/.
[5] Clea Schumer, "How National Net-Zero Targets Stack Up After the COP26 Climate Summit," World Resources Institute, November 18, 2021, at https://www.wri.org/insights/how-countries-net-zero-targets-stack-up-cop26.
[6] EVN Solar, "Do You Know," updated March 6, 2022, at https://solar.evn.com.vn/#/.
[7] USAID, ASEAN Center for Energy, and US-ASEAN Business Council, Digital Technology for ASEAN Energy: How Digitalization Can Address ASEAN's Power Sector Challenges, November 2019, page 32.
[8] International Energy Agency, The Future of Cooling in Southeast Asia, November 2019, page 10. Accessible at https://www.iea.org/reports/the-future-of-cooling-in-southeast-asia.
[9] Shaun Turton, "Cambodia's shift to coal power riles global brands," Nikkei Asia, August 11, 2020, accessed May 17, 2022, at https://asia.nikkei.com/Business/Energy/Cambodia-s-shift-to-coal-power-riles-global-brands.
[10] Singapore Energy Market Authority, "New Singapore Standard launch to support management and use of Renewable Energy Certificates," October 26, 2021, at https://www.ema.gov.sg/media_release.aspx?news_sid=20211026xnJX3nGtlY4p.
[11] Rina Chandran, "In a posh Bangkok neighborhood, residents trade electricity with blockchain," Reuters, August 28, 2018, at https://www.reuters.com/article/us-thailand-renewables-tech/in-a-posh-bangkok-neighborhood-residents-trade-energy-with-blockchain-idUSKCN1LD0Z8.
[12] Jessica Jaganathan and Chen Lin, "Singapore plans electricity imports to boost security, diversify supply," Reuters, October 25, 2021, at https://www.reuters.com/business/energy/singapore-plans-electricity-imports-up-4-gw-by-2035-2021-10-25/.
[13] The White House, "ASEAN–US Special Summit 2022, Joint Vision Statement," May 13, 2022, at https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/13/asean-u-s-special-summit-2022-joint-vision-statement/.
[14] The White House, "Fact Sheet: US–ASEAN Special Summit in Washington, DC," May 12, 2022, at https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/12/fact-sheet-u-s-asean-special-summit-in-washington-dc/
[15] The White House, "Fact Sheet: Strengthening the US–Singapore Strategic Partnership," August 23, 2021, at https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/23/fact-sheet-strengthening-the-u-s-singapore-strategic-partnership/

Sustainable Considerations for Inclusive Digital Futures

Natalie Pang, PhD

The COVID-19 pandemic over the last two years has intensified the adoption and development of digital technologies. Digital literacy and having access to digital devices has become essential to daily functioning, and have quickened the pace of development of smart cities. According to the Smart City Index 2021 conducted by the International Institute for Management Development and Singapore University for Technology and Design (SUTD), cities like Singapore, Zurich, Auckland, Seoul, and New York have topped other cities in terms of technological provision across five areas: health and safety, mobility, activities, opportunities, and governance.[1]

Singapore launched its Smart Nation initiative in 2014, and has steadily introduced smart technologies in a range of public services. For instance, smart technologies are deployed in planning and managing residential areas to conserve energy, manage waste, and improve public health. The city of New York launched its smart city pilot in 2020, and introduced smart technologies in various districts. Other than using smart technology for services such as waste management and car sharing to reduce carbon emissions, the New York City Blockchain Center also brings together different stakeholders to work on blockchain innovations.

The future of smart cities seems bright, with all its promises and potential to tackle important issues such as congestion, waste, rising temperatures, and public health. But alongside the excitement, concerns about digital vulnerabilities have also emerged.

Gaps in inclusive digital futures

What the pandemic has also reminded us of is the importance of addressing unequal access to devices, broadband networks, and digital literacy. Without the availability of an adequate digital device or a stable internet connection, individuals have reported difficulties in accessing education, work opportunities, and essential public services.[2] When left unchecked, such unequal access can widen class divides in society and ultimately undermine democracy and social mobility.

