

02/2018



# PANORAMA

Insights into Asian  
and European Affairs

PANORAMA  
INSIGHTS INTO ASIAN  
AND EUROPEAN AFFAIRS

# Digital Asia

*Panorama: Insights into Asian and European Affairs* is a series of occasional papers published by the Konrad-Adenauer-Stiftung's "Regional Programme Political Dialogue Asia/Singapore".

© 2019 Konrad-Adenauer-Stiftung, Singapore

Editors: Christian Echle, Katharina Naumann, Megha Sarmah

Publisher:  
Konrad-Adenauer-Stiftung Ltd  
Arc 380  
380 Jln Besar  
#11-01  
Singapore 209000  
Registration Number: 201228783N  
Tel: (65) 6603-6160  
Tel: (65) 6227-8343  
Email: [Politics.Singapore@kas.de](mailto:Politics.Singapore@kas.de)  
Website: [www.kas.de/singapore](http://www.kas.de/singapore)

All rights reserved. No part of this book may be reprinted or reproduced or utilised in any form or by any electronic, mechanical or other means, now known or hereafter invented, including photocopying or recording, or in any information storage or retrieval system, without permission from the publisher.

Manuscript offers, review copies, exchange journals, and requests for subscription are to be sent to the editors. The responsibility for facts and opinions in this publication rests exclusively with the authors and their interpretations do not necessarily reflect the views or the policy of Konrad-Adenauer-Stiftung.

Cover design by Flava Design LLP

Design, Layout and Typeset:  
Select Books Pte Ltd  
65A, Jalan Tenteram  
#02-06, St Michael's Industrial Estate  
Singapore 328958  
Website: [www.selectbooks.com.sg](http://www.selectbooks.com.sg)

ISSN: 0119-5204

PANORAMA  
INSIGHTS INTO ASIAN  
AND EUROPEAN AFFAIRS

# Digital Asia



# CONTENTS

Preface .....	7
China's Techno-Utilitarian Experiments with Artificial Intelligence ... <b>Dev Lewis</b>	9
Social Credit System in China .....	23
<b>Chris Fei Shen</b>	
China's Tech Giants: Baidu, Alibaba, Tencent .....	35
<b>Hong Shen</b>	
Japan's Innovation Systems at the Crossroads: Society 5.0 .....	45
<b>René Carraz and Yuko Harayama</b>	
Taking Stock of Smart Nation Development in Singapore .....	59
<b>Teck-Boon Tan</b>	
Redefining Parity at Work in India .....	71
<b>Terri Chapman</b>	
Dissecting the Rise and Plateau of Digital Payments in India .....	83
<b>Bedavyasa Mohanty</b>	
Promoting Prosperity and Providing Protection: Australia's International Cyber Engagement Strategy .....	93
<b>Damien Spry</b>	
Asia Pacific Contributions to International Cyber Stability .....	107
<b>Caitríona Heint</b>	
Digital Transformation and Industry 4.0 in Southeast Asia .....	121
<b>Raja Mikael Mitra</b>	

Energy Security in the Digital Age and Its Geopolitical Implications for Asia .....	147
<b><i>Frank Umbach</i></b>	
Defying Gravity: Europe in the Digital Transformation .....	161
<b><i>Mario Voigt</i></b>	

# Preface

Happy Birthday, Internet! In 2019, we are celebrating the World Wide Web's 30th anniversary. Growing from ARPANET, a decentralised network created by the Pentagon that was designed to withstand a nuclear attack, to its current status as a global platform that connects billions of people and devices, the development of the Internet has long been guided by the United States. US companies developed the first personal computers, smartphones and social networks that we use to communicate as well as the routers and servers that carry the world's data.

It is Asia, however, where the future of the Internet is most likely to be written. Already today, China has the highest number of internet users in the world. India is simultaneously home to the second-largest number of smartphones in the world and the world's largest offline population. "The next billion users" are mainly Asian.

Concurrently, Asian companies are making their way onto the list of top technology companies: South Korea-based Samsung is the second-biggest tech company in the world. In 2018, China's Tencent broke into the top ten, after Foxconn Technology Group joined the club in 2017.

While during the advent of the internet, the US has taken a market-centred approach, policymakers of today operate in a complex, dynamic and uncertain environment, where governments are increasingly asked to act as facilitators in the face of these constantly changing conditions. In late 2014, Singapore rolled out the Smart Nation Initiative – a mega-digitalisation project to transform the city-state into a hyper-connected nation. In Japan, the concept of "Society 5.0" was introduced as a foundation for future economic growth.

China is rising as a cyber superpower. In a very short period of time China has established a leading role in Artificial Intelligence, dominating in global investment, number of AI companies, and applications of new technologies like facial recognition. Baidu, Alibaba and Tencent (BAT), the three most powerful companies providing web applications in China, are sharing the same stage as Apple, Google, Facebook and Amazon. Not least there is the social credit system, often depicted as a draconian mass surveillance project driven by almighty technologies to curtail personal freedom.

On a global level, digital networks play an increasingly important role in international relations, trade security, and strategic deliberations. In the absence of a global agreement for international cybersecurity, the contribution of Asia Pacific states to finding common ground on state operations in cyberspace is ever more important.



In this issue of our biannual *Panorama: Insights into Asian and European Affairs* the authors discuss the implications of digital policies and the impact of digital technologies on economies and societies in Asia. The authors map out the size of China's AI ecosystem so far, analyse the factors behind BAT's success and point towards an underlying motivation for the social credit system: lack of trustworthiness at all levels of society. The issue presents Singapore's Smart Nation Initiative, Japan's Concept of "Society 5.0", and Australia's Cyber Engagement Strategy, discusses trends in employment relations driven by technology adoption in India and digital economy transformation in ASEAN. Where does Europe come into play? Read on!



Christian Echle  
Director  
Political Dialogue Asia, Singapore

# China's Techno-Utilitarian Experiments with Artificial Intelligence

*Dev Lewis*

## INTRODUCTION

Any article talking about China's journey with Artificial Intelligence (AI) has to begin with the board game Go. More specifically, the face-off between Lee Sedol, winner of 18 world titles and widely considered to be the greatest player of the past decade, and Google's DeepMind-AI-powered Alpha Go. In a now landmark match, Alpha Go didn't just trounce Lee Sedol 4-1, it displayed uniquely inventive tactical abilities, in a match that was watched by over 200 million people worldwide<sup>1</sup>. Go, a highly strategic game with more than 2,500 years of history in China and the East Asia region, has served as an essential game for intellectuals and thinkers in Chinese bureaucracy for centuries and plays a central role in military and strategic planning in China today. DeepMind's victory over Lee Sedol and then later over Chinese champion Ke Jie captured the minds of people all over the world, especially East Asia. In China it lit the ignition of the Chinese combustion engine that has since stayed in 6th gear, driving an ambition to first catch up to and then surpass all others as the world's leading AI power.

AI development is regularly framed as an arms race, which, although misleading because it ignores the significance of cross-border exchanges of talent and investment, does convey the very real sense of competition between countries to lead in this domain. There is a very real historical geopolitical dimension to this, as the Chinese Communist Party (CCP) believes it has been kept at arm's length by Western countries from access to the latest technology. Weaning off dependence on Western-built technology is as much a political and security imperative as it is an economic one. For China, AI is seen as a strategic technology that will help it

---

<sup>1</sup> "Innovations of AlphaGo," DeepMind, accessed 31 August 2018, <https://deepmind.com/blog/innovations-alphago/>.

achieve its core national economic, social, political, and military objectives, which will see the country transition to a developed, prosperous economy with the Party at the helm<sup>2</sup>. This was outlined as such when the State Council of China – the premier policy body – issued the “Next Generation AI Development Plan” in July 2017, which unambiguously called for China to become the number one global source of AI innovation by 2030.

The document notes China’s recognition that ever since the first industrial revolution it has consistently played catch-up to the West, particularly the US, lagging behind in patents, talent, and scientific research. In AI, China wants to make the leapfrog to be a trailblazer. In the context of AI this means: breakthroughs in fundamental research, building a commercial ecosystem, cultivating and attracting the best talent, and setting global standards and norms. Prior to this plan, Chinese companies such as Baidu and Alibaba had already placed their bets on AI, while previous government plans had made references to AI.

This State Council plan sought to develop a “whole-of-nation-approach,”<sup>3</sup> creating an incentive structure for all stakeholders – entrepreneurs, students, scientists, investors, policy makers, and government bodies – to leverage China’s strengths, better understand the technology and craft appropriate legal frameworks, grow the talent pool of AI engineers, and develop indigenous innovation that will enable this leapfrog. Fast forward to nearly two years, how big is China’s AI industry in commercial terms?

