FRAMING POLICIES FOR THE DIGITAL ECONOMY

TOWARDS POLICY FRAMEWORKS IN THE ASIA-PACIFIC
National University of Singapore (NUS) is a leading global university centred in Asia influencing the future. Ranked 1st in Asia, the university is renowned for its high quality of pedagogy standards and teaching faculty to develop future ready graduates.

Institute of Systems Science (ISS) is a training institute of NUS and aims to nurture leaders of the infocomm industry, as well as develop aspiring and seasoned infocomm professionals through the sharing of real world insights and experiences.

Singapore e-Government Leadership Centre (eGL) is a Centre of Excellence for Digital Government capacity building, research and consulting at the ISS, NUS.

www.iss.nus.edu.sg

UNDP partners with people at all levels of society to help build nations that can withstand crisis, and drive and sustain the kind of growth that improves the quality of life for everyone. On the ground in more than 170 countries and territories, we offer global perspective and local insight to help empower lives and build resilient nations.

The Global Centre for Public Service Excellence is UNDP’s catalyst for new thinking, strategy and action in the area of public service, promoting innovation, evidence, and collaboration.

www.undp.org/publicservice

Author: Peter Lovelock

Disclaimer: The analysis and policy recommendations in this publication do not necessarily represent those of the of the National University of Singapore, the United Nations, including UNDP, or the UN Member States.

© 2018 UNDP Global Centre for Public Service Excellence, #08-01, Block A, 29 Heng Mui Keng Terrace, 119620 Singapore, Singapore
We hold these algorithms to be self-evident, that all Internet users are created equal, that they are endowed by their software with certain unalienable Rights, that among these are digital Life, e-Liberty and the pursuit of Internet Happiness.

The fourth industrial revolution is sweeping the world by storm. A digital ‘Declaration of Independence’ is demanded to enable all humanity to benefit fairly from the coming upheaval. In this new digital economy, every country is faced with unprecedented opportunities and challenges which are fundamentally different from the previous revolution. Entire industries are being disrupted and transformed.

New platforms of collaboration and competition across the public, private and people sectors are presenting urgent imperatives for governments to innovate, to redesign services, and to rethink policies. The legitimacy of digital government will depend on fostering citizens’ consent through a digital social contract that embraces e-equity and value creation.

Digital government policies must foster agility, innovation and value creation. Every public servant, industry professional and citizen must embrace digital transformation, and have access to learning opportunities to develop deep and holistic skills to thrive in this new era.

Singapore e-Government Leadership Centre
Institute of Systems Science, National University of Singapore

Global Centre for Public Service Excellence
United Nations Development Programme
Table of Contents

CHAPTER 1: Framing the Digital Economy ................................................................. 5
  What is a Digital Economy? .................................................................................. 5
  Digital Disruption .............................................................................................. 7
  What is New about the Digital Economy? .......................................................... 12
  Challenges for Policy Makers and Regulators ..................................................... 13
  What Does the Government Need to Do? ............................................................ 14

CHAPTER 2: Regulatory and Policy Challenges ................................................. 16
  Creating a National Broadband Network .............................................................. 16
  Interoperability of Platforms .............................................................................. 18
  The Sharing Economy ....................................................................................... 18
  Privacy and Data Protection ............................................................................... 19
    Personal Data Privacy ....................................................................................... 20
    Data Protection ................................................................................................. 20
  Cybersecurity ..................................................................................................... 21
  Sovereignty and Cross-border Data Flows .......................................................... 22
    Sovereignty Issues ............................................................................................ 22
    Cross-Border Data Transfer Issues .................................................................. 23

  Approaches to Digital Development .................................................................... 24
  Government-led EU vs Private Sector led US ...................................................... 24
  Top-down Singapore vs Bottom-up Hong Kong ............................................... 25
  Innovative China vs Regulated Japan .................................................................. 27
  Other Digital Transformation Strategies that Provide Global Benchmarks ............ 29
    Box 1: Estonia: A Digital Society for Digital Citizens ....................................... 30
    Box 2: India: A Digital Identity Platform to Build On ....................................... 30
    Box 3: Kenya: Financial Inclusion via Mobile Phones ....................................... 31

CHAPTER 4: Digital Economy Planning in Asia: Malaysia, Thailand and Vietnam ........................................... 32
  Malaysia .............................................................................................................. 32
  Digital Planning in Malaysia .............................................................................. 34
Thailand .................................................................................................................. 36
Digital Planning in Thailand .................................................................................. 37
Vietnam .................................................................................................................... 38
Digital Planning in Vietnam .................................................................................. 39
Comparative Assessment: Malaysia, Thailand, Vietnam ........................................ 40

CHAPTER 5: Recommendations: Building Blocks for a Digital Economy Framework ........ 44

Measurement and Goal Setting ............................................................................. 44
Leadership and Coordination Competencies ...................................................... 44
Strategic Choices on Platforms ............................................................................ 46
Policy Approaches and Tools for Effective Digital Governance ......................... 47
CHAPTER 1: Framing the Digital Economy

In September 2017, Alipay users can walk into any KFC (Kentucky Fried Chicken) in Hangzhou (China) and ‘smile to pay’ enabled by facial recognition technology – as part of a pilot programme by Alibaba’s Ant Financial. By 2018, students at the tropical campus of the National University of Singapore will see drones carrying parcels as part of a trial by Airbus Helicopters and the Civil Aviation Authority of Singapore - the same technology has already been tested to deliver medicine in rural Rwanda and New Zealand.

These are just a few examples of the rapid changes over-taking economies and societies as they ‘go digital’. The emergence of the digital economy is transforming the world at an unprecedented scale, scope and complexity. Challengingly, the transformation is characterised by disruption across almost all sectors of industry and society leading to the emergence of new forms of production, management and governance. The opportunities emerging for governments to reach and enable citizens with services are quite profound, but so too are ways in which the government must reappraise its role and approach. To begin to frame this dynamic, this chapter provides a broad definition of what the digital economy is, and an overview of the impact and potential of the new technologies underpinning and driving digital disruption. It then discusses the unique characteristics of the digital economy in terms of scale and scope and briefly introduces the effect of digital transformation on governments.

What is a Digital Economy?

There is no universally accepted definition of the digital economy, but a most common, albeit somewhat narrow understanding is the share of GDP accounted for by the ICT sector. (Identifying what this is and comparing across different economies raises its own set of problems.) This report relies on a much broader concept and defines the digital economy as “the entirety of sectors that...”

---

4 Note, the term ‘disruption’ is here used to denote the upsetting of existing businesses and/or business models, and as such, is part of a process of transformation; while the term ‘transformation’ implies a much broader change in economic and social parameters, for example, the demise of agriculture or heavy industry and the rise of the information society.
operate using Internet Protocol (IP)-enabled communications and networks” irrespective of industry.6

Digital technologies have been deployed in different parts of national economies for decades, notably in communications networks, but it was the Internet and IP-enabled networks that created a universal platform to form the foundation of the digital economy for all sectors. The distinction between the Internet economy and the digital economy (though the terms are often used interchangeably) rests on the difference in sectoral impact: Internet economy “refers to the economic activities, inputs, outputs and employment directly associated with the use of the Internet.”7 By contrast, the digital economy relies on enhanced interconnectivity of networks and the interoperability of digital platforms in all sectors of the economy and society to offer convergent services. For example, digital traffic can cross between telecommunications and banking networks – such as in the case of payments apps running on India’s Unified Payments Interface, which enable funds transfers among customers and merchants using various mobile network service providers and financial institutions.8

“Going digital”9 is an all-encompassing shift beyond the economic sphere, which impacts society, culture, politics, and technological development. For this reason, governments and public bodies responsible for the welfare of citizens need to understand what “going digital” entails, and what challenges and opportunities it offers.

There have been numerous studies on the economic impact of the digital economy upon the GDP of countries. Such attempts at quantifying have thus far been somewhat problematic due to the lack of well-established measurement criteria, and thus the lack of reliable data. An oft-cited 2011 study by the McKinsey Global Institute estimated that the Internet accounts for 3.4% of overall GDP in the 13 nations studied.10 In 2014, the OECD measured the digital economy, defined more widely as the ICT sector, as accounting “for 6% of total value added, 4% of employment and 12% of total fixed investment in the OECD area.”11 These studies provide useful benchmarks and indicators of the extent of the impact, but they have proven less applicable as policy guides or models for governance. Studies focused on measuring the impact on a sectoral level (e.g. e-commerce) or on non-financial metrics (e.g. the rate of financial inclusion) offer more straightforward assessments,

8 National Payments Corporation India (2016), Unified Payments Interface (UPI), http://wwwnpci.org.in/UPI_Ba gground.aspx
9 The title of the landmark book by Nicolas Negroponte in 2000
but are also hard to evaluate as a comparative analysis is impossible in the absence of a methodology for consistent and extendable digital data collection. This is important because the choices required and the opportunity cost involved in assigning resources to the development of the digital economy can be significant and without a demonstrable case of impact, such resource diversion can be hard to justify and maintain.

**Digital Disruption**

Digital disruption occurs in various ways:

1. *Product or service substitution*, such as the displacement of music cassettes and compact disks with streamed music online, or more starkly, the displacement of printed motorway maps by GPS systems in smartphones which are now widely used to navigate drivers
2. *By-pass*, whereby for example, payment no longer goes through the existing gatekeeper thereby eliminating demand for its services, as in the case of P2P funds transfer offered by TransferWise, which by-passes banks or online insurance sales platforms, which eliminate the need for an agent network;
3. *Technological paradigm shift*, such as cloud computing, which represents a fundamental change in how consumers procure, access and use IT infrastructure while offering lower costs and rapid scalability.

Cloud computing, blockchain or the Internet are what economists call a General Purpose Technology (GPT), meaning they bring a significant impacting shift *across all sectors* of an economy and society as a result of the technology’s introduction. GPTs’ rate of adoption may vary from sector to sector, but as economies become increasingly interconnected they become embedded and ubiquitous. Classic examples of a GPT include electricity or the combustion engine.

The table below describes the impact of such “game changing” technologies, which have been or will be most likely disrupting the economy and society. The impact potential of most of these GPTs is yet to be fully revealed, but their applications are already being widely forecast likely giving rise to shifts in technology paradigms.

<table>
<thead>
<tr>
<th>Technologies</th>
<th>Impact</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>5G (or ubiquitous connectivity)</td>
<td>5G networks will enable data collection and computation with</td>
<td>The capacity, transmission speeds and latency that 5G needs to achieve</td>
</tr>
</tbody>
</table>

12 For the distinction between 'disruptive' and 'transformative' see footnote 4 above. Table 1 abstracts from cross-cutting issues, such as the impact on employment, investment, data analytics, etc.
billions of devices by providing seamless and continuous connectivity. More than just being faster than 3G and 4G LTE, 5G will "become the underlying fabric of an entire ecosystem of fully connected intelligent sensors and devices, capable of overhauling economic and business policies, and further blurring geographical and cultural borders." 5G is predicted to create 22 million jobs worldwide and USD 12.3 trillion of revenue across a broad range of industries.\(^\text{13}\)

requires operators to invest heavily in network trials and rollouts, with no guarantee as to returns on investment. In China alone, mobile network operators are forecast to spend a combined USD180 billion by 2023.\(^\text{14}\) Also, challenging will be standardizing spectrum bands and network interconnectivity, both of which will enable the low-cost access and universal interoperability demanded by core 5G use-cases, and which will be key to recouping investment.\(^\text{15}\)

### Internet-of-Things and Machine-to-Machine networks

By 2020, there will be more than 20 billion installed IoT devices around the world generating massive amounts of data. With access to this kind of information, industries of all kinds will be able to reach new levels of efficiency as they add products, services, and capabilities.\(^\text{16}\)

Security is a major challenge to the IoT as newly connected "things" bring about new vulnerabilities. The hacking of baby monitors, surveillance cameras, smart fridges and so on exemplify the security threat that can only grow with the scale of the IoT. As the number of connected "things" increases, so will the amount of personal data collected, stored and transmitted over networks, therefore exacerbating risks that such data is compromised.\(^\text{17}\) Moreover, as data can be compromised at any one point in the IoT ecosystem, stakeholders (device maker, platform, network provider, end-user etc.) throughout the ecosystem should be vigilant and responsible for IoT security.