To deal with unequal access to broadband connectivity, Singapore launched Wireless@SG in 2006 with the aim of making broadband access freely available in densely populated areas such as community centers and tourist attractions. The service has limited reach for low-income households living in rental housing, as these areas often lack the infrastructure necessary for the installation of fibre-optic cables. In response to such gaps, policies such as the Home Access scheme aim to make broadband affordable or free for households with schoolchildren or persons with disabilities. Similarly, the Affordable Connectivity Program in the US under the Bipartisan Infrastructure Law provides important support for low-income households. Having deliberated and responded to issues associated with the digital divide, Singapore and the United States could combine their efforts and experience to provide leadership in the area of digital inclusion.

Yet despite the policy responses, individuals and households continue to face challenges due to gaps in digital literacy. Addressing this may be the most demanding task of all. Benchmarking or developing minimal digital literacy has grown much more complex compared to two decades ago, as digital and smart technologies have grown more advanced. Digital literacy will need to go beyond acquiring knowledge about how to use devices, navigate mobile apps, or search the web—citizens will also need to understand how to manage privacy settings, and gain computational and algorithmic knowledge so that they can be critically aware of the use of algorithms in different online applications. They may also need to understand the data policies of different platforms, or the data infrastructures involved, so that they can actively curate and manage their digital identities.

And while it used to be clear to citizens that they may be lacking certain digital skills as they use online applications and services, it may not be so when algorithms are used to make certain assumptions and decisions for people, or when they are unclear about how their personal data is collected, managed, and analyzed. People will need to be engaged as digital citizens who take active ownership of and a role in shaping key aspects of their digital futures, such as policies associated with personal data and how they flow between sovereign borders.

The other barrier has to do with digital economics. Many tech platforms operate globally with operations in different markets, yet often find themselves having to deal with local constraints, values, and legislation. This imposes certain complexities, including the possibility of dealing with issues such as data privacy, content moderation, and the protection of vulnerable persons differently in different markets. No framework exists at the moment to guide platforms in how to address potential conflicts between the markets they are operating in. The gap also presents

a potential opportunity for Singapore and the United States to explore working together in developing frameworks to address digital inclusion at a transnational level, and to develop standards or best practices through a multi-sectoral collaboration.

Digital futures are also material

Technological innovations, especially those implemented in smart cities, have often been lauded for their role in resolving environmental issues such as waste management and traffic congestion, and in helping to reduce emissions. These are significant, but it is important to pay attention to the ways they can also impact the environment.

One of the most prominent examples where digital technology and climate change can collide is in the growth and demand for data centers in recent years. Fuelled by global increases in the number of internet users, the rise of mobile networks and 5G connections, and the greater digitalisation of services, the volume of data generated by governments, organizations, and individuals has increased exponentially.

The United States has the highest number of data centers in the world,[3] and Singapore is also a sought after location to develop data centers because of its "robust infrastructure, high-speed connectivity and widespread adoption of digital technologies."[4] Data centers are physical facilities that require significant resources such as land and electricity to run, and highly specialized labor to set up and maintain, as well as generating outputs such as waste and emissions. In Singapore, data centers are estimated to account for around seven percent of the total energy consumption.[5]

Another material aspect of digital technologies is in the generation of waste. Mass adoption of technologies and improvements in digital literacy also imply larger volumes of e-waste generated by individuals and organizations, including data centers. In Singapore's case, this amounts to about 60,000 tonnes of e-waste every year. To respond to the problem, the Singapore Green Plan 2030 launched in February 2021 focuses on green citizenry and scaling up e-waste recycling efforts with the target to reduce the amount per capita of waste going to landfill by 20 percent.[6]

However, the issue of e-waste must also be understood globally. Developing countries often receive e-waste from developed countries and the intensity poses significant environmental and health risks to local communities.[7] A study by Toxics Link found that soil and water from regions that receive and process e-waste from developed countries contained significantly higher levels of metals, including lead and mercury.[8] Such movements of hazardous waste have been regulated

under the Basel Convention on the Control of Transboundary Movements of Hazardous Waste and their Disposal, in force since 1992.[9] However, the main challenge lies in implementing and enforcing the convention.

Another type of waste is heat. Computers and servers in data centers run using electricity, generating much heat which needs to be dissipated as such equipment requires optimal temperatures to function and thrive. In addition to generating heat waste, data centers also consume a lot of energy. The problem is exacerbated in tropical Singapore as even more energy is required. Singapore's approach is to seek balance and moderation: while acknowledging the benefits and importance of data centers, policymakers in Singapore introduced a moratorium on new data centers in 2019 in recognition of land use and sustainability issues.