According to the Tsinghua University Technology Policy and Research Institute’s China AI Report (中国人工智能发展报告) the size of China’s AI industry in 2017 is estimated to be RMB 23 billion (Euro 2.9 billion)<sup>4</sup>. But it is very difficult to accurately make such assessments because AI itself is a catch-all term for a number of different technologies and appliances<sup>5</sup>, not to mention the difficulties in accessing data. An illustration of the disparity: the Tsinghua AI report counts 1,011 AI companies

---

<sup>2</sup> “Translation: Chinese Government Outlines AI Ambitions through 2020,” New America, accessed 1 September 2018, <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-government-outlines-ai-ambitions-through-2020/>.

<sup>3</sup> Kania, Elsa, “China’s Artificial Intelligence Revolution,” The Diplomat, 27 July 2017, accessed 31 October 2018, <https://thediplomat.com/2017/07/chinas-artificial-intelligence-revolution/>.

<sup>4</sup> 清华大学正式发布《中国人工智能发展报告2018》，Tsinghua University Technology Policy Research Centre, “China AI Development Report 2018,” [http://www.sohu.com/a/241293549\\_680938](http://www.sohu.com/a/241293549_680938), accessed July 2018.

<sup>5</sup> According to the 3-year AI implementation plan issued by the National Development and Reform Council (NDRC), AI is: basic research in fields such as deep learning, the development of basic software and hardware such as chips and sensors, and applied research in areas like computer vision and cybersecurity.

in China, while the Beijing Municipal Commission of Economy and Information Technology in its White Paper “Beijing AI Industry Development White Paper” (北京人工智能产业发展白皮书) counts 4,000 AI companies, with Beijing alone home to 1,070. It is reasonable to settle on a number closer to the former, as efforts by the China Money Network<sup>6</sup> and think tank Yiyou<sup>7</sup> counted 1,122 companies and 922 companies respectively. For context, the number of AI companies globally is estimated to be anywhere between 3,465 to 4,925<sup>8</sup>.

Given these numbers it is not surprising to see that China makes up a significant share of global funding in AI. China received 60% of global investments in AI between 2013 and 2018, according to the Tsinghua report, while a CB Insights report attributes 48% of worldwide AI investments in 2017<sup>9</sup> to China. That a lot of the investment took place in the past two years is reflected in the fact that 81% of the companies are between angel, seed, and Series A rounds, as per the China Money Network report cited above. According to the Tsinghua report the growth in the AI industry is expected to peak at 75% in 2018 and eventually decline to 40% by 2020<sup>10</sup>. For context: The State Council is aiming for China’s “core AI industry” to reach RMB 10 trillion (Euro 1.2 trillion), the amount the sector needs to grow 25 times between 2018 and 2030<sup>11</sup>.

Any talk of investment in technology in China has to mention Baidu, Alibaba, and Tencent, collectively referred to as BAT, but also now Huawei. None of them are strictly AI companies as defined above, but they are key architects driving research and development (R&D) and mergers and acquisitions and are of course, the owners of data. According to a huxiu.com report these four companies are linked, mainly through investments, to 65% of 190 Chinese AI companies surveyed. Each of these four companies focus their R&D and investments in areas that currently boast a competitive AI advantage due to their existing businesses and platform. Alibaba

<sup>6</sup> Using the definition “private companies with a core focus on AI technology”.

<sup>7</sup> “Artificial Intelligence Research in China 2018,” 亿欧\_产业创新服务平台 Iyio, August 2018, accessed 15 October 2018, <https://www.iyio.com/intelligence/reportPreviewH5?id=87240&&id=574>.

<sup>8</sup> “China AI Top 50,” China Money Network, 19 September 2018, accessed 15 October 2018, <https://www.chinamoneynetwork.com/china-ai-top-50-2018>.

<sup>9</sup> “AI 100: The Artificial Intelligence Startups Redefining Industries,” CB Insights Research, 18 September 2018, accessed 24 September 2018, <https://www.cbinsights.com/research/artificial-intelligence-top-startups/>.

<sup>10</sup> 清华大学正式发布《中国人工智能发展报告2018》, Tsinghua University Technology Policy Research Centre, “China AI Development Report 2018,” [http://www.sohu.com/a/241293549\\_680938](http://www.sohu.com/a/241293549_680938), accessed July 2018.

<sup>11</sup> Ibid.

in retail, finance, and entertainment marketing; Baidu in search and AI applications, especially in autonomous vehicles, Tencent in education and social, and Huawei in hardware through its phones and AI chips.<sup>12</sup> Yet, increasingly so, public capital is important, most notably through Government Guidance Funds (GGF) (政府引导基金), which will be touched upon in more detail in the next section, and which have investments in several large and small AI companies.<sup>13</sup>

Finally, China has risen as a source for AI research by several quantitative measures. The number of AI papers published in China has seen a dramatic increase by 150% between 2007 and 2017 and now makes up 25% of the number of AI papers globally, according to the Stamford University published AI Index 2018. These papers are also being cited on average 44% more now than in 2000, suggesting a greater relevance, although for now China still lags behind Europe and the US who lead the way by measure of citation.

## WHAT DO WE MEAN WHEN WE SAY AI?

Computer Vision, Natural Language Processing, and Voice Recognition are among the most important core machine learning-based technologies that have seen significant breakthroughs in application worldwide and this is the case in China as well. Facial recognition makes up 35% of all AI applications in China<sup>14</sup> and it is in this area that some of China's most well-known, and globally controversial, AI unicorns, such

---

<sup>12</sup> Qian Dehu, "Map to Understand China's AI Close-quarters Combat: Only Baidu and Huawei are Really Doing AI", <https://docs.google.com/document/d/1lidRNebNblouizG2jjW7LqySbD-fl61Xx0ujVgZbp4/edit#> (translation by Jeffrey Ding).

<sup>13</sup> Ibid.

<sup>14</sup> 清华大学正式发布《中国人工智能发展报告2018》, Tsinghua University Technology Policy Research Centre, "China AI Development Report 2018," [http://www.sohu.com/a/241293549\\_680938](http://www.sohu.com/a/241293549_680938), accessed July 2018.

as Sensetime 商湯科技<sup>15</sup>, Megvi Face++<sup>17</sup>, and Yitu 依图<sup>18, 19</sup> have emerged. Natural Language Processing (NLP) and Voice Recognition make up 31% and 25% of AI applications in China respectively. Provincial-level and city-level government bodies are also important clients as they too seek to digitise or risk being outshone by a neighbouring district or province in areas ranging from better urban management to improving the quality and access of government services. The most controversial area is, of course, the use of these technologies to bolster security, which is resulting in heightened state surveillance. Examples include Yitu's technology being added to CCTV cameras across Shanghai to aid law enforcement<sup>20</sup>; Sensetime, which is now moving towards working more closely with the security apparatus in Xinjiang; and experiments with the use of big data collection and algorithmic policing that may take place within the arches of the Social Credit System, which is seeking to improve people's accountability in the face of the law. This reflects the dual-use edge of these technologies and China is at the forefront of applying AI in its law enforcement apparatus, unobstructed by significant legal obstacles or strong privacy protection concerns at the moment.

The Chinese private sector is responsible for China's technology sector success, especially for developing commercially successful applications around payments and e-commerce. However, the extent of the influence of the State, which can be read interchangeably with the CCP, on the future path of technology is on the rise. A flurry of laws and regulations on domestic Internet governance, coupled with the lofty State ambitions around AI, outlined above, have emboldened the strong nexus between the State and all stakeholders in the industry.

---

<sup>15</sup> SenseTime independently develops deep learning platforms, supercomputing centers, and a range of AI technologies such as face recognition, image recognition, object recognition, text recognition, medical image analysis, video analysis, autonomous driving, and remote sensing.

<sup>16</sup> Russell, Jon, "China's SenseTime, the World's Highest-valued AI Startup, Closes \$620M Follow-on round," TechCrunch, 30 May 2018, accessed 24 September 2018, <https://techcrunch.com/2018/05/30/even-more-money-for-senstime-ai-china/>.

<sup>17</sup> Megvii Technology operates a face detection, recognition, and analysis platform for websites, mobile applications, and smart televisions.

<sup>18</sup> "Yitu Technology," Crunchbase, accessed 24 September 2018, <https://www.crunchbase.com/organization/yitu-technology#section-web-traffic-by-similarweb>.