### Cloud computing

Cloud computing technology delivers IT resources (such as)

While the benefits of cloud computing are widely understood

---


\(^\text{15}\) ITU News (2013), Challenges to 5G standardization, [https://itunews.itu.int/en/4619/challenges-to-5g-standardization.note.aspx](https://itunews.itu.int/en/4619/challenges-to-5g-standardization.note.aspx)


software, computing power for data analytics, data storage) online as a service. Cloud services are scalable and on demand, accessible from all connected devices. They are changing procurement models both in the private and public sector and offer flexibility and lower costs with increased security features compared to traditional IT resources.

<table>
<thead>
<tr>
<th>Platform (or Management) Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data analytics</strong></td>
</tr>
<tr>
<td>Big data is the fuel of the digital economy and data analytics is essential to make data-driven decision making possible. Data analytics also aid the optimisation of service delivery and create competitive value chains in every industry.(^\text{19})</td>
</tr>
<tr>
<td><strong>Digital identity</strong></td>
</tr>
<tr>
<td>Digital identity schemes are largely biometric and state-operated platforms, which enable the identification, verification and authentication of citizens. As a cornerstone of government services, such initiatives allow for targeted public service delivery without intermediaries, and increased participation.</td>
</tr>
<tr>
<td><strong>Blockchain</strong></td>
</tr>
<tr>
<td>Blockchain technology can optimise the time and costs of any transaction with fast, verified, and highly secure movement of records based on decentralised and publicly validated distributed ledger. Blockchain has the potential to enable applications that allow to</td>
</tr>
</tbody>
</table>

---


\(^\text{20}\) Ashit Talukder (2015), Big Data Open Standards and Benchmarking to Foster Innovation, https://kb.osu.edu/dspace/bitstream/handle/1811/75417/1/ISILP_V10N3_799.pdf

\(^\text{21}\) The Straits Times, Benjamin Goh (17 Mar 2017), One digital ID to rule them all?, http://www.straitstimes.com/opinion/one-digital-id-to-rule-them-all
keep, identify and track exchanges and registers at minimum cost avoiding the potential risk of corruption. It allows community collaboration and business consolidation in various industries including payments, business services and logistics.\(^\text{22}\)

While there have been various initiatives, including the formation of an ISO technical committee, to examine standardization issues related to blockchain, a lack of internationally-accepted standards has made firms developing blockchain Proof of Concepts (PoCs) wary about committing to the technology.\(^\text{23}\)

### Quantum computing

Quantum computers will become the sixth paradigm in computing replacing bits with quantum bits, which allow them to solve complex problems beyond the capabilities of conventional computers.\(^\text{24}\) This leap forward in computing capability will enhance data processing and pattern recognition in machine learning, and significantly improve modelling capability in drug development, material science, climate change research and AI development.

Development of actual quantum computers is still at an early stage due to the complexities in building an actual practical quantum computer. The quantum system needs to be protected from outside interference, yet still able to be used to make calculations and churn out an answer.\(^\text{25}\) Current solutions involve features like dampeners and extreme cold (approaching absolute zero) to insulate the actual quantum computer chip.\(^\text{26}\)

### Application (or end-user) issues

| Cryptocurrencies | Cryptocurrencies are digital currencies, where encryption technologies regulate the generation of units of currency and verify the transfer of funds, operating outside of the banking system. Bitcoin or Ethereum are well-known examples, though even they face public uncertainty about security and operational resiliency. | The real-life values of cryptocurrencies are highly volatile as they are dependent on demand and supply of users. A cryptocurrency’s value is largely determined by the number of users and the amount of transactions that indicate the demand.\(^\text{27}\) In addition, liquidity is dependent on the demand and supply, where the lack |

---


\(^\text{23}\) BSI, Advait Deshpande et al. (May 2017), Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospect for standards, [https://www.bsigroup.com/LocalFiles/zh-tw/InfoSec-newsletter/No201706/download/BSI_Blockchain_DLT_Web.pdf](https://www.bsigroup.com/LocalFiles/zh-tw/InfoSec-newsletter/No201706/download/BSI_Blockchain_DLT_Web.pdf)

\(^\text{24}\) The first five paradigms in computers were: (1) Electromechanical; (2) Vacuum Tube; (3) Relay; (4) Transistors; and (5) Integrated Circuits. [https://singularityhub.com/2016/10/10/massive-disruption-quantum-computing/](https://singularityhub.com/2016/10/10/massive-disruption-quantum-computing/)


\(^\text{27}\) Medium, Alex Fork (15 Dec 2016), The Challenges of Cryptocurrencies, [https://medium.com/@Alex_Fork/the-challenges-of-cryptocurrencies-3d78591941a6](https://medium.com/@Alex_Fork/the-challenges-of-cryptocurrencies-3d78591941a6)
| Artificial Intelligence | Artificial Intelligence (AI) enables new form of automation combining robotics and machine learning. AI will improve the speed, quality, and cost of available goods and services, but is also likely to displace large numbers of workers. \(^{29}\) | In addition to the challenges AI will face in its application to robotics and autonomous vehicles, the reliance of AI development on data input can lead to AI inheriting human-originated biasness that may limit the possibilities of applying AI in certain regards. For example, the dominance of white males in the AI industry has led to skewed outcomes such as AI-judged beauty contest that awarded mostly white candidates. \(^{30}\) |
| Robotics | Robots have been reshaping the division of labour between men and machines, and will increasingly do so outside of large factories as small-scale, adaptable production becomes more common in manufacturing processes. Robots will have a significant role in plastics, medical devices, food and beverages and the high-tech industries. | A common concern among policy-makers, workers and consumers is the ability to balance the economic and social impacts of robotics advancement. In Dongguan, China, a factory replaced 90% of its human workforce with machines, resulting in a 250% increase in productivity and 80% reduction in defects. \(^{31}\) Tax, liability and the displacement of workers are some issues that need to be addressed amid the co-existence of robots and humans in the workplace. |
| 3D printing (Additive manufacturing) | 3D printing makes products via an additive layer-by-layer approach and is a game changer in manufacturing as it enables mass-customisation and reduces waste. It reduces time-to-market, eliminates the need for | 3D printing may bring forth copyright issues as strict enforcement of intellectual property rights on digital files containing information required for 3D printing may prove to be difficult, expensive |


\(^{30}\) TNW, Ben Dickson (2017), 4 Challenges Artificial Intelligence must address, https://thenextweb.com/artificial-intelligence/2017/02/27/4-challenges-artificial-intelligence-address/#.tnw_GkJj2Dx9

\(^{31}\) Futurism, Kirstin Houser (9 Feb 2017), Production Soared After This Factory Replaced 90% of Its Employees with Robots, https://futurism.com/2-production-soars-for-chinese-factory-who-replaced-90-of-employees-with-robots/
<table>
<thead>
<tr>
<th>Large inventories, lowers labour costs and transportation needs. By 2025, 3D printing can have an impact of USD 577 billion annually. and even counter-productive. In addition, the ability to use 3D printing technology to manufacture proprietary items, as well as illegal or controlled items such as guns, could trigger the need to regulate access to machines and materials, keeping costs high and out of reach of the mass market.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autonomous vehicles</td>
</tr>
</tbody>
</table>

**What is New about the Digital Economy?**

The digital economy is built off two key network developments of the Internet and IP-enabled communications systems – such as mobile networks, electronic payments systems and public service networks:

1. **Interconnectivity** of networks means that traffic can travel across and between networks. This enables economies of scale as the fixed costs of infrastructure rollout are spread across a greater level of output bringing about a fall in unit costs. In the early days of networks, resistance to interconnection was a way to maintain a dominant position, but following

---

35 Nidhi Kalra (2017), Challenges and Approaches to Realizing Autonomous Vehicle Safety, [https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT463/RAND_CT463.pdf](https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT463/RAND_CT463.pdf)
regulatory intervention, the network effect of interconnection in the market-as-a-whole could operate.

2. **Interoperability** of operating platforms means that traffic can run effectively across different types of networks (e.g., from telecoms to banking to educational to health networks and so on). This enables economies of scope, as fixed costs are spread across a wider range of output of different products and services. However, it is still the case in many markets that inter-operability is resisted to maintain exclusivity and market dominance. Regulators need to decide if intervention will disrupt innovation or will accelerate the network effects.

Economies of scale arise from the network effects of having everybody come online, while economies of scope is what fuels innovation and offers cross-fertilisation of opportunity across sectors, hence the emergence of FinTech (finance+technology) and agritech (agriculture+technology), among others. Economies of scale and of scope create a virtuous cycle by driving down costs, increasing user choice of products and services and, in turn, stimulating market innovation and economic growth. A good example is the completely new combination of Artificial Intelligence and high-speed broadband. AI works through apps and algorithms applied to data, and creates innovative products and services in several industries from manufacturing to entertainment. Broadband provides the network capacity and speeds required, and operates based on economies of scale.

**Challenges for Policy Makers and Regulators**

From a policy maker and regulator’s point of view, the emergence of the digital economy changes the landscape. As industries, markets, and pricing strategies are transformed, the traditional industry-specific approach to policy setting will increasingly fail to enable expected economic growth and social development outcomes. How to advance financial inclusion without focusing on connectivity, social media, identity profiling? How to successfully advance **effective** universal education without consulting data analytics, behaviour profiling, content delivery, and collaborative communication? Even more challenging is the job confronting the regulator with the traditional risk management-oriented approach failing to deliver expected regulatory control or provide adequate

---

37 GSMA (2016), Advancing Digital Societies in Asia, [https://www.gsmaintelligence.com/research/?file=9f48d32ff0671fb7dbbcb4efb84ecb0&download](https://www.gsmaintelligence.com/research/?file=9f48d32ff0671fb7dbbcb4efb84ecb0&download), p. 5
38 It is a combination that has given rise to what has been termed ‘Industry 4.0.’ It reflects a shift in economic value from manufacturing (2.0) and services (3.0) to information and intellectual property. This needs some clarification. The growing importance of ‘data’ as market intelligence or as patents for innovative services or as programmed information for machine tools, has been around since the industrial revolution, and was greatly accelerated as economies shifted from a focus on manufacturing to services. This was widely known by the 1980s as the rise of the Information Society. However, more recent advances in AI and in broadband technologies have lifted economies to a ‘Next Generation’ level.
consumer protection. Is Uber a taxi company or a software company? Is Alipay a bank or non-bank financial institution, or is it a technology (or e-commerce) company?

