RSIS Webinar on "Technology Nationalism and Its Impact on Southeast Asia"

Speakers: Farlina Said, Jikon Lai and Alex Capri

9 October 2020

Background

The Centre of Excellence for National Security (CENS), S. Rajaratnam School of International Studies (RSIS), invited speakers Farlina Said, Analyst at the Institute of Strategic and International Studies (ISIS) Malaysia; Assistant Professor Jikon Lai, S. Rajaratnam School of International Studies (RSIS); and Alex Capri, Visiting Senior Fellow, NUS Business School, Research Fellow for Hinrich Foundation; for a RSIS webinar on "Technology Nationalism and Its Impact on Southeast Asia". The seminar was held in conjunction with the Singapore International Cyber Week 2020 (SICW). The audience was comprised of both international and local participants.

Presentation on *"Making the Technological Leap: Techno nationalism & Developing Nations"* by *Farlina Said, Analyst at the Institute of Strategic and International Studies (ISIS) Malaysia*

- While techno-nationalism can be defined as the linking of tech innovation to economic prosperity, social stability and national security, it is also about technological dominance which nations may wish to pursue.
- The strategic nexus of developing nations can differ, as nations are not homogeneous in technological development and have differing considerations in Southeast Asia (SEA). For instance, the ASEAN masterplan of connectivity in 2011 revealed that in some larger economies, only 2 out of 5 of people had 4G capabilities in their countries, while research from Google and Temasek revealed that 90% of citizens in ASEAN countries are connected to standard mobile data.
- SEA has welcomed MNCs to the region to upgrade technological content and labour skills. The transfer of technology has historically shown that it can be a pathway for development. Tech development can be used for furthering growth and opening opportunities in the region. Countries need to balance economic opportunities with trade-offs towards security and development, and having a sound knowledge of global and regional power dynamics.
- Each nation in SEA engages 5G partners differently (e.g. some partner with European telecomm or Chinese companies), and engagements are characterised by strategic perceptions. Vietnam, for instance, has engaged Ericsson to support 5G mobile services. Vietnam has also developed its own indigenous technologies, and has conducted trials in neighbouring Cambodia and Myanmar. Indigenous technologies allow for a firmer control on 5G capabilities and the facilitation of knowledge-based exchange (e.g. with South Korea).

The Centre of Excellence for National Security (CENS) is a research unit of the S. Rajaratnam School of International Studies (RSIS) at Nanyang Technological University, Singapore. Established on 1 April 2006, CENS is devoted to rigorous policy-relevant analysis of a range of national security issues. The CENS team is multinational in composition, comprising both Singaporean and foreign analysts who are specialists in various aspects of national and homeland security affairs.

Previous cyber incidents have led Vietnam to develop the importance of developing indigenous capacity to maintain control of information systems. In addition, strategic contestation in areas such as the South China Sea further drives the need to develop defensive capacity.

- Southeast Asian nations are likely to further strengthen and build engagements to develop domestic capacity in cybersecurity, IP and data protection. While increased engagements will continue to develop domestic capacity in respective countries, digital and physical literacy gaps within ASEAN countries could be a limiting factor for technological innovation ambitions. Countries should continue to develop a skilled labour force, build up knowledge bases and innovation systems.
- ASEAN nations need to prioritize Fulfilling the demands of domestic populations for digital connectivity and Improving the access of citizens to bridge existing digital divide.
- ASEAN nations can also set standards to ensure security by design in digital connectivity devices
- Lastly, greater cooperation amongst middle and small powers can contribute to lasting collaboration and cyber stability in the region.

Presentation *on "Economic Vulnerability & Dependency Indices"*, by *Assistant Professor Jikon Lai, Centre for Multilateralism Studies, S. Rajaratnam School of International Studies (RSIS)*