<sup>19</sup> Yitu conducts fundamental research on Artificial Intelligence aimed at finding comprehensive solutions for machine vision, listening and understanding, and builds pan-industry solutions.

<sup>20</sup> "Yitu Profile," Bloomberg, accessed 15 September 2018, <https://www.bloomberg.com/profiles/companies/1510312D:CH-shanghai-yitu-internet-technology-co-ltd>.

## ECOSYSTEM BUILDING WITH CHINESE CHARACTERISTICS

The Chinese technological ecosystem is distinctive in a number of ways, but the role and influence of the Chinese government arguably sets it apart. It is able to develop and implement visions with the same control as the lead conductor of a complicated orchestra. Lee Kaifu notes in his new book *AI Superpowers*<sup>21</sup> that in China the government sets the tone by putting AI at the front and centre of the agenda, which subsequently energises and drives the entire ecosystem, including local governments, entrepreneurs, students, and universities alike.

The Central government has issued a number of plans and strategy documents (See Table 1 for a list of all Central-level plans related to AI) that have acted as a call to action for provincial-level governments. At least 15 of China's 31 provinces have issued AI development plans of their own. On the surface, these plans are very much in line with the Chinese tradition of Leninist central planning. Rogier Creemers, an authority on Chinese techno-legal issues, described the Next Generation AI plan as "Santa's list of desiderata and objectives, but with little insight into how these should be achieved other than by throwing money at the problem"<sup>22</sup>. One clue is the audience it is meant for, i.e., not people sitting in India or Germany, but party and government officials at all levels of the central and provincial governments. Matt Sheehan of Macropolo explains: "The hope is that if local officials cough up a sufficient number of these gifts – factories adopting smart robots, new research centers pursuing natural language processing, autonomous agricultural drone demonstration projects – they will eventually add up to the plan's headline goal: global leadership in AI"<sup>23</sup>.

One phenomenon that captures this approach is the government-backed fund of funds known as GGFs first mentioned above. The first GGF was an experiment by the Beijing Municipal government in 2002, following official recognition by the NDRC in 2008, there are estimated to be between 800-1,000 of these funds across

---

<sup>21</sup> Lee Kaifu, *AI Superpowers*. Lee Kaifu is Chairman and CEO of Sinovation Ventures.

<sup>22</sup> Creemers, Rogier, "China's Plan to 'Lead' in AI: Purpose, Prospects, and Problems," *New America*, accessed 15 September 2018, <https://www.newamerica.org/cybersecurity-initiative/blog/chinas-plan-lead-ai-purpose-prospects-and-problems/>.

<sup>23</sup> Sheehan, Matthew, "How China's Massive AI Plan Actually Works," *MacroPolo*, 13 February 2018, accessed 15 September 2018, <https://macropolo.org/chinas-massive-ai-plan-actually-works/>.

China,<sup>24</sup> set up largely at the provincial and city level, aiming to raise subsidiary funds with an aggregate fundraising total of RMB 5.3 trillion (Euro 671 billion)<sup>25</sup>. While not aimed exclusively at spurring innovation in technology, a large number of these funds are aimed at areas such as big data, high-tech manufacturing, chipsets, etc.<sup>26</sup> Governments have long attempted to play a role in stimulating innovation, the major rationale being that private firms may under-invest in R&D activities. GGFs are unique to conventional government efforts to stimulate innovation in that apart from grants or subsidies, they invest in companies, taking an equity share. There is very little evidence or any publicly available impact assessments on whether these GGFs are an efficient use of State capital and are able to spur innovation, or whether this public capital is simply crowding out private investors rather than creating an additionality effect, or whether capital is truly being deployed to high-risk areas with low private returns. GGFs are a tool in China's attempts to build up a commercially viable indigenous semiconductor industry, a sector notorious for its extremely high market-entry barriers and high-risk capital investment, and some of the largest GGFs are especially prominent here, such as Guangdong Integrated Circuit Industrial Investment Fund, Shanghai Integrated Circuits Industry Investment Fund (RMB 50 billion/Euro 633 million), and China State-Owned Assets Venture Investment Fund (RMB 200 billion/Euro 2.5 billion), which is an investor in Cambricon, a unicorn chipset manufacturer. Time will tell as to how successful these State-led efforts are at growing the ecosystem and spurring innovation. So far, no GGF has made a successful exit.

In November 2018 the Ministry of Industry and Information Technology (MIIT) announced an open call for applications via a website, <http://www.aibest.org.cn>, for companies from across the country, with the goal to select a maximum of five companies from 17 distinct technical areas to “break bottlenecks in AI development, set up industry benchmarks, cultivate an innovation development army, and accelerate national AI industry development, and deepen integration with the

---

<sup>24</sup> He xie and Peng, 何杰 彭兴庭. 政府引导基金运行中存在的三大矛盾五大风险, Hexun, 11 August 2017, accessed 29 December 2018, <http://funds.hexun.com/2017-08-11/190401279.html>.

<sup>25</sup> “China's \$798B Government Funds Redraw Investment Landscape, Here Are The Largest Funds You Must Know,” China Money Network, 31 October 2017, accessed 1 November 2018, <https://www.chinamoneynetwork.com/2017/10/31/chinas-798b-government-funds-redraw-investment-landscape-largest-funds-must-know>.

<sup>26</sup> Ibid.



real economy”<sup>27</sup>. This effectively creates a national team of AI champions, presumably alongside Baidu, Alibaba, Tencent, iFLYTEK and SenseTime, handpicked by the Ministry of Science and Technology to develop open innovation platforms in four areas<sup>28</sup>.

Yet, if this top-down approach to building the ecosystem may lean more towards waste rather than innovation and efficiency, or stifle market competition, China’s approach towards adopting technology, which Lee Kaifu classifies as techno-utilitarian, may serve to give China a competitive advantage compared to Western countries in developing AI. This is already visible with the speed with which the government has moved to adopt AI in government services as outlined above. This can also be extended to Chinese consumers, who are known to be quick adopters of new technologies, for instance, digital payments or bike sharing, with concerns about privacy a much lower priority. Can this lead to a first mover advantage in AI?

It is illustrative to home in on specific industries or domains. Autonomous driving is a case in point. The first company to go to market may not be the one that is the first to develop the technology but the one that operates in a country that is the first to develop a nation-wide regulatory framework that allows autonomous vehicles to legally drive on the road. An interesting example here is the New Xiongan District being built in Hebei province, 80 miles outside Beijing. Among many novel features, the Chinese government, in partnership with Baidu, builder of Apollo, an open source platform for autonomous vehicles, used by BMW and Bosch, plans to build a road system designed for autonomous vehicles<sup>29</sup>. Another important area which requires not just technology but a strong private-public partnership is urban governance. For instance, Alibaba Cloud’s City Brain, currently being tested in cities such as Hangzhou and Suzhou, is among the global leading platforms enabling the creation of Smart Cities through the collection of data and real-time insights.<sup>30</sup>

---

<sup>27</sup> MIIT, 新一代人工智能产业创新重点任务揭榜工作方案, “Work plan for key projects for the development of next generation of AI,” 11 November 2018, accessed 27 November 2018, <http://www.miit.gov.cn/n1146295/n1652858/n1653018/c6492065/content.html>.

<sup>28</sup> “SenseTime Becomes the ‘National Open Innovation Platform for Next-Generation Artificial Intelligence on Intelligent Vision’”, 9 September 2018, accessed 27 November 2018, <https://www.sensetime.com/news/719.html>.

<sup>29</sup> USA, LLC Baidu, “Baidu and Xiongan New Area Sign Strategic Agreement to Develop Smart City,” GlobeNewswire News Room, 20 December 2017, accessed 25 September 2018, <https://globenewswire.com/news-release/2017/12/20/1267217/0/en/Baidu-and-Xiongan-New-Area-Sign-Strategic-Agreement-to-Develop-Smart-City.html>.

<sup>30</sup> <https://www.alibabacloud.com/et/city>.

Ultimately this brings the discussion to the fundamental questions of how societies approach AI and the values it wants to build into the technology, which are informed more by the socio-political DNA of a culture than by the technology itself.