Moreover, what is a ‘monopoly’ and what is adequate market competition in such cross sectoral growth? Previously-dominant regulated companies have lost ground to a new wave of ‘next generation’ companies. Market definitions that were vital to regulators when identifying “significant market power” are increasingly failing to work, or work effectively. As an editorial in the London Financial Times aptly put it, “Competition regulators need to arm themselves with new concepts. On mergers, rather than concentration in particular markets, the focus should shift to the potential for customer lock-in.”39 Two further important points are raised: “Ensuring the interoperability of technology will be key…. and the need for regulators to take account of the role of dynamic pricing algorithms which effectively “eliminate the very notion of market prices, and with it the consumer surplus.”40

Furthermore, in the digital world governments can deliver certain public services in a more targeted way at minimal cost with increased agility and impact. Once the digital infrastructure is in place – such as the broadband network, a digital identity and authentication system – new services can be added at a much lower cost. Governments can also experiment and innovate relying on the aggregate demand and direct feedback of citizens in an environment where location is immaterial, and the cost and methods of communication have been drastically altered. This increased ability to deliver innovative public services represent an opportunity for policy makers to create public good, at the same time requires improved agility and responsiveness from public administrations, particularly in the face of changing citizen expectations.

**What Does the Government Need to Do?**

For the policy maker, the opportunity cost in decision making and resource allocation changes substantially, as do the social development and economic growth targets that can be set. For the

39 Financial Times (31 July 2017), Competition authorities need a digital upgrade, https://www.ft.com/content/f6fe0f18-73d1-11e7-aca6-c6bd07df1a3c
40 Consumer surplus is the notion that some consumers will pay less than the price they would be prepared to pay because the market sets just one prevailing price that attracts the marginal consumer. Dynamic pricing can, in theory, charge each consumer exactly the maximum they are prepared to pay, which will differ from one consumer to the next. Dynamic pricing algorithms rely upon unprecedented access to data about consumer behaviour, right down to the preferences of individuals expressed through their social media accounts, with the result that by using this data, economic value moves away from consumers and to producers. In one sense, it is a passive loss of value to consumers as it consists of price differentials they were willing to pay, but it also represents a real shift in significant market power, and regulators are usually charged with protecting consumer interests.
regulator, a mindset shift becomes the fundamental requirement, moving from risk-manager to development enabler. Such developments need to occur at each layer:

- Develop policies towards a digital economy based upon Open Government data sharing and Big Data analytics, including establishing data protection regulations and then ensuring that such regulations are kept updated and relevant, particularly as they cut across ever more sectors and services.
- Ensure that critically important networks, such as telecoms and banking systems, interconnect, and that platforms become interoperable so that apps and services work across all systems, and are accessible by all, as much as possible at any time.
- Develop smart security policies – in this case, cybersecurity policies – to protect critical national information infrastructures (CNII), and promote rapid information sharing, including transnationally, about cyber-attacks.
- Create cross-agency (whole-of-government) frameworks (and agencies) for effective policies and regulations so as to enable the development and delivery of government and social services, and to incentivise innovation and investment, while at the same time protecting consumer interests.

In Chapter 5, ways to implement these policies are recommended, but from any of these developments to occur, policies need to reinforce the development of digital awareness, skills, knowledge and training, especially among government staff to manage the growth of the digital economy. These points are developed and further illustrated in Chapter 2.
CHAPTER 2: Regulatory and Policy Challenges

Existing policy tools and governance frameworks have been outdated by the rapid emergence of the digital economy leaving policy makers and regulators constantly challenged in an ‘arms race of applied knowledge’ to try and stay up to date with the pace of change. This chapter outlines and considers the disruptive digital challenges confronting policy makers – such as privacy, security, surveillance, sovereignty, data protection, and cross-border data flows. Examples of each of these are provided in Chapter 4 with respect to Malaysia, Thailand and Vietnam to illustrate the impact of emerging technologies on regulatory and policy frameworks in particular country contexts.

This chapter first considers the need for, and approaches towards, investment in a national broadband infrastructure. The attention then turns to policy and regulatory challenges, notably the networking benefits that accrue to a digital economy from either encouraging or regulating networks to become inter-operable, and the applications that arise from that, such as sharing-economy apps that work across different mobile network platforms. The data generated by these networks and apps is becoming the currency of the digital economy, and that raises new challenges for data privacy, data security and data sovereignty, which are the subject of the final part of the chapter.

Creating a National Broadband Network

Creating a national high-speed broadband infrastructure is a major financial and regulatory challenge for most developing countries, even though the necessity for an accessible and reliable broadband network is acknowledged. In the Asia-Pacific there are now several alternative models to consider. In the Australian and Malaysian models, governments have combined a state subsidy with a broadband network contract to the dominant national telecommunication carrier, with target penetration rates to be met. Singapore has taken a different route by separating the underlying broadband network of dark fibre (NetCo) which received a state subsidy, from the wholesale business (OpCo), from the retail business which is a competitive market. Competing operators can still invest in their own networks if they choose to do so. In Thailand, the government is proposing a national holding company to build and operate the country’s national fibre assets on a wholesale basis, a policy that risks reducing competition and slowing down broadband infrastructure roll-out.

---

41 Financial Times (31 July 2017), Competition authorities need a digital upgrade, https://www.ft.com/content/f6fe0f18-73d1-11e7-aca6-c6bd07df1a3c
42 In Malaysia, utilities are licensed to lease out their dark fibre, and in many countries private corporations can do likewise.
The contribution of ICTs to GDP in Malaysia, Thailand and Vietnam is around 13%, 6% and 6% respectively. This is one indicator of the level of growth of the digital economy, and although it is not a measure of how ICTs are used or who has access to them, nevertheless the ITU’s fixed broadband penetration rates track them quite closely: Malaysia (10%), Thailand (8.5%) and Vietnam (6.5%).

More telling, however, are the penetration rates of broadband mobile: Malaysia (58%), Thailand (80%) and Vietnam (31%). Because Thailand was less developed in fixed lines, mobile substitution rates galloped ahead. As is true in most Asian countries, broadband mobile is now the primary means of access to the Internet, although for large enterprise usage, such as banks, fixed broadband remains essential.46

Asian economies can be typically grouped into three 'clusters’ of wealth and development: low income economies, lower-middle income emerging economies, and upper-middle income economies.47 In most cases network access parallels such income clusters quite closely. Malaysia is an upper-middle income country, wherein the majority of the population can access the Internet, similar in this regard to Brunei. Thailand, while in a similar national income bracket, has more limited accessibility and in this regard, can be grouped together with Vietnam (which belongs to the lower-middle income class) and the Philippines. The third cluster of countries – such as Indonesia, Myanmar, Laos and Cambodia – is characterized by low-income and low access. The obvious outlier within ASEAN is Singapore, which acts as a benchmark for the digital future, notably in three ways: (i) the degree of interconnectedness of the economy and society, (ii) the coordination and consistency of policy and regulation across government agencies, with leadership and coordination coming directly from the Prime Minister’s Office indicating the priority assigned to the digital economy, and (iii) the promotion and clear articulation of a ‘Smart Nation’ set of objectives, combining new digital technologies with policy adjustments and flexible regulations, that in turn promote innovation in business models. But if connectivity and digitalization raise the prospect of accelerating economic growth, and of potentially leapfrogging development stages, then how these approaches are next mapped out, integrated and deployed becomes strategically extremely important. This is explored further in Chapter 4 which looks at the digital infrastructure policies of Malaysia, Thailand and Vietnam.

46 Broadband is also essential to backhaul wireless traffic and for national long-distance transmissions.
**Interoperability of Platforms**

The challenge for policy makers beyond financing the communications infrastructure, is to promote the interoperability of network platforms so apps and services can be shared across them. Policy makers and regulators will need to make decisions about when it is in the public interest to require the interoperability of platforms, and which apps must be allowed through. For example, interoperability among mobile money services can drive adoption and financial inclusion as the number of transactions increase if consumers can transfer money using an application run by a telecom service provider to a customer of a competing telecom service provider, or a customer using a commercial bank. Mandating interoperability, however, runs the risk of discouraging investment from players and may limit the growth of nascent business models.⁴⁸ As with interconnection, there are always two stages with interoperability:

1. Determine when to require it of the platforms. Governments can engage industry players to examine market conditions and maturity levels in order to understand both the benefits and risks associated with mandating interoperability.

2. Determine when to permit blocking, for example of child pornography or hate speech, or throttling of particular types of traffic for the purposes of network management.⁴⁹ Such decisions should be made about censorship and net neutrality issues, keeping in mind the benefits of free flow of data for the development of the digital economy.

**The Sharing Economy**

An oft-quoted observation about the sharing economy sheds light on its transformative impact on the economy: “Uber, the world’s largest taxi company, owns no vehicles. Facebook, the world’s most popular media owner, creates no content. Alibaba, the most valuable retailer, has no inventory. And Airbnb, the world’s largest accommodation provider, owns no real estate.”⁵⁰

The sharing economy is an economic model based on the borrowing or renting of assets owned by someone else, but not fully utilised all the time (Figure 2, left side). The rise of the sharing economy is taking advantage of the shift from client-server to peer-to-peer (P2P) Internet architectures – good examples are P2P ride-sharing apps such as Grab and Uber, or accommodation sharing sites such as Airbnb and Couchsurfing (although the emerging opportunities go well beyond these examples, see Figure 2, right side). Challenges posed by the sharing economy are largely on (1) the conflict

---

⁴⁸ GSMA (2016), Advancing Digital Societies in Asia, https://www.gsmaintelligence.com/research/?file=9f48d32ff0671fb7dbcb4efb84eabc0&download, p. 59
⁴⁹ WB Broadband Handbook
⁵⁰ TechCrunch (3 March 2015), The Battle is for the Customer Interface, https://techcrunch.com/2015/03/03/in-the-age-of-disintermediation-the-battle-is-all-for-the-customer-interface/
between traditional industries and newly emerging platforms, (2) the reliability of reputation ratings in the shared economy, and (3) consumer protection issues – such as data protection, including the selling of user data by platforms, liability and insurance.

Figure 2: The Sharing Economy

In the case of ride-sharing apps, policy makers are under pressure from traditional transport companies to protect them against these more flexible services, while regulators are under pressure to ensure that laws are not being broken. In Singapore, new laws are clarifying the conditions required for these services to operate, including minimum periods of driving experience, the vetting of drivers and appropriate insurance. The result is a traditional taxi service augmented, but not replaced, by a thriving ride-sharing service, with many drivers using multiple apps and traditional taxi companies changing business and pricing models to compete effectively. The flexibility shown in Singapore seems to be working, and illustrates the need for consultation and flexibility, but also for timely policy adjustments.

Privacy and Data Protection

Data is, as the saying goes, the currency of the digital economy. In a digital economy, economic value shifts increasingly to data, as discussed in Chapter 1. There are several steps involved: (1) collecting data and conforming to the regulations governing that collection, (2) storing and then processing the data, abiding by restrictions that may apply to non-identification of individuals within any given sample of data, and (3) using the data in ways that conform to the conditions of its collection. Step 1 involves two types of data protection, (1a) the protection of personal privacy, and (1b) the security of the data collected.

Personal Data Privacy

Personal data privacy laws have been passed in many countries, the most common element being the need to seek the permission of citizens before data about them can be collected. The purpose of the collection must be specified, usually with a commitment to destroy the data once it has been used – unless the use is ongoing, such as a credit card number for e-commerce, or a social security number for frequent claims. Data may still be used if seeking permission is not feasible but is judged to be in the best interests of the individual, such as medical data when a person is incapacitated. Malaysia has such a law and a Personal Data Privacy Commission to enforce it, but there is no such legislation in Thailand or in Vietnam.