The moratorium is complemented by efforts to explore innovations to reduce energy consumption and cooling solutions. For instance, the Sustainable Tropical Data Centre Testbed (STDCT) program launched in June 2021 is a joint effort by the National University of Singapore and Nanyang Technological University to pioneer sustainable and innovative cooling solutions for data centers in the tropics.[10] Such research and development are significant and impactful, especially in resolving the problems associated with data centers in the tropics, but it takes time to explore the feasibility and impacts of the proposed solutions. The challenge is in coming up with interim solutions to address how data centers can consume less energy while dealing with increasing volumes of data.

Next steps for US–Singapore collaboration

As Singapore and the United States continue their collaboration in the areas of cybersecurity, big data, and artificial intelligence, it is crucial to consider what inclusive digital futures could look like for both countries. While the populace and socio-cultural contexts in both countries are quite different, there are many similarities in terms of the factors driving gaps in universal access to devices, network connectivity, and digital literacy.

The emphasis on addressing digital inclusion through education, identifying vulnerabilities in data literacy, and improving access policies remains important. But for a more comprehensive and holistic approach to the topic of inclusive digital futures, it is also critical to consider the issue of sustainability identified in this essay: a) the development and maintenance of data centers, especially in land-scarce Singapore; b) e-waste and equity issues, especially in the Global South where many developing countries receive e-waste from developed countries; and c) heat waste and the high consumption of energy by data centers in tropical climates like Singapore.

There are many insights and lessons that Singapore can offer, especially in terms of dealing with all the issues identified, and Singapore and the United States could work together to promote the advancement of digital futures that are also sustainable. Such collaborations can be impactful, especially for Asia, and promote greater equity globally.

[1] Singapore University of Technology and Design, "Singapore maintains its lead and European cities dominate top 5, with Swiss cities in the spotlight, in 2021 global smart city index," October 28, 2021. https://www.sutd.edu.sg/About/happenings/Press-Releases/2021/10/Singapore-maintains-lead-in-2021-smart-city-index#:~:text=Singapore%20(1st)%2C%20Zurich%20(,of%20the%20COVID%2D19%20pandemic.

[2] Irene Y.H. Ng, Sun Sun Lim, and Natalie Pang, "Making universal digital access universal: lessons from COVID-19 in Singapore," Universal Access in the Information Society, 2022. https://doi.org/10.1007/s10209-022-00877-9.

[3] Statista Research Department, "Data centers–statistics & facts," June 13, 2022. https://www.statista.com/topics/6165/data-centers/#topicHeader__wrapper.

[4] Kent Chow. "Commentary: Where do data centres fit into Singapore's vision of green growth?", Channel News Asia, March 23, 2022. https://www.channelnewsasia.com/commentary/data-centres-energy-digital-economy-jobs-sustainability-2550996.

[5] Ibid.

[6] SG Green Plan, "Singapore Green Plan 2030 Key Targets," March 4, 2021. https://www.greenplan.gov.sg/key-focus-areas/key-targets.

[7] Knut Breivik, James M. Armitage, Frank Wania, and Kevin C. Jones. "Tracking the Global Generation and Exports of e-Waste. Do Existing Estimates Add up?", Environmental Science & Technology, 48(15) (2014): 8735-8743.

[8] Toxics Link. "Impact of e-waste recycling on water and soil," 2014. http://toxicslink.org/docs/Impact-of-E-waste-recycling-on-Soil-and-Water.pdf.

[9] United Nations Environmental Programme, "Basel Convention on the control of transboundary movements of hazardous wastes and their disposal," 2011. https://wedocs.unep.org/bitstream/handle/20.500.11822/8385/-Basel%20Convention%20on%20the%20Control%20of%20Transboundary%20Movements%20of%20Hazardous%20Wastes%20-20113644.pdf?sequence=2&amp%3BisAllowed

[10] National University of Singapore, "NUS and NTU launch first-of-its-kind tropical data centre testbed," June 16, 2021. https://news.nus.edu.sg/nus-and-ntu-launch-first-of-its-kind-tropical-data-centre-testbed/.

PACIFIC FORUM
INTERNATIONAL

pacforum.org | pacificforum@pacforum.org