## GOVERNANCE AND PRIVACY: IDEAS AND APPROACHES

Discussions about ethics, societal impact, future of work, and governing algorithms are increasingly becoming a part of the global AI discourse. These are difficult futuristic questions with no easy answer and China is not different in this case. And just as in most countries, the Chinese people too are most concerned about job losses and societal risks. At the recently held World AI Conference in Shanghai, President Xi Jinping raised the need to “develop laws, safety, employment, ethics, and governance of AI from all aspects” and noted that this would “require deep cooperation with all countries”<sup>31</sup>. Jeffrey Ding, a researcher at the Future Humanity Institute in Oxford, notes that, the world needs to shift its attention from whether China is having these discussions to what the substance of the discussions are.

In China, questions about ethics, unlike in most democracies, are not framed around the individual but instead the collective. In an interview with this author, Rogier Creemers explains: “China does not share those concerns [of the West] because its ‘OS’ [operating software] is not built on the State as the facilitator of the individual good, which lies at the heart of the liberal democratic idea of the State and citizenship....So the question about algorithms in China is very likely not going to be about whether they violate anyone’s specific individual rights or not, but rather, whether or not they contribute to the solution of the identified socio-economic problems. This is where the question of fairness might get a look in: not from an identity or class-based perspective, but more from a classically Leninist approach.”<sup>32</sup>

China too is looking both inwards and also outwards for values and a philosophical framework to approach AI. Professor He Huaihong, a professor of Chinese philosophy at Peking University, has argued that China needs to rebuild its social ethics based on Confucian values in the face of rapid changes and developments in

---

<sup>31</sup> The Paper, “习近平致2018世界人工智能大会的贺信 (Xi Jinping Address at WAIC),” [https://m.thepaper.cn/newsDetail\\_forward\\_2448320](https://m.thepaper.cn/newsDetail_forward_2448320), 20 September.

<sup>32</sup> Lewis, Dev, “Dev Lewis,” Digital Asia Hub, 14 August 2017, accessed 15 September 2018, <https://www.digitlasiahub.org/2017/08/14/interview-with-dr-roger-creemers-ai-social-credit-algorithmic-governance-cybersecurity-vpns-cross-border-dataflows/>.

Chinese society<sup>33</sup>. Baidu became the first Chinese company to join the Partnership on AI while other companies are increasing their efforts to engage with leading American and European research institutes.

The issue of data protection and the need to balance it with the needs of data-hungry Machine Learning systems is also a fundamental pain point. China has long been a thriving ground for data theft, enabled by lax data protection standards and a population (and government) still unaware or unable to stem the tide. The Cybersecurity Law (2017), which is now more than a year in implementation, places strict restrictions on the flow of cross-border data as well as sets higher data protection standards, the effect of which is already being seen with violating companies being flagged. China's main standards body also passed the Personal Information Security Specification (not a binding law), said to have been modelled on the European Union's General Data Protection Regulation (GDPR)<sup>34</sup>, which raises the bar for Chinese companies to protect their users' data, given rising concerns about misappropriation of personal information by the private sector. The law also seeks to create a framework for managing data with the rise of smart cities and big data systems.

How to balance the need to innovate with the need to protect personal data? A commentary published by the *People's Daily* captured the dilemma as such: "The updating and iteration of technology is an important force pushing forward societal progress, and people should not 'give up eating for fear of choking' because of privacy issues, but the development of artificial intelligence also cannot come at the cost of sacrificing privacy"<sup>35</sup>.

## CONCLUSION

In just a short span of time, China has begun to channel a significant amount of capital to seed the building of a commercial ecosystem and to spur the adoption of AI in several industries, including government services. This has seen China dominate recent global investment in AI as well as contribute to the second-most number of

---

<sup>33</sup> Ding, Jeffrey, "How China Seeks to Govern AI," Medium, 5 September 2018, accessed 15 September 2018, <https://medium.com/@ChallengesFnd/how-china-seeks-to-govern-ai-baf1c0cd1a54>.

<sup>34</sup> "China's Emerging Data Privacy System and GDPR," China's Emerging Data Privacy System and GDPR | Center for Strategic and International Studies, 23 October 2018, accessed 1 November 2018, <https://www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr>.

<sup>35</sup> Caiyinghao, 蔡映洁, *People's Daily*, 27 August 2017, accessed 15 September 2018, <http://opinion.people.com.cn/n1/2017/0823/c1003-29487792.html>.

AI companies across the world, with this trend looking to continue into the next few years as a number of Chinese unicorn companies grow and mature. The number of AI patents filed by China is rising fast<sup>36</sup>, as are academic papers published by Chinese researchers. However, as China's own AI plan, which looks more than a decade to 2030, suggests, the "AI race" is more a marathon than a sprint, with several fundamental issues that will need to be addressed, as much in the realm of politics as in the laboratory.

There are two critical winds of change in international relations. First is the unmistakable convergence between technology and politics. Technology companies and their platforms are impacting elections and national discourses, the scale and real-world impact of cybersecurity attacks continues to rise, and governments are moving to create laws and frameworks to set governance standards that reframe how people use technology. China is a major actor in each one of these areas. This is intertwined with the second critical trend – China's rise as the second largest economy and challenger to the United States-led order. The geopolitical shifts and political decisions made by countries and societies will shape the future technology leadership.

This issue is already flaring up as 5G technology edges closer to commercialisation. The Chinese company Huawei has emerged as a leader in developing the technology; yet, it is facing resistance in many important countries, with Australia recently banning Huawei from participating in the bidding of its national 5G networks, and the US unambiguously urging its allies to do the same<sup>37</sup>. The opaque relationship Chinese companies have with the State has been a long-standing national security concern for many countries, further amplified by an uptick in CCP branches set up within technology companies<sup>38</sup>, or new laws such as the Cybersecurity Law (2017), which requires Chinese companies to share data and open up source codes under the pretext of national security. At this moment Germany has set up a cybersecurity lab to exclusively review Huawei's source code before it is given the green light to bid in Germany's 5G network infrastructure build-out. The outcome of this process will have a significant say on whether Chinese telecommunication compa-

---

<sup>36</sup> Huang, Echo, "China Has Shot Far Ahead of the US on Deep-learning Patents," Quartz, 2 March 2018, accessed 25 September 2018, <https://qz.com/1217798/china-has-shot-far-ahead-of-the-us-on-ai-patents/>.

<sup>37</sup> *Wall Street Journal*, "Washington asks allies to drop Huawei," accessed 27 November 2018, <https://www.wsj.com/articles/washington-asks-allies-to-drop-huawei-1542965105?tesla=y>.

<sup>38</sup> Chen Qin Ching, *People's Daily*, "Technology companies strengthen CPC committee role in management, development," 21 November 2018, accessed 27 November 2018, <http://www.globaltimes.cn/content/1128433.shtml>.

nies are able to build 5G networks in major developed countries. Which leads to the next question: Can Chinese technology companies truly become global giants without truly being global or catering to developed countries?

The domination of Chinese companies is still mostly felt only within China's borders. With the exception of Southeast Asia, Chinese internet companies have a negligible global presence compared to their American counterparts. Many have begun going global, but like their counterparts in energy and infrastructure, are focused on catering to emerging markets. Chinese AI companies will struggle to match American giants like Google, Facebook, and Amazon, without access to data from around the world. This brings the discussion back to China's competitive advantages and innovative capabilities.

Can China make breakthroughs in fundamental research, whether in AI or technologies such as Quantum computing? China is spending large amounts on research and development, including in Quantum computing, but there are few quantitative assessments that suggest that this funding is significantly pushing the innovation needle forward. Despite becoming one of the world's leading filers of patents, both domestically and internationally, evidence suggests that a large percentage of these patents are not leading to commercial use and are not renewed. Research ecosystems and university systems in Western Europe and the US are still the benchmark for research and attract the world's best talents.

All these questions reflect the complexity around assessing AI and indicators of its success. China's size, economic power, and ambition suggest that it has the important characteristics to be a very important power in the AI realm. China may come to lead in several industries, as it does now for example in mobile payments, but it may not necessary result in Chinese companies taking this technology to the rest of the world. Any deterministic claims of global dominance are off the mark and still too early, with many future flash points around technology, politics and economics that may affect this. As are claims about the kind of society that China wants to build for itself using AI. The Chinese society is still relatively new to digitisation and faces similar problems that many other societies do when negotiating its relationship with technology. China's AI ecosystem will be a product of China's domestic political system and economic realities and therefore unlikely to look like the West. Yet there will be lessons and models from China's approach that will be valuable for ecosystems around the world and it is important that these differences do not prevent an open exchange of ideas and discourses and that China is allowed to play its role in the global decision making on the future of AI.