Data Protection

Data protection (Step 1b) refers to the security of the data and the potential loss or misuse of data, often involving cybercrime. Step 2 is about processing the data, and often this is outsourced by the data controller to a third-party. Privacy laws typically hold the data controller liable for any breaches that may occur, but if this data is stored and processed overseas it may be difficult to monitor or enforce the law. The issue of ‘localisation’ is examined below. An associated problem of data processing is intended or unintended identification of individuals. Much of the data being harvested today comes not from individuals giving their consent on websites or in written documents, but from a myriad of sources, including social media, locational data associated with the use of smartphones, and online browsing. Despite data controllers needing to anonymise data, the reality is that using Big Data sources, algorithms can, if they are so programmed, identify individuals by multiple triangulations of information. However, if national security agencies are the most likely to use such methods, they are typically exempt from personal data privacy laws. In some cases, for example Malaysia and Singapore, all government agencies are exempt, while in Hong Kong the law includes government agencies and generally precludes them from sharing personal information between agencies.

Step 3 is about data usage and this is where the impact of Big Data analytics is proving a game-changer, and a challenge to regulatory thinking. Dynamic pricing algorithms are being developed which can all but “eliminate the very notion of market prices, and with it the consumer surplus.”52 By charging different prices to different consumers, consumers willing to pay more do pay more, and

---

52 Financial Times (31 July 2017), Competition authorities need a digital upgrade, https://www.ft.com/content/f6fe0f18-73d1-11e7-aca6-c6bd07df1a3c
economic value shifts from consumers to vendors. In one sense, it is a passive loss of value to consumers as it consists of price differentials they were willing to pay, but it also represents a real shift in significant market power, and regulators are usually charged with protecting consumer interests.

**Cybersecurity**

It must be recognized up front that interoperability can be something of a gift to cyber-criminals, and this poses inevitable and important problems for regulators – now and moving forward. Cybersecurity has already grown from a nuisance to a direct threat to critical national information infrastructure, and it is an issue which will continue, and will continue to evolve as the networks and platforms continue to evolve, both in their architecture and their usage. If everything is connected it is not difficult to install malware, ransomware, spyware and other malicious code which can rapidly spread, exactly like a virus.

Further, much of the data generated in an Internet-of-Things (IoT) environment will relate to private citizens and their usage of devices, websites, medical facilities, video, etc. The traditional approach to personal privacy protection is to require data collectors to obtain consent, but this becomes impractical in a world saturated with IoTs, and where the usefulness of data is often not so much in its raw collected form, but in its collated and analysed result – tracing such use back to the original consent rapidly becomes impractical. But there are important opportunities as well. Arrangements to have commercial organisations, such as public utilities, share data, and for government agencies to make data available for commercial developers and other members of the public, can incentivise apps developers to produce socially useful and sometimes economically profitable services. Such a policy was advocated by U.S. President Obama in 2009 as the Open Government Initiative, and has been championed by the World Bank.

Storing and making use of that data requires more and more sophisticated IT systems, cybersecurity notwithstanding. Decisions need to be made whether to store it in a database in-house, or to use a cloud computing system (be that a private cloud, public cloud or a hybrid system). However, making these decisions is probably less of a challenge than recruiting staff with the requisite IT skills to manage them, especially if the public sector cannot compete on salaries with the private sector, and if there is a national shortage of persons with those IT skills.

---

53 The White House (2009), Open Government Initiative, [https://obamawhitehouse.archives.gov/open](https://obamawhitehouse.archives.gov/open)
Sovereignty and Cross-border Data Flows

Data can be stored anywhere on the planet. It does not need to be stored locally even if the data is generated and collected locally. The exponential growth in international broadband submarine capacity – by 2016 there were 30 high-capacity submarine cables with an estimated designed capacity of over 380 Terabytes serving ASEAN countries, with more cables planned – means data transfers are fast and low cost, and the value associated with these data flows – such as orders and payments for goods, remittances, streamed media sales – increasingly underpins world trade. If policy makers can promote such value-chain development, and regulators can enable participation – for example, many central banks are now studying whether and how best to encourage the use of cloud computing for the FinTech sector and to permit the data to be stored outside the country – the impact on GDP can be significant: 0.5% in the case of Malaysia, 1.5% in Thailand and 6.6% in Vietnam, according to World Bank estimates for 2016.

Sovereignty Issues

The challenges arise due to extra-jurisdictional issues, such as domestic earnings that flow overseas and may be by-passing local taxation authorities. One response to this trend has been an insistence in some countries that data generated locally should be stored locally (‘data localisation’ or ‘data residency’) and made available for either tax assessment or security reasons – or both. China and Vietnam require the localisation of data, as does Indonesia, of ISPs serving the local market directly. Indonesia’s tax department has plans to require a permanent local presence (regulation no. SE-04/PJ/2017) to ensure taxation can be levied. Localisation is usually not welcomed by foreign companies because it adds significantly to the cost of doing business in a country that has only a small market. Also, a purely nationalistic response, if the consequences are discriminatory, will also be a challenge to the norms of world trade. At the same time, developing countries need efficient, effective and equitable ways to raise revenues from taxes, customs and excise duties. If regional assemblies of governments could harmonise approaches to the levy and collection of taxes, possibly as aspects of trade agreements, this would be a huge step towards avoiding beggar-thy-neighbour policies.

**Cross-Border Data Transfer Issues**

It is the norm to place restrictions on the overseas transfer of personal data under personal data privacy laws (see above), such as sensitive financial data held by banks or medical data. And when the data is transferred overseas, there remains a question of how to monitor its use and how to enforce domestic laws on overseas data controllers. Each country has its own legislation and regulations governing the transfer and use of data. In some countries, an enterprise needs to appoint and register a data controller who may be held legally personally responsible for any data breach; in others, enterprises must be licensed for each category of data they are handling. These variations in laws add to the costs and complexities of doing business, and should be reviewed with cross-border harmonisation in mind.58

Closely-related security issues include applying Anti-Money Laundering/Counter-Financing of Terrorism (AML/CFT) regulations, detecting cybercrimes and anti-terrorist surveillance (see above). This raises an important issue; given that the UN adopted a Convention against Transnational Organized Crime (UNTOC) in 2000, to address ways to overcome the hurdles of jurisdictional differences, it should be possible for regional associations of countries, such as ASEAN, APEC and SAARC to work more closely together, alongside international agencies such as Interpol – and its Asian regional equivalent ASEANPOL – and the International Multilateral Partnership Against Cyber Threats (IMPACT). The Mutual Legal Assistance Treaty (MLAT) exists between some countries, but it is not universal and is in need of a revamp to meet the demands of the digital economy era. Cybercrime and cyber-criminals and terrorists recognise no boundaries and the Internet’s digital technologies, notably through social media and the use of end-to-end encryption, are making it a game of catch-up for regulators.

The answers to meeting all the challenges listed above inevitably vary from country to country, as each frame their approach according to the socio-economic and political economy conditions that prevail domestically. Chapter 3 looks at these alternative ways of framing policies towards the digital economy.

CHAPTER 3: Driving Digital Opportunity: Enabling Transformation and Seeding Capacity

Approaches to Digital Development

Every government works within the context of its legacy institutions, policy making processes and its socio-economic conditions. Accordingly, the approaches towards creating a policy framework for the digital economy vary quite significantly even among countries with similar levels of economic development and access to innovative technologies. Some of the different approaches adopted, and how they may impact upon the digital economy, are illustrated below with three brief case studies: (1) Government vs. private sector leadership in the European Union (EU) and the United States (US); (2) Top-down vs bottom-up approaches in Singapore and Hong Kong; and (3) Innovation vs regulation in China and Japan.

Government-led EU vs Private Sector led US

The European Union and the United States take different approaches to who is driving policy and regulatory change for the digital economy. The European Commission (EC) of the EU is not merely a regional coordinating body, but often the lead advocate in regulating emerging digital technologies, with Brussels adopting a government and regulatory-led approach to digital development. This can be seen, for example, in the areas of privacy, data protection, net neutrality and regulating the search engine market. The EU takes the position that regulating the digital economy needs to happen through frameworks set and developed by national governments. The EU’s Data Protection Directive established common rules for creating a high standard of protection for European citizen’s personal data both at home and when transferred across borders – these protections will be further enhanced when the General Data Protection Regulation (GDPR) comes into force in 2018.⁵⁹ To control the data handling practices of the large US technology vendors in particular, the EU-US Privacy Shield was negotiated following a successful legal challenge to the previous Safe Harbour Agreement,⁶⁰ which illustrates the importance of decisions by the European Court of Justice in shaping the global discourse on privacy and data protection regulations.

---


By contrast, in the United States it is the private sector which leads much of the digital regulatory agenda, with the government seeking to create an enabling environment for private sector initiatives. For example, the majority of sharing economy apps were first launched and allowed to flourish in the US, including Uber, Lyft, Airbnb, and TaskRabbit, and the app-based companies and regulators work together to balance innovation with the public interest. In the case of data privacy regulation, and in contrast to the European approach that places more direct emphasis upon compliance and the risk of penalties, in 2016 the US Department of Justice took Apple to court to gain backdoor access to the iPhone of a suspected terrorist, which the company refused to grant in order to protect users’ data, security and privacy.

Whether the American approach to digital technology policy tends to be more enabling and nimble, responding to signals from the market, with policy and regulation being tools to foster or enable innovation and market growth (as opposed to stability), or whether this is due to the clustering effects of locations such as Silicon Valley, is open to argument. What is clear is that the dynamic of the US market is unmatched elsewhere. This further results in the regulatory interests of American technology companies being advocated by the same the mechanisms the US has traditionally used to further its business and trade agendas, namely American chambers of commerce, business associations and the US Commercial Service.

Top-down Singapore vs Bottom-up Hong Kong

Singapore and Hong Kong offer a somewhat similar case study of contrasts in digital development, except in this case the difference is much more on how digital initiatives are implemented and deployed, rather than on the framing. Once again, both approaches can be seen to have their benefits. Singapore, for example, was globally the first country to allow driverless cars on its streets. With urban transportation congestion becoming a major issue the world over, the Ministry of Transport set up the Committee on Autonomous Road Transport for Singapore (CARTS) in 2014 to create a strategy for launching autonomous vehicles (AVs) in the city state. With the guiding support of the Prime Minister’s Office and the head of Singapore’s civil service, the country’s R&D umbrella agency, A*STAR, and the Land Transportation Authority (LTA) launched the Singapore Autonomous

---

62 “Apple believes deeply that people in the United States and around the world deserve data protection, security and privacy. Sacrificing one for the other only puts people and countries at greater risk.” https://techcrunch.com/2016/03/28/justice-department-drops-lawsuit-against-apple-over-iphone-unlocking-case/
Vehicle Initiative (SAVI) to explore the technological possibilities that AVs can create for Singapore. The initiative has been one of Singapore's 'big bets' in digital transformation, with enabling AV as part of the broader government strategy for establishing alternative transportation to deal with the limitations of a growing population and scarce supplies of land for development. Accordingly, SAVI has been implemented in a top-down fashion by forward-looking government agencies that are coordinated at the very top of the political chain to serve long-term policy goals. Hence, being first 'out onto the streets' was an important benchmark and validation for the government.

