Key Findings
US-Singapore Tech & Innovation Virtual Dialogue
Session #5: Considerations for US-Singapore Digital Economies in the Wake of the Invasion of Ukraine
April 18, 2022 (US) | April 19, 2022 (Asia)

On April 18, 2022, with the support from the US Embassy Singapore, the Pacific Forum hosted the fifth session of the *US-Singapore Tech & Innovation Virtual Dialogue*, "Considerations for US-Singapore Digital Economies in the Wake of the Invasion of Ukraine," with 25 participants from the government, private sector, academia, and other non-governmental organizations.

Lyle Goldstein, Director of Asia Engagement at the Washington think tank Defense Priorities; **Jaclyn Kerr**, Senior Research Fellow for Defense and Technology Futures at the Institute for National Strategic Studies (INSS) at National Defense University (NDU); and **Manoj Harjani**, Research Fellow in the Future Issues & Technology cluster at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University examined impacts of the Ukraine-Russian crisis for the US, Singapore, and Southeast Asia. The Key Findings from this closed-door meeting are below.

Key Takeaways

- No significant change has been observed in Sino-Russia relations as a result of the invasion of Ukraine. Chinese media has taken a largely pro-Russian stance.
- The Russia-Ukraine crisis could dramatically alter Russia-North Korea relations and Russia-Japan relations.
- ASEAN continues to struggle with the diverse and fragmented interests of individual member states, making a unified approach toward the conflict unlikely.
- Cyber warfare and cyberattacks have played a less significant role than initially expected. Russia has been relatively ineffective in information warfare beyond its borders.
- Conflict in Ukraine is likely to have widespread ramifications for digital supply chains and internet governance, challenging global internet freedoms and its openness.
- To prevent international sanctions from being circumvented, more cooperation is needed to address "crypto loopholes."
- Cross-border data flows and localization requirements will continue to be a difficult issue for many companies when trying to comply with sanctions.

Key Findings

Global and diplomatic ramifications

The Russia-Ukraine crisis has had far-reaching implications for the Southeast Asian region. No significant change has yet been observed in terms of Russia-Chinese relations.

Chinese media has taken a largely pro-Russian stance, identifying the West and NATO as key culprits in causing the conflict to erupt while highlighting Russian military successes. Although China has complained about the negative impact of sanctions and their financial consequences, its economy has not been highly affected.

Diplomatically, two areas within the Indo-Pacific where the conflict is likely to trigger dramatic shifts are 1) Russia-North Korea relations – which may evolve toward greater cooperation, and 2) Russia-Japan relations – where a further deterioration and consolidated bipolarity could emerge.

In terms of Southeast Asia and its response to the war and international sanctions, ASEAN member states continue to struggle with their diverse and often fragmented interests. This makes a unified and effective approach toward the conflict nearly impossible.

Internet freedoms and cybersecurity

Regarding discrete aspects of the Russian-Ukrainian conflict, cyber warfare has played a far less significant role than initially expected – particularly given Russia's extensive cyber capabilities. Although some cyberattacks were identified, these were reportedly successfully shut down.

The evident and relatively surprising lack of cyberattacks may be due to a variety of reasons. First, cyberattacks may have simply failed. Second, as Russia relies on the same infrastructure as Ukraine and the West, it may have refrained from attacks as initiating these would have negative consequences for its operations. Third, Russia may deem cyberattacks to be unpredictable and wants to avoid such unpredictability during ongoing military operations.

In terms of information warfare, Russia has not been very effective beyond its borders – Ukraine has had an upper hand in the information space. Nevertheless, to what extent Russian information operations have affected societies in the developing world or various extremist groups across Europe remains to be seen.

Of the many ramifications of the conflict, speakers focused on the impacts on digital supply chains and governance of the internet. They noted that until recently, the spread of the internet has occurred during a period of unipolarity and democratization. Whether the West will be able to guarantee a minimum level of global internet freedom and openness moving forward is unclear.

In the short term, countries – particularly those that openly stood up in support of Ukraine, including Singapore and the United States – need to prepare against further disinformation and cyberattacks and focus on enhancing their intelligence-sharing processes. In the long-term, the focus needs to be on ensuring and protecting global digital supply chains and internet freedoms.

Singapore's perspective

Singapore's overall trade and finance are unlikely to be significantly affected by the international sanctions. Presently, Russia accounts only for 0.1% of Singapore's total exports and 0.8% of total imports. Nevertheless, areas that should be closely monitored include "crypto loopholes," data flows, and localization requirements.

In terms of crypto loopholes – utilizing cryptocurrencies to circumvent financial sanctions – Singapore has put in place various national measures to prevent such operations. Similar measures have also been implemented by Japan. Crypto loopholes, while potentially relevant for individual and relatively small-scale circumventing operations, are unlikely to be significant on the macroeconomic level. Still, more international cooperation is needed to effectively address the issue.

For many companies, cross-border data flows and localization requirements represent a particular challenge in complying with international sanctions. Since 2006, Russia has had a data localization law that effectively pressures companies to store their data on in-country servers. More countries are expected to implement various data localization measures, which will further complicate companies' ability to navigate multiple jurisdictions.

Finally, speakers highlighted that while Singapore could serve as a key bridge to a more inclusive security architecture in Indo-Pacific, it cannot do so on its own. More engagement, more forums, and more participation are needed. The US and Singapore can collaboratively work toward these efforts.

This document was prepared by Michal Bokša. For more information, please contact Dr. Crystal Pryor (crystal@pacforum.org), Vice President of Pacific Forum. *These preliminary findings provide a general summary of the discussion. This is not a consensus document. The views expressed are those of the speakers and do not necessarily reflect the views of all participants. The speakers have approved this summation of their presentation.*