**Table 1**

Policy	Agency	Content	Year
Make in China 2025	China State Council	Push forward Smart Manufacturing	May 2015
Guiding Opinions concerning Vigorously Moving Forward the "Internet Plus" Plan	China State Council	AI as one of Internet Plus' 10 Key Points	July 2015
Outline of the 13th Five-Year Plan for the National Economic and Social Development of the People's Republic of China	China State Council	Includes AI in the Outline	March 2016
"Internet Plus" and AI: 3 Year Implementation Plan	National Development and Reform Council (NDRC)	Pushing for development of AI applications	May 2016
13th Five-year Plan for Scientific and Technological Innovation	China State Council	Development of AI-based methods driven by big data	July 2016
Government Work Report (2017)	China State Council	AI enters into the government work report for the first time	March 2017
New Generation Artificial Intelligence Development Plan	China State Council	Three-phase plan for China to become the world's leading AI innovation centre by 2030	July 2017
3-Year New Generation Artificial Intelligence Development Implementation Plan	Ministry of Information Industry and Technology (MIIT)	Action plan for integrating AI into the real economy	December 2017

Source: 北京人工智能产业发展白皮书 Beijing AI Development White Paper, Beijing Municipal Government, [http://www.sohu.com/a/238841203\\_473283](http://www.sohu.com/a/238841203_473283), accessed June 2018.

**Dev Lewis** is a Yenching Scholar at Peking University and a Research Associate at Digital Asia Hub. His research focus is on the intersection between technology, society, and politics, in China and India. He previously held roles at Infosys China, an IT services and consulting MNC, and Gateway House, a foreign policy think tank. He has a degree in International Relations from Roger Williams University, and studied Mandarin at East China Normal University and Zhengzhou University.



# Social Credit System in China

*Chris Fei Shen*

## INTRODUCTION

The Chinese government has long been seeking to harness the economic benefit of information technologies while using the same tools to maintain political and social stability. The ambitious plan for developing an all-encompassing social credit system resembles a similar attempt: to make use of big data technologies to create a society where individuals, enterprises, and the government all act with integrity so that a thriving economy and a stable regime become possible. The plan has no equivalent elsewhere in the world. Whereas Western societies use financial credit scores to motivate people to maintain good credit records, the Chinese social credit system extends from finance to almost all areas of social life. Plus, the Chinese system intends to include not only individuals, but also enterprises, government branches, and non-government organisations.

Chinese people are paying increasing attention to the topic of social credit. Over the years, the domestic media in China has mostly covered the topic with a positive perspective. Yet the media outside China tend to depict the social credit system as a draconian mass surveillance project driven by almighty technologies to curtail personal freedom. A few telling examples of headlines are: “The odd reality of life under China’s all-seeing credit score system”,<sup>1</sup> “China has started ranking citizens with a creepy ‘social credit’ system”,<sup>2</sup> and “China’s social credit system fuels authoritarian regime”<sup>3</sup>. Google’s search trend tool, Google Trends, suggests that the most closely related keywords to China’s social credit system is “Black Mirror,”

---

<sup>1</sup> <https://www.wired.co.uk/article/china-social-credit>.

<sup>2</sup> <https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4>.

<sup>3</sup> <http://www.atimes.com/chinas-social-credit-system-fuels-an-authoritarian-regime/>.



a British sci-fi television series that examines the unintended eerie consequences of technologies. With China being perceived as an authoritarian regime ruled by a single party, negative media speculations about the plan are not without reasons; however, they do not represent a comprehensive picture of the proposed social credit plan. A closer look at the system first demands attending to the original government documents to uncover the meanings behind the texts.

## TWO GOVERNMENT DOCUMENTS

There are two important government regulatory documents that defined the top-level design of the social credit system. As early as 23 March 2007, the State Council issued a notice entitled “Opinions of the General Office of the State Council concerning the Building of a Social Credit System.”<sup>4</sup> The document highlights the urgent need to create a social credit system for maintaining a “socialist market economy” given widespread commercial fraud, tax evasion, product piracy, and evasion or abolition of debts to banks in bad faith. On 14 June 2014, the State Council issued another document: “State Council Notice concerning Issuance of the Planning Outline for the Construction of a Social Credit System (2014–2020).”<sup>5</sup> Compared to the 2007 State Council document, the 2014 document lays out a more detailed picture about building a unified social credit system.

While the 2007 document primarily focuses on a finance credit system, the 2014 document extends to other areas of government regulation. The lack of trustworthiness happens at all levels of Chinese society: shoddy products, irresponsible medical treatment, and poisonous milk powder, etc. It is possible that the government realises that the root cause of financial fraud lies in the low awareness of keeping trust in general and the low cost of breaking trust and integrity, and has therefore rolled out a comprehensive plan for building a “reputation society” (*xinyong shehui*), meaning that everyone in the society should keep trust and integrity.

In addition, the 2014 document sets a timeline with clearly defined goals. The stated objectives are: by 2020, to establish fundamental laws, regulations, and standards for social credit, to construct a credit information system that covers the entire society, to build credit supervision and management systems, to foster a social credit service market, and to enforce reward and penalty mechanisms for keeping trust and breaking trust so that they play a full role in encouraging honesty and integrity. The overall framework of this huge project will be laid out by the

---

<sup>4</sup> [http://www.gov.cn/zwggk/2007-04/02/content\\_569314.htm](http://www.gov.cn/zwggk/2007-04/02/content_569314.htm).

<sup>5</sup> [http://www.gov.cn/zfwj/2014-02/10/content\\_2581766.htm](http://www.gov.cn/zfwj/2014-02/10/content_2581766.htm).

government, but all social organisations will contribute their share in carrying out the plan.

## **FOUR AREAS OF SINCERITY BUILDING**

Under the framework of the social credit system, the 2014 document lays out a very comprehensive working plan. There are four proposed important areas that are needed to develop social integrity and a social credit system: government affairs, commerce, social service domains, and the judicial system.

With regard to government affairs, the proposal encourages government branches to adopt various types of social credit products in its work. Civil servant credit dossiers were proposed to record annual reviews and acts such as violating laws and regulations.

With regard to commerce, a large number of industries are mentioned in the outline. For example, for manufacturing industries, a product quality credit system was proposed, to be connected with the current 12365 product quality complaint hotline platform. For trading and service businesses, it is proposed to develop a company credit system. For the financial industry, more individual and institutional financial activities are proposed to be recorded. For taxation, more information on taxpayers, including trading and asset ownership, need to be collected and verified. Similar plans were mentioned for other business sectors such as construction, government procurement, tendering and bidding, traffic and transportation, e-commerce, statistics, exhibiting and advertising, etc.

With regard to honesty and integrity building in the social service domains, healthcare, social security, labour and employment, education and academic research, culture sports and tourism, intellectual property, environmental protection and energy saving, non-government organisations, and internet applications and services are mentioned as the areas where severe problems in integrity exists and different types of database or blacklist systems will be set up. In particular, a job-related integrity record system will be constructed for people such as public servants, enterprises' legal representatives, lawyers, accounting employees, registered accountants, statist employees, registered tax advisors, auditors, evaluators, insurance brokers, medical personnel, teachers, scientific research personnel, patient service employees, project managers, news and media employees, and tourist guides, etc.

With regard to judicial credibility, the court system, prosecutorial system, public security system, and judicial and administrative system are required to further move forward with information openness so as to safeguard the public's right to

know and to carry out “sunshine law enforcement” so that the public will place more trust in these institutions.

## **PURPOSES AND MOTIVATIONS BEHIND THE SYSTEM**

A brief look at the two government documents suggests that the social credit system is a gigantic mixture of tools that aim to serve multiple purposes: to shape citizens’ and institutional behaviour, to push forward government transparency, and subsequently to reduce transaction costs incurred by a low-trust society. At the core of the plan lies the key of reputation building or sincerity development. “Xin” (信), credit or reputation or trust, is a quintessential concept in Confucius thought. But in contemporary China, dishonest behaviours trying to take advantage of loopholes in laws and regulations are rampant at different levels of society. The social credit plan could be seen as a tool introduced by the party to cure the social ills of low trust with a good intention but with potentially unpredictable results. Observers who see this as a surveillance plan tend to focus their attention on the technical details of data collection, while losing sight of its overall purpose (of course, the extent and method of data collection is controversial and disputable). As a matter of fact, only one tiny paragraph in the long document touches upon credit system development regulating internet use. After all, the party has already developed a very complicated internet censorship system employing technical, legal, and administrative tools. Therefore, the primary motivation behind creating a social credit system seems to be more economical and social than political.