By comparison, Hong Kong's digital economy develops in a bottom-up manner with a variety of initiatives from diverse stakeholders such as technologists, academics, and companies emerging competitively, both as experiments and responses to perceived market demand. In contrast to Singapore, for example, the use of the existing infrastructure such as lamp posts to which to attach sensors and WiFi and other communications equipment for AV and IoTs, is stalled owing to concerns by the relevant bureau that power supplies from other utilities might disrupt operations and add to costs. Such inter-agency issues stand in stark contrast to the unified approach of the Singapore government. But the Hong Kong approach does have the advantage of encouraging independent initiatives. An early but indicative example is that of the Hong Kong Internet Exchange (HKIX), the first Internet Exchange Point in Asia, established in 1995 on the campus of the Chinese University of Hong Kong. HKIX enables autonomous systems to interconnect with one another and exchange traffic. By the summer of 2017, the IXP was interconnecting 277 participants, including over-the-top service providers (OTTs), telecom service providers, universities and cloud service providers; and has up to 780 Gbps per minute total traffic. HKIX not only helps to keep intra-Asian Internet traffic within Asia, but has also enabled Hong Kong to become one of the most important Internet hubs in Asia by attracting all major technology and content providers. Hong Kong is a gateway for international data centres, with easy access China, and providing a useful communications and financial hub for Chinese tech companies wanting to expand overseas. The government is keen on such investors, and encourages the industry by providing access to land for over 50 operational data centres – the industry's projected revenue by 2020 is USD 1.39 billion. Hong Kong has remained an outlier in international connectivity over recent years, with the Asia Cloud Computing Association (ACCA) noting a 90% year-on-year growth and more than five times the capacity of second-ranked

---

65 Kenneth Chan (5 July 2017), HKIX Updates at JPIX User Meeting, [https://www.hkix.net/hkix/Presentation/JPIX_2017.pdf](https://www.hkix.net/hkix/Presentation/JPIX_2017.pdf)
Singapore in its annual Cloud Readiness Index rankings. According to the ACCA, Hong Kong ranked first among Asian economies on international connectivity and datacentre risk, and second on broadband quality, power grid, green policy and sustainability, and privacy. Just as Singapore is a gateway to South East Asia, Hong Kong has long been a gateway to mainland China and a major transit point for all Asian traffic to and from the US.

**Innovative China vs Regulated Japan**

With the private sector requiring both regulatory certainty (to underwrite investment) and regulatory freedom (to foster innovation), the relentless pace of technological change is challenging policy makers and increasing uncertainty about which regulatory approach works best in the fast-changing digital economy landscape: clearer guidelines that protect privacy, investments, IP, and so on, or a more laissez-faire regulatory environment that sponsors the fastest, strongest, most innovative, most efficient. As in the cases above, China and Japan present interestingly different attitudes and approaches to how government and the private sector can work together to enable, empower or oversee and manage the pace of innovation.

In China, innovation in the digital payments industry has flourished like perhaps nowhere else in the world as key public and private sector actors rapidly and exponentially grow digital payment ecosystems that increasingly are able to touch on all aspects of life by combing a variety of digital technologies, ubiquitous mobile connectivity, and advanced data analytics, by leveraging all existing e-commerce and social network platforms. Digital payments have grown rapidly from about 3.5% of all retail transactions in China in 2010, to a conservatively estimated 17% in 2015. Combined, the value of payments transacted via Alibaba’s Alipay and Tencent’s WeChat, have risen from less than USD 81 billion in 2012 to an estimated USD 2.9 trillion in 2016 – a 20-fold increase in four years. The growth of the digital payment ecosystem was enabled by the government’s “wait and see” approach to regulation which allows for innovation by industry participants within informal limits, under careful supervision by the relevant regulators, creating new business opportunities and increasing financial inclusion. From an international business perspective, this threatens a high degree of regulatory uncertainty, but for Chinese capital it is a well-understood environment.

---


Chinese Digital Payments Industry

China has essentially replaced cash with smartphone-based digital payments apps in the retail ecosystem between 2014 and 2017. Richard Lim, Managing Director of venture capital firm GSR ventures said: “From a tech standpoint, this is probably one of the single most important innovations that has happened first in China, and at the moment it’s only in China.” In 2016, China’s mobile payments hit USD 5.5 trillion, roughly 50 times the size of the USD 112 billion market in the United States. The number of total global transactions per day via WeChat and Alipay is expected to surpass Visa and MasterCard in 2018. As China’s online payments infrastructure is centred around these private smartphone-based payments network, companies involved in trade with China will need to create separate structures to link them with the international payments system currently dominated by credit cards.

By contrast, Japan has a more risk-averse and regulation-centric approach to managing technological change coupled with strong government involvement and a top-down approach. This has resulted in a curious mix of coexisting legacy technology and advanced high-tech solutions, while Japan has been through a so-called ‘lost decade’ of competitiveness. On the one hand, Japan is aspiring to be the “the world’s most advanced IT nation” with long-term strategic plans in place, and well-earned leadership in network performance and spectrum allocation for mobile services. On the other hand, certain core issues remain unresolved such as the interoperability of cloud services with legacy technology, and the international accessibility of Japanese payment platforms.

The failure of digital payments to take off in Japan can be attributed to this risk-averse regulatory approach by the government coupled with Japan being an early adopter of advanced technology almost two decades ago. In the early 2000s, Japanese flip phones could already be used to pay at stores and offered mobile wallet services, but ironically, their advanced functionality resulted in Japan becoming a technology laggard when it came to interoperable smartphone adoption, and without a broader ecosystem driving payments usage, digital payments have been slow to take off.

---

72 GSMA (2016), Advancing Digital Societies in Asia, https://www.gsmaintelligence.com/research/?file=9f48d32ff0671fb7dbcb4efb84eabc0&download, p. 65
73 Also called “Galapagos phones”, these models are still widely used in Japan.
The Japan times (18 May 2015), Japan’s ‘Galapagos phones’ making a comeback, http://www.japantimes.co.jp/news/2015/05/18/business/japans-galapagos-phones-making-comeback/#.WYbr0yfGM2w
Cash use still dominates, and security concerns about digital payments have held adoption back – only 19% of payments are cashless (including credit cards). The government is offering subsidies for the purchase of cashless payment facilities by businesses, including terminals for credit cards and other smart cards, to ease foreign tourists’ use of card-based payments during the 2020 Tokyo Olympics. A more forward-looking, but still painfully slow step compared to China, is that by 2020, roughly 60% of Japanese banks will allow developers into their systems to access users’ account information through open APIs (Application Programming Interfaces).

Other Digital Transformation Strategies that Provide Global Benchmarks

Beyond the trade-offs highlighted above, different approaches to digital economy planning and deployment have created some widely known initiatives which show the transformation of digital disruption into a powerful contributor to economic and social development in the form of better public services delivery, faster economic growth, increased financial inclusion, and so on. It is worth briefly highlighting some of these global examples before examining in Chapter 4 the way in which select Southeast Asian states are beginning their own transformation journeys.

---


75 Nikkei Asian Review (1 June 2017), Japan looks to double cashless payments in 10 years, https://asia.nikkei.com/Politics-Economy_Policy-Politics/Japan-looks-to-double-cashless-payments-in-10-years
**Box 1: Estonia: A Digital Society for Digital Citizens**

Having faced severe cyberwarfare in 2007 and fearing such attacks might happen again,\(^76\) Estonia decided to “put the country into the cloud”, to enable public administration to continue operating in the event of a subsequent attack, by utilizing digital infrastructure beyond the geographical boundaries of the country. This mentality fuels Estonia’s “Government as a Service” programmes and digital public services provision. Electronic identities (e-IDs) enable citizens to access 99% of state services online, such as paying bills, filing taxes and accessing medical records, which has created significant time and cost savings by eliminating the need for paperwork and physical travel.\(^77\) The ubiquitous use of e-signatures is estimated to save the Estonian economy approximately 2% of GDP each year.\(^78\) Somewhat uniquely, the country has opened its digital infrastructure to foreigners through its e-residency programme, which allows them to apply for the same e-ID cards, and access to e-services, such as seamless business registration where SMEs can enjoy 0% corporate tax when they reinvest corporate profits back into the company.\(^79\)

---

**Box 2: India: A Digital Identity Platform to Build On**

Aadhaar, India's biometric digital identity scheme,\(^80\) has enrolled 1.16 billion people between 2010 and August 2017.\(^81\) The Indian government considers Aadhaar as one of the key initiatives under the Digital India programme and a "strategic policy tool for social and financial inclusion, public sector delivery reforms, managing fiscal budgets, increasing convenience and promoting hassle-free people-centric governance."\(^82\) The Aadhaar authentication platform is widely used by the private sector, as well, including verification firms in business services, banks, and telecommunications companies – mobile operators were ordered to re-verify their subscribers with Aadhaar-based eKYC by March 2018.\(^83\) Aadhaar also provides authentication for the Unified Payments Interface (UPI), created by the National Payment Corporation of India. The single interface platform is used by digital payments applications, which have rapidly sprung up since November 2016 built by technology companies such as WhatsApp, banks, and the government itself.\(^85\)

---


\(^80\) Aadhaar number is a 12-digit random number issued by the Unique Identification Authority of India (UIDAI) to the residents of India irrespective of age and gender. Residents can enrol voluntarily and need to provide minimal demographic and biometric information during the enrolment process which is totally free of cost. [https://uidai.gov.in/about-aadhaar.html](https://uidai.gov.in/about-aadhaar.html)

\(^81\) Unique Identification Authority of India, Aadhaar Dashboard, [https://uidai.gov.in/aadhaar_dashboard/](https://uidai.gov.in/aadhaar_dashboard/)

\(^82\) Digital India, [http://digitalindia.gov.in/di-initiatives](http://digitalindia.gov.in/di-initiatives)
Box 3: Kenya: Financial Inclusion via Mobile Phones

Kenya’s M-Pesa is one of the early success stories in mobile money services launched in 2007 by telco Safaricom. The money transfer service relied on cheap mobile phones and an extensive agent network, and transformed bill payments (including airtime top-ups) and person-to-person (P2P) domestic remittances. According to the GSMA, these transaction types accounted globally for 96% of the volume and 87% of the value in 2015 in the case of M-Pesa-like providers.\(^\text{86}\) M-Pesa’s two core innovations have been proximity and simplicity made possible by large agent networks and simplified account opening processes. Customers have massively embraced the ability to access financial services close to home without complex administrative barriers, which have significantly increased financial inclusion. At the most basic level, low-cost communications platforms have enabled this, aided by a network of dispersed nodes for instant transactions.\(^\text{87}\)

Nonetheless, despite these innovations, the M-Pesa model does not necessarily offer clear-cut solutions other countries can directly copy. There have been several cases where governments or private sector stakeholders failed to replicate the success of these platforms, services and products when they launched them in different regulatory regimes and socio-economic settings. For example, M-Pesa, which has been highly successful in promoting mobile banking in East Africa, but failed in South Africa where a much higher percentage of the population already have bank accounts, and the perception of the service was more focused upon the financially-more secure middle class.\(^\text{88}\) In a different context, an attempt to introduce a national ID scheme in 2010 had to scrapped in the UK due to public antipathy, the lack of trust and privacy concerns by the public.\(^\text{89}\) Governments and the private sector need to understand the context in which they build a digital economy, and they build their own solutions based on well-defined policy choices and many of the building blocks defined in this paper.

\(^{83}\) Scroll.in (22 Dec 2016), How private companies are using Aadhaar to try to deliver better services (but there’s a catch), https://scroll.in/article/823274/how-private-companies-are-using-aadhaar-to-deliver-better-services-but-theres-a-catch
\(^{84}\) The Indian Express (27 Mar 2017), Aadhaar eKYC mandatory for mobile connections: Here’s how it applies to you, http://indianexpress.com/article/technology/tech-news-technology/aadhaar-ekyc-for-mobile-phone-connections-heres-what-you-need-to-know/
\(^{87}\) CGAP (20 July 2016), The Replication Limits of M-Pesa in Latin America, http://www.cgap.org/blog/replication-limits-m-pesa-latin-america
CHAPTER 4: Digital Economy Planning in Asia: Malaysia, Thailand and Vietnam

This chapter reviews how the governments of Malaysia, Thailand and Vietnam are aligning their existing strategies to enable the digital economy, and the frameworks they have developed and implemented as a part of their national digital agendas. Essential to any digital agenda is a broadband infrastructure. From Table 2 it is evident that despite its higher GDP per capita, Malaysia does only slightly better than Thailand in terms of fixed broadband infrastructure, but suffers from proportionately higher prices, and trails Thailand in terms of broadband mobile. Vietnam lags the others, with relatively high fixed broadband prices, but does better in broadband mobile. Internet speeds, as measured here by data from Netflix, show little difference between Malaysia and Thailand. At the time of writing, Netflix is not available in Vietnam.

