Annex B: Key points from Minister's remarks at panel session - "How can Governance Frameworks keep pace with Technology?"

Guiding Questions:

- Why does technology governance matter? How can it support trust and innovation?
- What is the existing architecture of technology governance for digital technologies? What are the remaining gaps and emerging issues?
- What role can norms and principles play in a more inclusive approach to technology governance?
- Singapore is a small but influential country in these discussions. What do you see as the main challenges for technology governance, in particular for digital technologies? What is Singapore's approach to technology governance?"

1. The landscape for technology changes quickly and often, unpredictably.

2. In navigating through such a landscape, **Singapore has only one NorthStar, and that is the well-being of our people.** What does that mean? It means, whether in the digital domain or any other domain, we will do what it takes to:

   a. Promote economic vitality
   b. Preserve social stability
   c. Protect public security

3. Where businesses are concerned, we **generally regulate with a light touch, provide clear rules and certainty, and give as much room as possible for innovative ideas to thrive**.

   a. Singapore-based tech start-ups have been able to innovate, test their business models, and attract investors at a rapid pace. Singapore accounts for the lion's share of unicorns in Southeast Asia – 15 out of 35 in the region (43%).[1] Ranked joint fourth in the world for how fast its start-ups turned into unicorns.[2]

   b. 40% of all new jobs created through new investments are "digital jobs". Tripled our IHL intakes.

4. It **doesn't mean we avoid rules when they are necessary**. For example:

   a. We were concerned about the risks of misinformation. True enough, six in ten people in Singapore received false information about COVID-19 on social media.[3]

[1] Source: Credit Suisse ASEAN Equity Research report on ASEAN Unicorns, released on 5 October 2021. The 15 unicorns in Singapore are: Acronis (software), Advance Intelligence Group (fintech), Carousell (e-commerce), Carro (e-commerce, car sales), HyalRoute (telecommunications), JustCo (real estate tech), Lazada (e-commerce), Matrixport (fintech), Moglix (e-commerce, industrial supplies), Ninja Van (logistics), NIUM (fintech), PatSnap (Software-as-a-Service), PropertyGuru (real estate tech), Secretlab (consumer goods), Trax (technology, retail solutions). Note: Credit Suisse's list excludes start-ups that are in the process of public listing, such as Grab.

[2] Source: British price comparison website Money.co.uk. Singapore is ranked after China (5 years 10 months), Hong Kong (6 years 1 month), Japan (6 years 3 months) and joint fourth with the US (6 years 11 months).

[3] 700 participants participated in the joint study conducted by the National Centre for Infectious Diseases, NTU Wee Kim Wee School of Communication and Information, and NUS Saw Swee Hock School of Public Health, which was published in May 2020.

    i. Egregious examples: Singapore had run out of face masks, and that COVID-19 vaccines are not effective.

    ii. Singapore's Protection from Online Falsehoods and Manipulation Act (POFMA) enables the government to fight the spread of online falsehoods through a variety of means, such as requiring facts to be put up alongside the falsehoods, issuing take-down orders, and imposing criminal charges on those who knowingly spread falsehoods.

    iii. Since POFMA came into force in October 2019, it has been used 32 times, of which over half (18) were to correct COVID-19 misinformation. Taking swift action against such falsehoods has helped to build trust about vaccines, and allowed us to achieve high vaccination coverage with 94% of eligible population fully vaccinated.

b. For gig workers, we watched closely for several years.

    i. Those depending on internet platforms are still just about 3% of our workforce.[4]

    ii. Decided that that there will be long term consequences for certain profiles e.g. delivery riders which approximate regular employment in terms of control and earn a modest amount.

    iii. Studying how best to safeguard their long term interests – ability to afford healthcare and retirement.

c. We were one of the first to have cybersecurity legislation.

    i. But we know it is not enough to secure critical information infrastructure (CIIs). Overall crime is low and continues to fall, but share of cybercrime shot up to 43% in 2020 (from 26.8% in 2019).[5]

    ii. Need to help enterprises - Singapore's Cybersecurity Agency has tailored cybersecurity toolkits for large enterprises as well as SMEs.

    iii. Also need to enhance protection for individuals through community outreach programmes and government-developed apps to block scam calls and scan messages (i.e. ScamShield).

5. Key challenge in tech governances is making an appropriate judgement.

a. Neither moving too early or too late.

b. Nor relying solely on rules and regulations, or avoiding them completely.

c. Not believing we get everything right the first time, nor lacking the courage to stay on course.

6. The **destination is clear.**

[4] Source: MOM COS 2021 speech.

[5] There were 16,117 cybercrime cases reported in 2020, up from 9,349 in 2019. Source: Singapore Cyber Landscape 2020, released on 8 Jul 2021.

a. We all need to embrace a digital future.

b. But territory is unchartered.