## **KEY FEATURES OF THE PLAN**

According to the 2014 plan, the social credit system has three important features. First, it is not a single system monopolised by the government. The 2014 proposal points out that the primary principle of the social credit system is that it is “led by government, but built by the society.” In other words, the government wishes to develop a social credit ecosystem with pluralistic products and services. However, deriving an overall social score is technically possible assuming that all data systems are connected. Second, the document highlights the role information technologies will play in building a social credit system. The use of information systems to record and curate credit information is encouraged for different industrial sectors and for different government branches. The plan also suggests the establishment of credit information exchange and sharing mechanisms. Without doubt, this could be the world’s largest data collection effort. Third, the document points out that rewards

and penalties are the keys to making the social credit system work; however, the text regarding rewards and penalties is very vague and brief. The specifically mentioned rewards include praising through media reporting, service priority, and expedited processing for government services. As for penalties, social moral condemnation, blacklisting, and market withdrawal mechanisms are mentioned for individuals and organisations.

## EXISTING NATIONAL SYSTEMS

The two regulatory documents only provide a framework and guiding principles for constructing a unified credit system. There is no existing unified social credit system in China. But there are credit services that have existed long before the unified social credit plan was mooted. One of the official and most important credit service providers is the Credit Reference Center of the People's Bank of China. As its name suggests, the credit report issued by the Reference Center only covers finance-related activities. The two main services provided by the center are individual credit reference reports and enterprise reference reports. Both databases were developed in the 1990s and the services went online in the 2000s. As of 2015, the center's database includes 860 million individuals and 20 million institutions.<sup>6</sup> Individual credit reports contain information such as personal loan and mortgage, credit card use, delayed payment record, civil judgment record, unpaid utility fee, administrative penalties, etc.<sup>7</sup> Obviously, the data sources of the Reference Center include banks, courts, and other government branches. Unlike most credit score products in Western societies, the credit reference reports do not derive a holistic score for individuals and enterprises.

A second important credit database that has some overlap with the Reference Center system is hosted by the Supreme People's Court: the dishonest individuals or enterprises subject to enforcement database.<sup>8</sup> In 2010, the Supreme Court issued a notice to limit the spending of individuals and organisations that refused or evaded their legal obligations. For individuals, they are subject to a ban on traveling on business class or above in flights, trains, and cruises, on purchasing real estates, and on staying in luxury hotels, etc.<sup>9</sup> According to statistics from courts at different levels, more than 70 percent of individuals or organisations tried to evade

---

<sup>6</sup> <http://www.pbccrc.org.cn/zxzx/zxgk/gywm.shtml>.

<sup>7</sup> <http://www.pbccrc.org.cn/zxzx/grzx/201401/2141558a28cd4f8dae8e2a6e70728210.shtml>.

<sup>8</sup> <http://shixin.court.gov.cn/index.html>.

<sup>9</sup> <http://www.court.gov.cn/shenpan-xiangqing-1650.html>.

enforcement and failed to perform obligations determined in an effective legal instrument. Thus, the government decided to create a blacklist system in 2013 to publicly name those who refuse to comply with court judgments.<sup>10</sup> The database is publicly accessible. Users can search for cases by individual or institutional name. In 2013, the Supreme Court also signed a memorandum with the Credit Reference Center of the People's Bank of China to incorporate the court's records into the unified social credit scheme.<sup>11</sup> In 2015, the spending limit decision was further revised. One of the revisions is to add a ban on travelling on high-speed railways with codes starting with "G".<sup>12</sup> The carrot-and-stick system that was implemented has shown effect in terms of settling long-outstanding debts.

A third government branch that collects massive amounts of individual data is the railway authorities. In 2017, the railway management authorities issued a document entitled "Railway Passenger Credit Record Management Method".<sup>13</sup> The regulation listed a number of dishonest or indecent behaviours that will be recorded by the database: endangering the security of railway transportation, smoking on high-speed trains, fraudulently purchasing and reselling tickets, selling fake tickets, using fake or other people's identity documents, using outdated tickets, taking a train without tickets and refusing to purchase tickets, etc. The records will be retained for five years.

There are many national-level government social credit-related systems (e.g., administration of taxation),<sup>14</sup> but the three mentioned above have received the most attention due to their visible penalties and heavy domestic news coverage.

## LOCAL-LEVEL SOCIAL CREDIT PILOTS

In response to the 2014 proposal, many provinces and cities have outlined their own local social credit plans or carried out their own social credit pilots. The pilot projects differ vastly in terms of their foci, which to some extent is a reflection of governance philosophy differences across local governments in China.

Some took a more incremental approach and placed more emphasis on government data transparency and data sharing. For instance, the Shanghai municipal

---

<sup>10</sup> <https://www.chinacourt.org/article/detail/2013/07/id/1038223.shtml>.

<sup>11</sup> <http://www.court.gov.cn/zixun-xiangqing-5968.html>.

<sup>12</sup> <https://www.chinacourt.org/law/detail/2015/07/id/148347.shtml>.

<sup>13</sup> <http://yuandiancredit.com/h-nd-1693.html>.

<sup>14</sup> <http://www.chinatax.gov.cn/n810219/n810744/n1672963/n1672968/c1673941/content.html>.

government issued a plan for social credit development in 2016 echoing the national plan.<sup>15</sup> The plan lists out a number of aims to achieve by 2020: all for-profit and non-profit institutions will be assigned a social credit number; all administrative approvals or penalties will be made available online in seven days; more than 600 categories of information need to be shared on the government social credit platform for governance transparency, etc.

Some other projects focus on assigning labels and scores to institutions and individuals. As an economically less-developed province, Guizhou has been trying to beat other provinces in terms of its social credit programme development. Qingzhen, a city in Guizhou, claimed that the city has evaluated 149,758 village households, consisting of 99.95 percent of its total households. An award system was further set up to give honorary titles to those households with high credit scores. Among them, 7,027 are considered as one-star households, 7,766 are two-star households, 3,619 are three-star households; 1,324 are four-star households; and 1,355 are five-star households.<sup>16</sup>

A similar pilot comes from Rongcheng, Shandong Province. Rongcheng is one of the twelve social credit development “model” cities.<sup>17</sup> Rongcheng’s social credit pilot system includes all types of individuals and organisations. To assign unique numbers to individuals and organisations, Rongcheng’s social credit system makes use of existing identifiers from different sources. The individual resident database uses the national identity number as the identifier; the government and party organisation database uses the organisation number as the identifier; the enterprise database uses the Unified Social Credit Number as the identifier; and the village social credit database uses the geographical administration code as the identifier. In addition, the Rongcheng model has a high coverage rate. All permanent residents, non-permanent residents, self-employed individuals, enterprises, social organisations, and villages are included in its database. Moreover, the Rongcheng model designed a comprehensive “social credit related information list”.<sup>18</sup> The list claims to cover all social and economic activities. But it seems the list and the method to evaluate individuals and organisations are not publicly available.

---

<sup>15</sup> <http://www.shanghai.gov.cn/nw2/nw2314/nw2319/nw12344/u26aw50043.html>.

<sup>16</sup> <http://www.hzcx.gov.cn/article/xinyongzixun/chengxinxinwen/1069.html>.

<sup>17</sup> [http://m.ce.cn/bwzg/201801/09/t20180109\\_27650515.shtml](http://m.ce.cn/bwzg/201801/09/t20180109_27650515.shtml).

<sup>18</sup> <http://xinhua-rss.zhongguowangshi.com/13701/6003014383535113117/2049163.html>.

## NEW FORMS OF FINANCIAL CREDIT SYSTEMS

New social credit products introduced by big internet companies have emerged in recent years. The best-known case is Sesame Credit (Zhima Credit). Many people outside China mistakenly consider Sesame Credit to be *the* social credit system. In fact, Sesame Credit is only a private credit score system developed by Ant Financial Services Group (an affiliate of the Alibaba Group). The Sesame Credit programme was started in 2015 but the data of Sesame Credit primarily come from Alibaba's Alipay, which was launched in 2003. Data generated on the Alipay platform include loan, payment, shopping, and insurance records.

Technically speaking, Sesame Credit is a functional component embedded in Alipay, a third-party online payment platform. Currently, there are about 520 million users of the service.<sup>19</sup> Sesame Credit does provide a score for individual users. The score ranges from 350 to 950, with five categories: super (700-950), excellent (650-700), good (600-650), okay (550-600), and not so good (350-550). The score derives from five dimensions: credit history, fulfilment capacity, personal characteristics, behaviour and preferences, and interpersonal relationships.