Table 2: Broadband Infrastructure

<table>
<thead>
<tr>
<th>Broadband contexts</th>
<th>Malaysia</th>
<th>Thailand</th>
<th>Vietnam</th>
</tr>
</thead>
<tbody>
<tr>
<td>GDP per capita</td>
<td>$9.5k</td>
<td>$5.9k</td>
<td>$2.2k</td>
</tr>
<tr>
<td>Broadband penetration</td>
<td>Fixed (%)</td>
<td>10%</td>
<td>8.5%</td>
</tr>
<tr>
<td></td>
<td>Mobile (%)</td>
<td>58%</td>
<td>80%</td>
</tr>
<tr>
<td>Cost</td>
<td>Fixed broadband prices (% GDP / capita)</td>
<td>3.2%</td>
<td>0.3%</td>
</tr>
<tr>
<td>Speeds</td>
<td>Netflix ISP Speed Index (Avg. Mbps, July 2017)</td>
<td>3.5</td>
<td>3.4</td>
</tr>
</tbody>
</table>


Malaysia

Malaysia is a market economy in which the state plays an active role in shaping economic development, with growth targets outlined in a series of Five Year Plans (FYPs). The 11th FYP (2016-2020) aims to raise the contribution of ICTs from 13% to 18.2% of GDP as a key component of the
country’s target to escape a middle-income trap.\textsuperscript{90} Developing the country’s technology capacity has been at the forefront of a series of national initiatives over the years, such as the Multimedia Super Corridor (MSC) designed to attract multinational investment and domestic flagship projects. Spearheading the drive towards a Digital Malaysia is the Malaysia Digital Economy Corporation (MDEC)\textsuperscript{91} which has identified five key sectors for digital development: ICT services, E-commerce, ICT manufacturing, ICT Trade, Content and Media.\textsuperscript{92} MDEC was also instrumental in supporting the establishment of a Digital Free Trade Zone (DFTZ) which, like the MSC, offers incentives to investors, particularly across the areas of e-commerce.

Holding Malaysia back has been the lack of accessible and affordable fixed broadband at the national level (with Malaysia recently slipping behind Thailand on affordable access per capita, and even behind Vietnam on same indices – see Diagram 1). To head this problem off, the Malaysian Communications and Multimedia Commission (MCMC) had given one-third subsidy to state-invested Telecom Malaysia (TM) to bring High Speed Broadband in two consecutive programmes (HSBB 1 and HSBB 2) with support from Khazanah Nasional Berhad, the strategic investment fund of the Government of Malaysia.\textsuperscript{93} As the monopoly fixed line carrier, TM owns around 90% of the national network of copper wires, fibre and ducts. Although retail prices are regulated, TM has been able to recoup its investments through high wholesale charges with what is known in the industry as a ‘profit squeeze’. Competition at the retail level holds down end-user prices, making it difficult for new facilities competitors to enter the market. As a result, competition has only been effective in the broadband mobile market.

\textsuperscript{91} Previously the Malaysia Multimedia Development Corporation (MDEC), the agency was renamed in 2016.
Nevertheless, Malaysia has been striving to become a regional hub for telecoms traffic and related data centre development, but high cable landing fees, interconnection fees and backhaul fees deter international submarine service providers from routing their traffic from the Pacific to the Indian oceans through Malaysia, preferring the lower prices and higher capacity available in Singapore. This has further consolidated TM’s stranglehold on the infrastructure market, leading to something of a vicious, rather than virtuous, cycle of investment and development. Many questions have thus begun to be raised about the sustainability and advantages of the state-funded HSBB approach, with Prime Minister’s office more recently soliciting proposal for a more aggressive ‘fiberization’ programme for the country. 

Digital Planning in Malaysia

Malaysia’s goal is to become a high-income country, with ICT contributing 18.2% of GDP by 2020. The country has a host of cross-cutting initiatives with digital components to achieve these targets.

E-commerce: There are more than 40 e-Commerce related initiatives and programs by more than 20 government agencies in Malaysia. The National e-Commerce Strategic Roadmap, under the supervision of the National eCommerce Council (NeCC), aims to double e-commerce growth in the country from the projected 10.8% to 20.8% between 2015 and 2020, and positioning Malaysia as

---

95 11th Malaysia Plan (2016-2020)
the leading hub for e-commerce in the ASEAN region. To promote this strategy the concept of Digital Free Trade Zones (DFTZs) has been developed to facilitate e-commerce including an e-fulfilment hub at KLIA with partners such as Alibaba’s Cainiao, Lazada and Pos Malaysia; and an Electronic World Trade Platform is to facilitate cross-border payments targeting SMEs. The challenge for Malaysia is to be able to attract foreign as well as domestic e-commerce and logistics companies to invest and locate in these zones. DFTZs have also been conceptualized in China, but in China’s case the size of the domestic market alone can be a great advantage to the future success DFTZs. In smaller Southeast-Asian markets, additional measures may be necessary to ensure success, ranging from investment and taxation incentives to fast-tracked business proceedings and regulatory certainty.98

**Public service delivery:** The Malaysian Administrative Modernization and Management Planning Unit (MAMPU) was established under the Prime Minister’s Office to transform public service delivery through accelerating the adoption of ICT by 2020. MAMPU’s key goals on digital, data, cloud and cyber security are outlined in the Public-Sector ICT Strategic Plan (2016-2020). The Plan proposes that certain government services will be offered only digitally, and citizens will get IDs to access online services. The government also intends to allow online payments, with 19 agencies to offer mobile payments by 2020. MAMPU will look to encourage broader use of data in government, with analytics used to improve digital delivery. It will build the Consolidated Secured Government Cloud Platform for agencies to consolidate and share data with each other.

While Malaysia has several initiatives to drive digital economic growth, the country lacks a coherent digital agenda as government agencies like the Malaysian Investment Development Authority (MIDA), the Malaysian Communications and Multimedia Commission (MCMC), the Malaysian Digital Economy Corporation (MDEC) and the Ministry of Science, Technology and Innovation (MOSTI) have at times seemed to be at odds with one another. For example, the MCMC and MDEC both hold positions under the Ministry of Communications and Multimedia (known as KKMM) but without a well-established coordination mechanism to formulate policies and foster programmes together. While the MCMC is primarily responsible for regulating the state-invested Telkom Malaysia (TM), MDEC is on record as wanting to see more competition in the sector. While the government is committed to the digital agenda – fostering entrepreneurship and a start-up culture is of particular interest – it has failed to create an institutional or regulatory environment that can resist vested interests, or the short-term requirements of national politics, and a fragmented administrative structure. Both in the case of DFTZs and MAMPU’s initiative to digitize public services, this gap

translates into slow implementation due to the need for coordination with multiple stakeholders within the government and with external stakeholders.

**Thailand**

The context of Digital Thailand is markedly different from Malaysia or Vietnam due to the coming to power of the military in 2014. The new government has re-written the national digital plan as a Digital Economy Master Plan and created a new Ministry of Digital Economy and Society (MDES) from the Ministry of Information and Communication Technology (MICT). The Plan is an ambitious transformation undertaking, particularly aggressive in its timelines, and comprehensive in its coverage and scope (Figure 1).

[Figure 1: Thailand's Digital Planning]

Source: Digital Economy and Thailand 4.0, [http://thaiembdc.org/%E0%B9%84%E0%B8%97%E0%B8%A2%E0%B9%81%E0%B8%85%E0%B8%99%E0%B8%94%E0%B9%8C-4-0/](http://thaiembdc.org/%E0%B9%84%E0%B8%97%E0%B8%A2%E0%B9%81%E0%B8%85%E0%B8%99%E0%B8%94%E0%B9%8C-4-0/).


Also new is a National Committee of Cyber Security (NSC) and a Digital Commission for Social Affairs and the Economy. Under the powers to be given to the NSC, telecom operators and ISPs will be required to submit cyber information on users without court warrants.99 The most controversial change has been the replacement of the independent broadcast and telecommunications regulator, (the NBTC) with a Digital Economy Policy Committee, chaired by the Prime Minister. This has raised questions as to the long-term independence of the state-invested incumbent carriers, the TOT and the CAT. The policy of auctioning of radio spectrum will be continued as it is designated as one of the sources of funding for the Digital Economy Fund, which will be used to support universal service and

to support a new national holding company to build and operate (as a wholesale business) Thailand's fibre and telecom tower assets. Thailand's new government is adopting a more assertive top-down approach to promoting and managing the digital economy, although it remains an economy open to foreign direct investment in most sectors.

**Digital Planning in Thailand**

Digital Thailand 4.0 aims to promote creativity, innovation, and the application of technology in various economic activities, to launch a new economic model to develop Thailand into a valued-based economy, and enable the country to break out from the middle-income trap. The Digital Thailand 4.0 initiative relies on the public and the private sector working together with society at-large in six key action areas:

1. Digital infrastructure
2. Digital innovation ecosystem
3. Digital technology for an equitable society
4. E-government services
5. Human capital
6. Holistic frameworks for a Digital Thailand

The National Science and Technology Development Agency (NSTDA) has responsibility within the plan to promote smart city applications. As part of the government’s push for implementation, the new policies were implemented in 2016/2017 including the Ministry of Information and Communication Technology Reform Act/Ministry of Digital Economy and Society Act, which restructured the ICT Ministry into the Ministry of Digital Economy and Society (MDES); and the Digital Development Act.

**Digital Development Act:** The bill established the Digital Economy Promotion Agency to manage the Digital Development for Economy and Society Fund, which promotes enterprises and initiatives that advance the use of technology that would foster economic and social development. It also establishes the National Committee for Digital Economy and Society, which will be responsible for setting policies and directions for the country’s digital economy development.

**Digital Economy Master Plan:** MDES has been tasked to draft the twenty-year Digital Economy Master Plan which will replace the existing IT 2020 ICT master plan, and is expected to be completed

---

100 Open Gov (15 February 2017) ‘Thailand PM announces Digital Government Plan 2017-2021 to achieve integrated, citizen-centric digital government within 5 years’

by November 2017. The plan will consist of five main domain missions, namely (i) hard infrastructure, (ii) soft infrastructure, (iii) service infrastructure, (iv) digital economy acceleration, and (v) digital workforce.  

The government’s commitment to transformational change for the digital economy is well-supported by institutional restructuring and regulatory changes. Nevertheless, political uncertainty and leadership changes in the leading agencies make implementation less efficient, and such issues hindered execution in the past, as well. Also, issues around personal data protection, taxation for technology companies and cybersecurity have not been resolved in the newly emerging digital economy framework. Most importantly, while Thailand 4.0 is comprehensive and holistic, it fails to offer a clear implementation path: it does not prioritize among the various goals and policy areas; nor are the agency leadership roles made clear. In a broader sense, the military government of Thailand faces the challenge of how to manage competing vested interests and tackling the implementation gaps in the programme as they arise.