7. No **single path that works for every country**. How we can help each other:

a. Develop better compasses.

b. Share roadmaps.

c. Establish rules of the road that make the journeys safer for everyone.

8. At the same time, we also see space for policy collaboration with tech companies which want to step up as responsible players in society, especially in emerging fields like AI and 5G.

a. Co-developing standards or certification to provide assurance, and opening up test-beds more widely to get a better sense of how the technology is developing first, before assessing whether there is a need for further regulation.

i. AI governance testing[6] - allows AI system owners to demonstrate that their AI is trustworthy. Singapore is pilot testing our AI Governance framework and toolkit with several companies. Have aligned the governance principles of the testing framework with global standards, such as those by the OECD, and the EU, as well as our Model Governance AI Framework.

ii. 5G test-beds – opened up 4 test-beds across the country to all businesses, to encourage innovation of new use cases, while studying any potential risks.

Guiding Questions:

- What new principles are needed?
- How can governments foster agile regulation?
- What are possible new approaches to technology governance? What new frameworks, processes and institutional arrangements are required? How can these be made inclusive?
- How to move forward on technology governance at the global level?
- How do we move forward on these challenges? How is Singapore seeking to build trust in digital technologies? What opportunities do you see in Asia, including in the ASEAN context?”

1. We are quite fortunate in Singapore, and perhaps unusual, in that the degree of trust in society and institutions is quite high.

a. International surveys like the Edelman Trust Barometer indicate that in Singapore:

[6] The AI Governance Testing Minimum Viable Product (MVP) consists of two components: (a) a testing framework and (b) a testing toolkit. The testing framework is developed by referencing global principles, such as those issued by OECD, EU High Level Expert Group, and our own. Some elements can be audited (e.g. documentation), but there are certain elements of trustworthiness that can be tested through software tools, e.g. explainability, and bias. The toolkit is a selection of open source testing tools that PDPC has assembled into a single package that companies can use to conduct the tests. PDPC has developed an MVP and is in the process of pilot testing them with 5 companies.

i. Trust in all institutions have increased over the past year during the pandemic, and;

ii. The government is the most trusted institution (ahead of NGOs, businesses and media).[7]

b. The challenge is less in building trust but not allowing it to be eroded.

c. Much harder to regain trust when it is lost.

2. This is why we take the risks very seriously.

a. Misinformation – do we wait or we take preventive measures before people have lost confidence in what they come across online?

b. Personal Data Protection – we allow for legitimate business use and supply companies with business intelligence tools that process data responsibly, but there must also be accountability when there are breaches. We make clear the rules on notification, for example, and ensure problems are rectified.

c. Cybersecurity – e.g.:

i. For our 5G networks we're interested in not just performance, but security and resilience. MNOs know how strictly we audit them.

ii. We developed a Cybersecurity Labelling Scheme for consumer smart devices, the first of its kind in the Asia-Pacific region.

3. Still, we must not expect everything to be smooth-sailing. There will inevitably be occasions when trust is shaken. How can we prepare for them?

a. Build multilateral partnerships and develop international norms.

i. In our region, Singapore hosts the ASEAN-Singapore Cybersecurity Centre of Excellence to strengthen regional cyber resilience and capabilities to deal with cyber threats.

ii. ASEAN has been a champion for international cyber rules, and is the only regional organisation to subscribe in-principle to the UN's 11 voluntary, non-binding norms of responsible state behaviour in cyberspace.

iii. Also helping to drive the multi-stakeholder approach to strengthen cybersecurity cooperation at the UN. Our Permanent Representative to the UN in New York has been elected as chair of the five-year UN Open-Ended Working Group (OEWG) on cybersecurity.

b. Certification mechanisms are also important to signal responsible practices.

i. Singapore developed a Data Protection Trustmark for companies, and also adopted the standards in the APEC Cross-Border Privacy Rules (CBPR) so as to allow businesses to exchange data across borders more seamlessly.

[7] Source: Edelman Trust Barometer report released on 18 Mar 2021.

4. One area of great potential is AI.

    a. Our Model AI Governance Framework provides detailed guidance to the industry and organisations to address key ethical and governance issues when deploying AI solutions.

        i. Also developed a Self Assessment Guide so that businesses can translate the high level principles into practical action

    b. The Model AI Governance Framework has also been adapted further by sectoral regulators to address their specific sectoral needs – for example financial sector (which focuses on issues of fairness and discrimination) and healthcare (patient-centricity and managing use of sensitive healthcare data).

    c. As mentioned earlier, we are also developing an AI governance testing and certification framework to help businesses be more transparent about their AI systems, to build trust with their stakeholders.

5. If I can just supplement what I said earlier about navigating in uncharted territory.

    a. Apart from compasses, roadmaps and rules of the road, we're really trying to **develop the safety harnesses and airbags**, if you will.

    b. Making sure businesses **have and know and their obligations**, but also having **the tools to succeed in the digital domain.**