No specific explanations are provided by Alipay as to how a concrete score is calculated by records coming from the five dimensions. It seems that credit history, fulfilment capacity, and behaviour and preferences data come from one's transaction data on Alipay. Personal characteristics data are optional and completed by the users themselves. They include education level, driver's license, and vehicle registration information, etc. The last category, interpersonal relationships, sounds somewhat scary and weird. It implies that if you have good-credit-score friends then you will be a good individual as well. Conversely, if your social network is filled with low-trustworthy friends, then your score will be lower. (Alipay has a social media function designed into the app but it is not as popular as Tencent's WeChat.) However, the algorithms are not transparent. As for rewards and penalties, a high Sesame Credit score could lead to deposit-free rental services provided by third-party companies, including shared bike, car rental, apartment rent, etc. But Sesame Credit is a rather commercialised programme, to the extent that many of its claimed high-credit-score individual "benefits" are actually services and products offered by other companies that run promotions and marketing campaigns on Alipay. Another benefit is that high-Sesame-Credit-score individuals can apply for travel visas without being required to provide too many documentation proofs for destinations such as Singapore. In addition, a high Sesame Credit score could mean higher loan

---

<sup>19</sup> [http://www.xinhuanet.com/fortune/2018-01/03/c\\_1122206175.htm](http://www.xinhuanet.com/fortune/2018-01/03/c_1122206175.htm).

and credit limits from Ant Jiebei and Ant Huabei respectively, both of which are Ant Financial Services Group's services.

Sesame Credit is just one case among many. In 2015, the government decided to open up the market for private companies' individual credit services and products. Eight companies, including Sesame Credit and Tencent Credit, were invited to apply for formal licenses. Nevertheless, two years later, in 2017, none of the companies were considered to be qualified.<sup>20</sup> In other words, currently in China, there are no private companies providing individual social credit services with a formal license. The Internet Finance Association set up by the central bank is the only company with a license to launch a credit scoring business.

## PROBLEMS AND CONTROVERSIES

China's social credit system is plagued by controversies and problems. Even the Chinese authorities are aware of it. The rejection of all pilots privately run financial credit programmes in 2017 is a case in point. The director of the Credit Reference Center, People's Bank of China mentioned three reasons for the rejection.<sup>21</sup> First, all eight products' data are derived largely from customer transactions on their respective platforms. Data-sharing mechanisms are not in place, which could lead to inaccuracy. Second, all eight products lack third-party independence, which could lead to conflicts of interest. Third, all eight companies lack knowledge about credit reference. They derive credit scores from very limited data, which could potentially be highly biased.

It is important to point out that the credit reference (“征信”) system and the social credit (“社会信用”) system are two different but related concepts. Credit reference covers a smaller range of activities that strictly deal with money, and is regulated by the People's Bank of China. The nature of financial credit reference demands higher accuracy. But the social credit system covers all types of social activities and could be regulated by different government bodies.

In contrast to the credit reference privatisation programme which has progressed slowly, the development of the social credit system seems to be much faster and has operated in a decentralised fashion. Different local governments invented different pilot programmes and plans, some of which were to impress the central government with their “achievements”.

---

<sup>20</sup> <http://finance.caixin.com/2017-04-22/101081924.html>.

<sup>21</sup> <https://www.yicai.com/news/5271750.html>.



Despite the fact that the 2014 State Council proposal lays out a detailed plan, the proposal invites more questions and controversies than provides answers.

First, strict data regulation complicates the collection and sharing of data, which constitutes the fundamental basis of a social credit system. Over the past few years, cases of data misuse and abuse have helped to raise public demands for data protection. Recently, China's data privacy law extended its reach. In 2017, the Standardisation Administration of China issued a new regulation on protecting personal information.

Second, constructing a nationwide comprehensive social credit database is not impossible, but numerous barriers stand in the way of data sharing. On the one hand, technical challenges are easily foreseeable. How will different organisations adopt the same data format so that information can be transferred across institutions? Currently, there is no central government body for standardising and managing the vast volumes of data. On the other hand, resistance due to economic concerns are also possible. Getting companies to share their data with the government might be difficult to achieve. Companies have almost no incentive to share their data with the government because it is one of their most valuable assets. Currently, only public security bureaus can request for data from enterprises through appropriate procedures. But how this will work out with regard to the social credit system remains vague and unknown.

Third, if a large social credit system comes into existence, the scale of the data security problem that the government faces is immeasurable. A database with such rich information would definitely attract all forms of attack. Even if the system can fend off all external attacks, leakage from within the system is highly possible. China has a huge black market for the buying and selling of personal information that comes from personnel who work in the institutions producing the data.

Fourth, the same reason that the People's Bank of China mentioned for rejecting the private company credit reference service license applications applies to the social credit system as well, that is, how will the government run the social credit system in an impartial way like a third-party actor? Despite the 2014 State Council plan calling for more government transparency to enhance government credibility, ironically, some of the social credit pilot programmes themselves lack transparency. For instance, detailed information with regard to how Qingzhen and Rongcheng assigned scores to individuals and organisations is not available online.

Fifth, and relatedly, when transparency is not in place, fraud and manipulation of the system could fail the mission of China's effort to build a reputation society and reputation government. In simple terms, the social credit system would not be very credible without checks and balances. There are numerous cases where the

central government tries to implement a new policy with good intentions but local governments carry out the policy with different forms of distortion for their own benefit. Following this line of reasoning, it is possible that social credit programmes could be used to limit personal freedom, including freedom of speech.

## CONCLUSION

The social credit system is a complex nationwide system envisioned by the Chinese government. It is a tool to push forward government transparency and to enhance the credibility of the whole society. Theoretically speaking, a well-designed social credit programme with transparency, checks and balances, and public deliberation could lead to a thriving economy and a better society. But, given the scale of the plan, the future of the social credit system remains largely unknown due to the technical, legal, and administrative problems the Chinese authorities face.

**Dr. Fei Shen (“Chris”)** is associate professor at the Department of Media and Communication, City University of Hong Kong. He is a keen observer of the social and political impacts of new media technologies. His empirical work examines how people make use of new media technologies in different settings and how the internet helps reshape people’s behaviour and redistribute power in societies.



# China's Tech Giants: Baidu, Alibaba, Tencent

*Hong Shen*

## WHO ARE THE BATS?

With the rise of a group of powerful internet companies – especially the BATs – the Chinese internet has become the centre of global attention.

Who are the BATs? This seemingly simple question turns out to be surprisingly difficult to answer. Referring to Baidu, Alibaba, and Tencent, the BATs are the three most powerful companies providing web applications in China. Originated in search (Baidu), e-commerce (Alibaba), social media and mobile gaming (Tencent), all three tech conglomerates started their businesses in the late 1990s or early 2000s. Twenty years later, they each occupy a dominant position and enjoy a near monopoly in their respective areas. With market values of \$484 billion (Alibaba), \$447 billion (Tencent) and \$89 billion (Baidu) as at the middle of 2018, they have entered the club of the world's most valuable tech companies, sharing the same stage with American tech giants like Apple, Amazon, Alphabet, and Facebook.<sup>1</sup>

The BATs are more than just search, e-commerce or social media companies, however. Over the past two decades, they have each developed an extremely complicated digital empire, extending their tentacles into almost every aspect of China's political economy. Take Alibaba as an example. Although in its 2014 initial public offering (IPO) prospectus, the company described itself as "the largest online and mobile commerce company in the world",<sup>2</sup> e-commerce, however, appears to be only the "tip of the iceberg" of its now eclectic empire. Alibaba's massive corporate system constitutes not only its core in commerce (both online and offline), but also the supporting layer of logistics, payment and finance, cloud computing

---

<sup>1</sup> Jeff Desjardins, "Tech's 20 Largest Companies are Based in Two Countries," 9 July 2018, *Business Insider*, <https://www.businessinsider.com/techs-20-largest-companies-are-based-in-2-countries-2018-7>.

<sup>2</sup> Alibaba Group, SEC Form F-1/A, 100.

and consumer services, and the outermost layer that extends from media and entertainment to healthcare and even automobile manufacturing. Its multifunctional mobile payment app Alipay (now part of Ant Financial, an Alibaba-affiliated financial company), commands 600 million users.<sup>3</sup> In a similar vein, Tencent has also developed its mega app, WeChat, combining functions from messaging and social networking to mobile payment, wealth management and even public services – including paying public utility fees or applying for travel visas. In March 2018, it hit 1 billion monthly active users.<sup>4</sup> Baidu, on the other hand, has accelerated its growth in the emerging field of Artificial Intelligence, including developing voice assistants and driverless cars.<sup>5</sup> In sum, by the end of 2018, all three internet companies have not only consolidated their core businesses in search, e-commerce and social networking, but have also evolved into multifaceted tech platforms.