**Vietnam**

Vietnam’s shift towards a digital economy is taking place within the context of a transition from a centrally-controlled to a state-directed mixed economy in which markets play a greater role. Digital policies are being driven by the ministries of Science & Technology, Planning and Investment, Information & Communications, and Finance.

Competition is being introduced between state-invested networks, with government encouraged market-focused investment, and supported by universal service charges (USC). On the down side, the implementation phase of the USC ran into inefficiencies due to carriers competing to give discounts to subscribers, but on the up side the spread of broadband has been rapid, especially of mobile services. Government policy aims to have at least 40% of households and individuals covered.

---

101 The Master Plan takes a holistic approach to digital development and sets specific goals and targets:
- 10,000 free Wi-Fi spots across the country, nationwide broadband, doubling of submarine cable capacity
- 15,000 one-stop online SME merchants
- Promote SMEs in the tourism industry
- Promote 1,500 start-ups each year
- Establish Smart Cities (Phuket and Chiang Mai)
- Develop Electronic Health Records (EHR)
- Establish 600 community digital centres
- Target 1,600 farmers for technology use
- Train 4,000 underprivileged individuals and elderly
- Establish Massive Online Open Course (MOOC)
- Develop G-Cloud, Software as a Service (SaaS) in 30,000 villages

102 The Ministry of Digital Economy and Society has 24 projects planned in the effort to create the Digital Thailand programme, at a total cost of BT3.76bn ($113.2m)

by fixed broadband Internet networks by 2020, 60% of Internet users supported by download speeds of 25Mbps, with 100% public Internet access points linked by fixed broadband and over 50% of them with downloads speeds of 50Mbps.\textsuperscript{104}

The adoption of digital technologies across industries, including agriculture, healthcare, security and defence is being promoted up to 2020 by the National Technology Development Programme. Vietnam is also aiming to reduce the use of cash to less than 10% of daily transactions and to promote mobile payment platforms for rural areas. E-commerce is one of the drivers of going cashless, valued at around 4% of GDP and growing rapidly.\textsuperscript{105} One very important aspect of the Programme is to promote start-up incubators, venture capital and more IT trained and skilled workers, including visas for foreign workers. Foreigners can now own property in Vietnam and operate 100% foreign owned companies. This is part of a more general opening of Vietnam. For example, access to social media such as Facebook has been permitted since 2013, and import tariffs, for example, on mobile phones, from ASEAN countries falls to zero under the ASEAN Economic Community (AEC) which formally came into existence in January 2017.\textsuperscript{106}

**Digital Planning in Vietnam**

Vietnam does not have a comprehensive strategy for digital economy development, but it has national-level strategies and initiatives with a digital component, and the government has acknowledged the importance of digital transformation for national competitiveness and keeping pace with global technology developments. The government aims to make Vietnam an international software hub and promote entrepreneurship as well as smart cities development, and has been trying to strengthen policy mechanisms and dialogue with the business community.

**E-Commerce:** The Vietnamese e-commerce market is forecast to be worth USD10 billion by 2020 with the mobile Internet creating some 150,000 new jobs, or 3.2% of total employment growth.\textsuperscript{107} The e-Commerce development plan (2016-2020) seeks to boost the sector and digital payments. The National Payment Corporation of Vietnam (NPCV) operates and manages an inter-bank connection system with 43 domestic commercial banks and foreign banks and provides e-commerce services to

\begin{itemize}
\item \textsuperscript{104} Compterweekly.com (8 Mar 2016), Broadband will reach 40% of Vietnam households by 2020, claims government, \url{http://www.computerweekly.com/news/4500278154/Broadband-will-reach-40-of-Vietnam-households-by-2020-claims-government}. Vietnam has also committed to switching to digital terrestrial television (DTT) by 2020, with a subsidy plan to help the low-income replace analogue TV sets.
\item \textsuperscript{105} Fintechnews.singapore (31 Jan 2017), Vietnam Announces Major Initiative to Become Cashless by 2020, \url{http://fintechnews.sg/7786/vietnam/vietnam-announces-major-initiative-become-cashless-2020/}.
\item \textsuperscript{107} USAID (2017), Promoting the Digital Economy in the ASEAN and APEC Regions, p. 3
\end{itemize}
over 200 merchants helping to overcome the limited interoperability among foreign payment providers.

**Smart Cities:** Vietnam has started the gradual development of smart cities that include Hue (2015), Da Nang (July 2016); Ho Chi Minh City (August 2016); Can Tho (September 2016). Free city-wide Wi-Fi has been installed in ten major cities. Smart city initiatives are more localised and are aligned to regional planning strategies.

Given the importance of the Internet to the successful development of digital industries in Vietnam, the government maintains a strict regulatory approach to the Internet which may restrict the impact of entrepreneurship and innovation. The scope and clarity of digital economy building efforts by the state remains limited compared to the opportunities a more enabling role might create, especially given the vibrancy of Vietnam’s private sector which is engaged in a broad range of industries from online learning to e-commerce. Hence the gap between the government’s support of the digital agenda and what it actually does is defined more by the role it chooses to play as opposed to inherent problems with its initiatives.

**Comparative Assessment: Malaysia, Thailand, Vietnam**

As the examples in the country cases above suggest, the approach they have taken to develop their digital economies differ significantly. These differences are based on the level of economic maturity, legacy institutions, power distribution vis-à-vis to the central authority, the level of economic liberalization and state involvement among other factors. This assessment aims to give a brief overview without attempting comprehensive analysis of the differences.

<table>
<thead>
<tr>
<th>Government vs Private Sector Leadership</th>
<th>Malaysia and Thailand both consider government leadership to be paramount in shaping the digital agenda. In Vietnam, the state’s primary self-identification as a regulator and “controller” of the economy, coupled with an enterprising and vibrant private sector gives more opportunities to the latter to shape a forward-looking agenda.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Down vs Bottom Up</td>
<td>All the three economies illustrate a more top down approach, although in Vietnam’s cases this is of limited scope. Only Malaysia and Thailand have comprehensive national digital plans as blueprints</td>
</tr>
</tbody>
</table>

108 TRPC (5 Dec 2015), Going Digital: The Status and Future Potential of Internet-Based Economies across Asia, p. 55
for state promotion of the digital economy. Vietnam has issued a five year (2016-2020) National Development Programme which sets out a Tech 2020 Plan, mostly focused upon supporting sector-specific developments and grants for start-ups.109

| Innovation vs Regulation | All three governments place importance upon both, which sometimes helps and sometimes hinders innovation-led development. An OECD report on Malaysia found that a vibrant economy nevertheless suffered shortages of requisite skills and low levels of productivity, while national plans were trying to address both110. A UNCTAD assessment in 2015 of innovation in Thailand points to a supply-side dominated approach, citing the preponderance of research institutes, but “a lack of clear and strategic orientations and a dispersion of resources on multiple, uncoordinated projects with an insufficient critical mass.”111 A World Bank report on innovation in Vietnam noted the country’s strong attraction to foreign investment, but low levels productivity and especially a “seriously underdeveloped information base for innovation policy making.”112 |

Besides the different approaches, these countries also differ in their capacity both in terms of institutional resources in the government and technological readiness to address the challenges driven by the digital transformation. For example, Thailand’s digital agenda was able to successfully reflect its core strengths in manufacturing and IoTs – this does not appear in Vietnam’s plans at all, even though the Vietnamese economy has very developed manufacturing capacity in certain industries. Similarly, Thailand focuses on the issues of cybersecurity and data privacy, but has limited acknowledgement of data sovereignty issues, which weakens the country’s ability to enforce data security. Malaysia, which has one of the earliest data privacy laws in the ASEAN, has issues of data privacy and protection from state investigation which hinders the country’s ability to compete for hosting data centres which are fundamentally concerned about data sovereignty issues. Neither Vietnam nor Thailand has a cybersecurity law, which is a concern to the emerging digital industries sectors.

Table 3 summarises where Malaysia, Thailand and Vietnam currently stand with regards to data security/cybersecurity and data privacy.

### Table 3: Cybersecurity and Data Privacy in Malaysia, Thailand and Vietnam

<table>
<thead>
<tr>
<th>Country</th>
<th>Cybersecurity</th>
<th>Data Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Malaysia</strong></td>
<td>Malaysia has comprehensive legislation covering cyber security and national security. The National Security Council Act was passed in 2016, giving the new NSC extensive powers of surveillance and detention of persons deemed a threat to the state. In 2006, the National Cyber Security Policy (NCSP) was established to protect the Critical National Information Infrastructures (CNII) and encourage greater cross-agency reporting of cyber-attacks. Cybersecurity Malaysia (CSM) was created to foster greater co-operation with the private sector and overseas government agencies. Other legislation overlapping with NSC powers and CSM, and which gives authorities wide powers of search and seizure, includes the Computer Crimes Act (CCA) 1997 and the 1998 Communications and Multimedia Act (CMA).</td>
<td>The PDPA does require data on Malaysians to be stored on local servers, but cross-border data transfers are permitted subject to the agreement of the data subject, or where it is the personal interest of the data subject, and where reasonable steps to protect the data have been taken. However, there are certain restrictions on the use of the cloud for financial data. Bank Negara’s approval is required until policy towards FinTech companies has been finalised.</td>
</tr>
<tr>
<td><strong>Thailand</strong></td>
<td>The disclosure or transfer of data may be considered a wrongful act under the Thai Civil and Commercial Code, if it causes damage to the data owner. Besides that, Thailand does not have a specific law to protect personal data privacy, but it does have laws giving the authorities widespread powers of surveillance and cybersecurity, including the Special Case Investigation Act of 2004, covering the interception of communications in postal, digital and telephonic forms, and the Computer-Related Crime Act (CCA), which came into effect in 2016. Under the Cybersecurity Bill, currently being considered by the National Assembly, the powers of the Cyber Security Commission (CSC) would be further strengthened. The chairman of the CSC is the Digital Economy Minister, and other commissioners represent the Secretary of the National Security Council, the Digital Economy Permanent Secretary, the Defence Permanent Secretary and the Commander of the Technology Crime Suppression Division. Despite there being a civilian government in Malaysia...</td>
<td></td>
</tr>
</tbody>
</table>
and a military government in Thailand, the current approaches to national and cybersecurity security are rather similar.

**Data Privacy**

There is no direct reference to data transfers in Thai law, but under the Thai Civil and Commercial Code, a person who wilfully, negligently, or unlawfully injures the life, body, health, liberty, property or any right of another person has committed a wrongful act and is required to compensate the victim. Disclosure or transfer of data may be considered a wrongful act if it causes damage to the data owner. In practice, the prior written consent of the data owner should be obtained before transferring the data to any third person. Disclosure of data without the consent of the data owner is permissible in very limited circumstances (e.g. pursuant to an order from a government authority or Thai court).  

**Vietnam**

**Cybersecurity**

Vietnam plans to introduce an import licensing requirement for cyber information security products, falling into three categories: (i) products that scan, check, and/or analyse the architecture, status, and record data of an information system, detect its flaws and weaknesses, and examine risks to information safety; (ii) products that supervise and analyse data in an information system, collect and analyse record data in real time, and detect and alert on unusual events or those with potential danger to information safety, and (iii) products that stop attacks and intrusions into information systems (a category that could be broadly interpreted to include many products that have standard mechanisms to deter cyber-attacks. These are under discussion with international trade partners.