- China remains the biggest source of imports for goods to countries. The indices reveal that fewer countries that expected were heavily reliant on China – about 8 countries with a vulnerability index of over 50% had a heavy reliance on China for export goods. Countries such as South Sudan, saw export goods comprising up to 40% of the country's GDP. Within the Asia Pacific region, Hong Kong had the highest percentage in exported goods to China, totalling about 54.54%, followed by Australia, with 33.38%. Most countries in the indices were more heavily reliant on the US. In ASEAN, countries such as Vietnam and Singapore had a heavier dependence on the United States for export goods. Countries within ASEAN most exposed to China include Laos and Myanmar. The US remains the regional bloc's biggest trading partner, with inflows comprising up to 18.46% between the bloc and the country, followed by Japan.
- While countries have utilised economic instruments to influence and leverage economic vulnerabilities to sway the economic behaviours of trade partners and countries (e.g. export controls as a punitive measure against certain trade partners), SEA countries can focus on improving intra-ASEAN vulnerabilities, including the value of exports within ASEAN economies. Decoupling and risk management is dominated by a small number of economies who are particularly exposed to either US or China.
- The decoupling of economies and the fragmentation of production networks has made countries more vulnerable to erratic or random behaviours by great powers. The factors contributing to economic vulnerability include exports, inward investment flows, exporting trade in commercial services, and inward flow of remittances. A balanced

inflow and outflow of goods, services and investments would contribute to a greater level of economic interdependence. The balance of vulnerability versus interdependence is crucial for countries.

Presentation on "*Techno-nationalism and Southeast Asia*" by *Alex Capri, Visiting Senior Fellow, NUS Business School, Research Fellow, Hinrich Foundation*

- Techno-nationalism is defined as mercantilist behaviour that links a nation's technology prowess and capabilities with national security, economic competitiveness and social values and standards. A nation's preparedness and innovation is linked to national security. This creates a blur, fuzzy line in which strategies such as hybrid warfare and techno-diplomacy are deployed to create advantages in the tech nationalism arena, as economic competition hinges on the constant need for technological innovation.
- The current US-China technological 'cold war' tethers technology to ideological underpinnings. This tech hybrid 'cold war' focuses on specific strategic industries, such as technology and internet industry. Export controls and sanctions are targeted with the aim of creating a bifurcation of technology – with native domestically produced products touted as a secure, alternative viable option (e.g. 'make in India').
- Companies worldwide are facing urgent concerns over ring-fencing and strategic decoupling actions, as the impacts of nationalist policies would reduce the efficiency of supply chains. The diversification of supply chains, emphasis of localisation and the fragmentation of global supply chains would increase costs to businesses. Companies would need to increase localisation of supply chains, and re-shore some key activities to hedge against potential sanctions or tariffs.
- The main area for technology bifurcation revolves around the restrictions in sharing strategic dual-use technologies, in areas such as AI, semiconductors and robotics. Other areas of bifurcation include innovation (reducing collaboration in R&D, academia). The decoupling of data value chains (e.g. internet and cloud platforms in digital environments) is also of concern. Such actions have already taken place, with the proposed ban on TikTok and WeChat in the US, while India has already banned these Chinese apps.
- Future moves could see the potential decoupling of monetary systems, and see a gradual shift towards domestic digital currencies. China, for instance, has introduced e-RMB, its digital currency. Such moves would enable a reduction in dependence on the US dollar in trade, and to leverage its own digital business ecosystem (e.g. digital payments), encouraging trading partners to utilise and adopt such digital currencies.
- As mercantilism in innovation is set to rise, governments are paying greater attention towards increasing collaboration with their domestic private sector. The US and its allies, including the European Union, focusing on public-private partnerships with allies across industries in businesses and academia to foster greater R&D and innovation efforts. Technology alliances between companies is also set to increase.

- In strategic bifurcated industries, new levels of cooperation between governments and businesses are increased. This adds to greater pressure on businesses, especially on multinational corporations, as MNCs are increasingly viewed as strategic assets by home governments, or are conversely seen as strategic assets which further the tech nationalist objectives/policies of countries – and be potentially viewed as threats or government proxies by opposing governments. For instance, Chinese companies such as Tencent are building technologies which the Chinese government uses to pursue its objectives. Western Governments could view companies like Tencent as complicit with China's tech nationalist policies, and introduce sanctions.
- Issues surrounding data privacy, free speech and mass surveillance link political values and social values directly to technology. We are going to see more decoupling and the usage of non-tariff measures (e.g. export controls) as the beginning of the coalescing of the world into different groups (e.g. digital democracy versus techno-authoritarianism), where countries coalesce on competing technology standards and rule frameworks (e.g. GDPR in the EU). For Chinese companies, this presents an existential crisis, and it remains to be seen if Chinese companies can compete outside of China, and convince foreign regulatory bodies that their operations are divorced from the Chinese state and its cybersecurity laws.
- From a corporate governance standpoint, companies should evaluate how to manage strategic bifurcation and ring-fencing, and evaluate the implementation of 5Ts (Truth, Trust, Transparency, Technology and Talent) to manage issues pertaining to data privacy and other corporate and technology standards.