**Data Privacy**

Vietnam has no laws protecting personal data privacy, and has relied upon its state-owned national carriers to conduct surveillance. ISPs, for example, are expected to monitor and block undesirable sites, but as this is done through the DNS (Domain Name Server) only whole sites can be blocked. The government is currently implementing the regulations of the 2015 Law on Network Information Security. Circular No. 38 came into effect in February 2017, detailing the cross-border distribution of public information. The Circular was the regulatory implementation of Decree 72 issued by the Ministry of Information and Communications in 2013. Government policies towards online data are restricted to public information and data transmitted over the Internet must be in accordance with Vietnam’s laws. But ISPs must store at least one copy of data pertaining to Vietnamese citizens in-country and make available for inspection by the relevant authorities.

---

CHAPTER 5: Recommendations: Building Blocks for a Digital Economy

Framework

This chapter outlines policy options and measures available to governments to build their digital economies. This digital development ‘toolkit’ outlines the policy and regulatory tools governments can use and the strategic choices they must make. These choices, coupled with cross-agency work within the government, can create more agile methods of governance preparing policy makers to become enablers of the digital economy. Enablers by way of direct state initiatives and investments; enablers by way of policy-incentives and market-sensitive regulations. For government agencies, the shift from the position of regulators and “risk managers” to becoming enablers is necessary as traditional policy tools and regulatory regimes developed in an industrial age of vertical policy silos are not suitable for the new interconnected landscape. The cross-cutting and horizontal issues discussed in Chapter 2 such as privacy, data protection, interoperability and cybersecurity require flexible tools and a good understanding of national regulatory issues, markets and legacy institutions. As the pace of innovation accelerates, countries must adapt their policy making and regulatory processes or risk being left behind.

Measurement and Goal Setting

A preamble to any digital economy framework building is the need of measuring the impact the government is setting out to achieve. But measuring the digital economy in national economic and trade statistics is often complicated as the cross-cutting nature of the Internet makes it hard to delineate and quantify its benefits.

However measurement of the digital economy is necessary not only for a better understanding of the state of the economy and society with statistical tools. Negotiating government budgets and resource allocation in agency portfolios is a highly politicised process, hence agencies and initiatives championing digital change need the ability to monitor and evaluate their projects, and measure and showcase their impact boundaries.

Leadership and Coordination Competencies

Cross-sectoral policy making: Traditional public administration functions are based on silos – where public servants’ expertise is mostly limited to a specific policy domain such as agriculture, education
or infrastructure. Creating a digital economy requires the breaking down of such boundaries within areas of policy, expertise and across areas of perceived or real institutional hierarchies working across sectors. This cross-sectoral approach depends on a sustainable mechanism which enables the continuous incorporation of digital into sectoral policy making.\footnote{The European Union uses the expression “digital mainstreaming” (along the lines of gender mainstreaming) to describe the process of incorporating the digital agenda into all its development policies.} Many governments have chosen to create distinct entities in charge of the digital economy – agencies like the MDES in Thailand and MDEC in Malaysia, or specialised departments within the Prime Minister’s Office. Singapore’s GovTech, “the CIO of the Singapore government” in charge of the digital transformation of the public sector, established a cluster group that collaborates closely with sectoral agencies (in finance, health, education etc.) to ensure that newly developed digital services answer the needs of their users.\footnote{GovTech Singapore, Clusters Group, \url{https://www.tech.gov.sg/About-Us/GovTech-Teams/Clusters-Group/Clusters-Group}} Specialised agencies alone won’t create a cross-sectoral communication process without establishing formalised communication channel and collaboration methods.

**Agility:** The pace of innovation has accelerated and rapid technological changes require governments to gauge, understand, make and implement regulatory decisions faster. The internal constraints of agencies, the risk of overregulation or simply taking a bet on a specific technology for policy making purposes means that agility is not only about speed, but more about flexibility. Agility should also be a defining characteristics of public service provisions (e.g. finding faster and more efficient ways to handle licensing, business registration).

**Multi-stakeholder approach:** Governments not only need to coordinate various public sector stakeholders, but engage the private sector, civil society and academia in setting the agenda for digital development, creating appropriate regulations and implementing digital initiatives. A widely used long-term cooperative arrangement is Public-Private Partnerships (PPPs). Malaysia, for example, uses the PPP model – for example, in April 2017, the Ministry of International Trade and Industry launched the M-Powered Platform, an employment portal for persons with disabilities, in collaboration with Microsoft.\footnote{Microsoft (13 Apr 2017), Microsoft launches M-Powered in collaboration with Dialogue in the Dark, \url{https://news.microsoft.com/en-my/2017/04/13/microsoft-launches-m-powered-collaboration-dialogue-dark/}} These initiatives are important, but only if they genuinely involve a partnership, with mutual responsibilities and accountabilities, and are not simply another name for outsourcing. For example, monitoring and evaluation are methodologies that are too infrequently applied in the public sector, and consequently there is no learning nor improvement, for example, in project management.
Strategic Choices on Platforms

Digital platforms range from social media to national e-identity schemes, from application stores to public cloud services, including infrastructure. Such platforms facilitate exchange between multiple communities (such as users and service providers) in a massively scalable manner. Governments using these platforms must make strategic choices around which ones to use for an efficient allocation resources. For example, some governments in the Asia-Pacific have launched 'cloud first policies', which aim to foster the use of cloud computing services in the public sector. There are different models for implementing such a policy – agencies can build their own proprietary systems (government or G-cloud) or the government can establish a cloud services panel, where agencies can procure from selected public cloud providers.

Building your own platform: Governments can get their own platforms built. Thailand’s e-ID scheme and India’s Aadhaar both run on servers stored in a government-owned data centre. Thailand has budgeted for the procurement of 200,000 smart card readers for 80 state agencies to improve accuracy and accountability in verification of e-ID.

Outsourcing the platform: Public and hybrid cloud services offer a cost-effective alternative to governments, who are not keen on investing in their own hardware, yet want to benefit from data storage and analytics capabilities. Malaysia has such a private cloud run by Microsoft for 1GovEA and 1GovUC initiatives.

Regulating existing platforms: Beyond making decisions about platform technologies used in public administration and service delivery, governments can regulate existing platforms to boost the digital economy. Mandating or facilitating the interoperability of platforms means that digital traffic can run effectively across different types of networks (including telecoms, banking, educational and health networks) enabling economies of scope. But the time must be ripe to mandate, and that time is usually after a market has been created and is in need of the removal of barriers to further expansion in a way that encourages competition. Lack of interconnectivity or interoperability will, at some point in time, become a barrier to new entrants and new services.

118 The interconnections of networks, which brings greater economies of scale as the fixed costs of infrastructure rollout are spread across a greater level of output bringing about a fall in unit costs. The interoperability of operating system platforms. This brings about economies of scope, as fixed costs are spread across a wider range of output of different products and services.
Policy Approaches and Tools for Effective Digital Governance

Whole-of-government (WOG) initiatives offer a methodology for cross-sectoral collaboration among various public sector agencies. The WOG approach requires agencies to make their vertical organisational structures permeable so that learning, communication, analysis and decision-making processes can take place across organisational boundaries. Most WOG initiatives are directed top-down from senior leadership, and require a disciplined approach to information gathering and sharing. The WOG approach allows agencies to move towards a more enabling approach, by rethinking the role of regulator, increasing agility and creating opportunities for cross-agency learning and exchange of knowledge on policy issues and tools to tackle them with.

The relationship between governments and the private sector in service of building a digital economy has several well-trodden avenues for engagement enabled by a commitment to the multi-stakeholder approach. PPPs, government procurement mechanisms and the transfer of expertise in niche areas such as cybersecurity are established practices.

- **Marketplace for government procurement.** To take advantage of innovative technologies such as cloud services, governments need to reform their IT procurement processes. Shifting from a capital expenditure base (where agencies buy distinct goods like computers) to the operating expenditure model would allow government to take advantage of scalable, on-demand services (such as public cloud infrastructure or data analytics). A marketplace model simplifies multi-layered procurement systems both on a departmental and national level. Agencies can shop at the centralised digital marketplace, which limits vendor participation by a shared set of standards. In Thailand, individual ministries have been trying to change procurement processes to access digital tools more easily, but are hindered by the lack of centralised government policy.

- **Sandboxing** is a regtech framework increasingly used by financial regulators experimenting with FinTech solutions in a low risk, but real-life setting without the burden of licensing or regulatory requirements. Sandboxing allows the private sector and regulators to engage in a fail-safe environment, while fostering innovation. The Monetary Authority of Singapore launched such a "regulatory sandbox" for organisations to test and trial FinTech solutions. In a similar vein, Bank Negara Malaysia released the Regulatory Sandbox Discussion Paper in July 2016 to set a space for FinTech companies to develop digital services and products to bring down regulatory barriers.

---

A different aspect of the relationship between governments and the private sector is the relationship with civil society organizations, and governments’ ability to engage with not-for-profit entities and incorporate their insights into building the digital economy. While political and legacy factors often create a top-down approach towards NGOs, creating avenues for bottom-up development has its merits as these organizations have the ability to advocate for and raise awareness among the public on various digital issues. In some cases, government-sponsored efforts can result in distrust arising within civil society as to the true motives behind the introduction of a digital technology, such as a nationwide ID system. In India, the spread of the Aadhaar card was seen by government as an effective tool for social inclusion in welfare payments and in the banking system, but was strongly opposed by some as an unwarranted form of mass surveillance.\footnote{The Hindu (31 Mar 2017), Is Aadhaar a breach of privacy?, \url{http://www.thehindu.com/opinion/op-ed/is-aadhaar-a-breach-of-privacy/article17745615.ece}}

Besides focusing on the relationship among government agencies, and between the public and the private sector, governments also need to have sufficient capacity to understand the changes in the international technological and policy landscape and their impact on national digital economy agendas. Cross-border data transfer, data privacy and security and the taxation of digital economy players present ever-shifting challenges to policy-makers and regulators and it helps of there is a good understanding international trends in these areas.

Interoperable regulatory regime setting requires accepting the principle of equivalence – for example, in the levels of data protection offered and expected when data is transferred from one jurisdiction to another. On the local level, national standards bodies have to consider the costs of setting localized standards as opposed to following international ones – differences can affect the costs and competitiveness various industries from phone manufacturing to the building requirements of data centres.

Technology foresight\footnote{UNIDO, Technology Foresight in Asia, \url{http://www.unido.org/foresight.html}} is an initiative by the United Nations Industrial Development Organization. The methodology aims to provide input in policy design and problem definition through capacity building and a knowledge exchange platform. Vietnam, for example, relies on the project to help developing policies and strategies on science, technology and industrial innovation, compatible with the economic and social goals of the country.\footnote{UNIDO, Technology Foresight in Asia, \url{http://www.unido.org/foresight/asia.html}}

Digital assessment\footnote{Digital assessment questions: Are there relevant ICT or Internet drivers influencing the way the problem is defined? Are there identifiable trends in your policy domain indicating that digital technologies will change the nature of the defined problem?} is a methodology used by EU institutions, which focuses on identifying digital technology related issues to an already identified problem definition or issue. The importance of
digital assessments is justified on the grounds that the sooner “the earlier ICT requirements and associated implications are identified and analysed, the greater the likelihood that appropriate solutions can be prepared which are accepted by stakeholders.”

How are ICT and the Internet linked to the problem? Is Internet based activity growing compared to classical activity (face to face; snail mail; broadcast, etc.)? Is amongst the causes of the problem the fact that ICT means are not used, or are insufficient/outdated and not responding to the needs?

Whether ICT and Internet factors are properly identified in the baseline scenario. How rapidly is the problem changing? To what extent? How stable is the baseline scenario you have established with respect to identifiable technology trends?

Who are the stakeholders and how they are linked to the ICT and Internet dimension of the problem?