Discussion/Q&A

Many countries, including Southeast Asia, rely on MNCs. What would happen to MNCs that do not have a large country home base in the event of a bifurcation scenario worsens?

Capri: One of the things we would see in the corporate world is massive restructuring. This would be a challenge. For instance, the European Union passing laws banning foreign companies from buying local technology companies which have become distressed due to the COVID-19 situation. Actions by MNCs are likely to include consolidation, setting up vertically integrated value chains, and acquiring other businesses. Smaller companies operating in SEA, for example, which are experiencing supply chain disruptions, will experience greater challenges. However, bifurcation and strategic decoupling could provide greater opportunities for capacity building throughout Southeast Asia – silver linings for a range of industries (e.g. logistics) for innovative approaches.

What do you think of the current response of Southeast Asia countries to the pressures from both China and the US to choose sides?

Lai: Southeast Asia economies are extremely open. From the data shown in the vulnerability indices, Southeast Asia countries are equally exposed to both US and China at an aggregate level. At an aggregate level, ASEAN countries cannot really afford to cut ties with one or the other countries, and as a result, ASEAN states rely on hedging and managing risks and exposure. For most countries, exposure to both countries are quite reasonably well-diversified but are more concentrated exposure within various sectors (e.g. telecoms). Policymakers should drill further down into economic vulnerability data, identify sectors which are particularly important or exposed, and adopt measures to address concerns.

Digital technology is crucial for the development of economies. Will getting people online be enough for sustainable development (e.g. economic resilience), or are other measures important? If so, what are the other measures that are needed for sustainable development?

Said: Some problems could grow as more people come online, including potential problems such as data management. However, for digitalisation to be successful and effective, society needs enhanced digital literacy skills. Fundamental knowledge bases (e.g. innovation capacity, highly skilled labour workforce) would be able to shore up sustainability efforts for development.

How will continuing progress and involvement in the Belt and Road Initiative (BRI) – specifically, the Digital Silk Road – affect long-term economic vulnerabilities and techno-nationalism across Southeast Asia?

Capri: The digital BRI will continue to be an increasingly contentious issue, particularly along the debate of values of digital democracy versus techno-authoritarianism. Chinese companies are providing most of the digital infrastructure for technology ecosystems along the digital BRI. The notion of negative reciprocity will continue to grow – the US, EU and Australia, for instance, are setting up funds to potentially convince countries along the BRI from buying Chinese equipment, and diverting them to potentially buy Nokia and Samsung equipment, thereby amplifying technology mercantilism linked to differing values on technology and ideology.

Lai: Governments, particularly in Southeast Asia, are struggling to balance perceived security issues and economic and technological wellbeing. Concerns over data privacy or security issues might not be highly prioritised over consumer choices, benefits and convenience by the average consumer when using a technology product or service. With respect to Western concerns over perceived security issues, the domestic debates of various countries, especially in Southeast Asia, should be respected. Ultimately there might be varied responses across Southeast Asian countries with regards to approaching the BRI.

Said: Although the Digital Silk Road has been launched for a few years now, some of the results of the initiative have yet to be seen. While some of the Digital Silk Road engagements on telecommunications have occurred, some components of the Digital Silk Road and BRI are bilateral in nature, and extend to partnerships on health and other technologies. It would be interesting to see if the Digital Silk Road promises to deliver on assistance to countries. One area for further study would be the 'Made In China 2025' and 'China Standards 2035' plan, and evaluate impact on geopolitical dynamics for the Southeast Asian region and create geopolitical vulnerabilities in the future.

The debate around techno-nationalism has revolved around the actions of the US and China. Do you see any role for Russia in the current economic and technological development of ASEAN states?

Capri: Russia is not likely to play a big role in Southeast Asia. Of concern might be the potential weaponisation of trade in rare earth minerals (used for technological devices), of which China has a monopoly on rare earth. As the global development of alternate rare earth continues, Russia might be a potential supplier in the rare earth industry, which could result in less leverage for China.