## THE FORCES BEHIND THE RISE OF THE BATS

How have the BATs constructed such massive digital empires in the past two decades? What are the factors behind their success? There are three potential forces.

First, the three Chinese web conglomerates are rooted in the world's largest online market, which has been – at least partially – shielded by the so-called “Great Firewall”. In 2017, China was home to 772 million internet users – more than Europe's total population.<sup>6</sup> Every day, those 772 million netizens will search the web using Baidu, send messages through WeChat and buy things on Taobao (Alibaba's e-commerce site) – instead of performing similar tasks on Google, Facebook or Amazon. The “Great Firewall” of China, despite its infamous political aspect, has also functioned as an economic shield for the state to reserve its domestic market for home-grown players. Moreover, this enormous home market has become increasingly lucrative as well, in tandem with China's growing economic power. In

---

<sup>3</sup> Zen Soo and Alice Shen, “Google steps up global fight for digital wallet as China dominates mobile payment,” 21 February 2018, *South China Morning Post*, <https://www.scmp.com/tech/innovation/article/2134123/google-steps-global-fight-digital-wallet-china-dominates-mobile>.

<sup>4</sup> Nicole Jao, 5 March 2018, Technode, <https://technode.com/2018/03/05/wechat-1-billion-users>.

<sup>5</sup> Bernard Marr, “How Chinese Internet Giant Baidu Uses Artificial Intelligence and Machine Learning,” 6 July 2018, *Forbes*, [https://www.forbes.com/sites/bernardmarr/2018/07/06/how-chinese-internet-giant-baidu-uses-artificial-intelligence-and-machine-learning/#366cbc002d55\\_](https://www.forbes.com/sites/bernardmarr/2018/07/06/how-chinese-internet-giant-baidu-uses-artificial-intelligence-and-machine-learning/#366cbc002d55_).

<sup>6</sup> China Internet Network Information Center (CNNIC), “2017 Statistical Report on Internet Development in China,” 2018, <https://cnnic.com.cn/IDR/ReportDownloads/201807/P020180711391069195909.pdf>.

2018, Alibaba's 24-hour shopping festival – “Single's Day” (similar to “Black Friday” in the US) – achieved a sales record of \$30.8 billion, easily surpassing the sales volume of any single US shopping holiday.<sup>7</sup> The booming Chinese economy, the state's protective internet policies, and the growing purchasing power of the Chinese “rising middle class” – a large number of the favoured social strata – have jointly provided a fertile home ground for the rise of the BATs.

Second, apart from a big and lucrative home market, the BATs have also benefited from the strong policy support from the Chinese government, especially its persistent focus on the development of communication and information technologies (ICTs) during the past three decades. Indeed, from Premier Zhou Enlai's “four modernisations” in the 1970s to President Jiang Zemin's “None of the four modernisations would be possible without informatisation” in the 1990s, the development of a modern information industry – under the influence of the then flashy international branding of the internet as the “information superhighway” – was regarded by the top leadership as a critical opportunity to reclaim China's historical position and to “catch up with the West”.<sup>8</sup> Moreover, if in the 1980s and 1990s, ICT manufacturing was considered as a “pillar industry” that spearheaded China's Foreign Direct Investment (FDI)-driven, export-oriented, and labour-intensive development, entering into the 2000s, network connectivity and online applications started to gain prominence and have been accorded a new role in propelling China's post-2008 restructuring toward an innovation and consumption-based economy, i.e., both moving up the global production value chain and transitioning to a more domestic-oriented economy.<sup>9</sup> The “Internet Plus” policy in 2015, which aims to further integrate digital technologies with traditional economic sectors, and the newly released “Next Generation Artificial Intelligence Development Plan” in 2017 are only the two most recent examples of a long-standing policy focus. China's internet industry in general, and the BATs in particular, have been the direct beneficiaries of this persistent government support.

<sup>7</sup> Arjun Kharpal, “Alibaba sets new Singles Day record with more than \$30.8 billion in sales in 24 hours,” *CNBC*, 11 November 2018, <https://www.cnbc.com/2018/11/11/alibaba-singles-day-2018-record-sales-on-largest-shopping-event-day.html>.

<sup>8</sup> Yuezhi Zhao, “After Mobile Phones, What? Re-Embedding the Social in China's ‘Digital Revolution,’” *International Journal of Communication* 1, no. 1 (2007): 92–120.

<sup>9</sup> Yu Hong, *Networking China: The Digital Transformation of the Chinese Economy* (Urbana, IL: University of Illinois Press, 2017).

The third force, and the one that has been relatively overlooked in the existing discussion, is the role of transnational capital. As I have discussed elsewhere,<sup>10</sup> although Beijing controls its domestic internet through various regulatory measures, it has exhibited an unusually high degree of tolerance toward foreign capital *as portfolio investment*, which literally jump-started its web economy in the late 1990s. Indeed, the BATs were all founded in the late 1990s and early 2000s with investment from transnational venture firms: Tencent in 1998 with \$2.2 million from Hong Kong's PCCW and Boston-based IDG, Alibaba in 1999 with \$5 million from a Goldman Sachs-led foreign investment team, and Baidu in 2000 with \$1.2 million from Silicon Valley-based venture capital firms Integrity Partners and Peninsula Capital. Along with their significant capital contribution, foreign investors have taken controlling stakes – as well as corporate board membership – in the three “Chinese” tech kings. In 2013, South African company Naspers controlled 34% of Tencent, US investment firm DFJ Venture Capital controlled 25.8% of Baidu and Softbank of Japan owned 31.9% of Alibaba.<sup>11</sup> Instead of a symbol of the rising “Chinese” tech power, therefore, the BATs are actually much more complicated products constructed collectively by state policies and transnational capital.

## THE BATS GO GLOBAL

Having secured a dominant position in their respected areas in the Chinese market, the BATs have also started to increasingly set their sights on the international market and are actively engaged in a global shopping spree. For example, Alibaba, following a record \$25 billion IPO in 2014, recently spent \$1 billion for a controlling stake in Lazada, the biggest e-commerce firm in Southeast Asia.<sup>12</sup> Baidu, similarly, confirmed its 2014 investment in Uber, the US-based taxi sharing company, with some estimating the figure to be around \$600 million.<sup>13</sup> In mid-2016, Tencent led

---

<sup>10</sup> Hong Shen, *Across the Great (Fire)Wall: China and the Global Internet* (PhD dissertation, University of Illinois at Urbana-Champaign, 2017).

<sup>11</sup> “Baidu/Tencent/Alibaba/Renren de zhenzheng dalaoban shishui?” 百度/腾讯/阿里巴巴/人人网的真正大老板是谁? [Who're the real big bosses behind Baidu/Tencent/Alibaba/Renren], [http://big5.gmw.cn/g2b/IT.gmw.cn/2013-11/05/content\\_9394755.htm](http://big5.gmw.cn/g2b/IT.gmw.cn/2013-11/05/content_9394755.htm).

<sup>12</sup> Newley Purnell and Alyssa Abkowitz, “Alibaba Thinks Outside the China Box,” *The Wall Street Journal*, 12 August 2016, [http://www.wsj.com/articles/alibaba-thinks-outside-the-china-box-1470995037?cxnavSource=cx\\_picks&cx\\_tag=contextual&cx\\_artPos=5#cxrecs\\_s](http://www.wsj.com/articles/alibaba-thinks-outside-the-china-box-1470995037?cxnavSource=cx_picks&cx_tag=contextual&cx_artPos=5#cxrecs_s).

<sup>13</sup> Lulu Yilun Chen, “Baidu Said to Buy Stake in Uber, Boosting App in China,” *Bloomberg*, 11 December 2014, <http://www.bloomberg.com/news/articles/2014-12-12/baidu-said-to-buy-stake-in-uber-boosting-app-in-china>.

an investment group to purchasing 84% percent of Finnish mobile games maker Supercell for \$8.6 billion.<sup>14</sup>

What is the aim behind these massive global investments?

First, the BATs have certainly used them as a way to fortify their core strengths. For example, over the years, Tencent has invested in various game makers in the international market, such as Riot Games, Epic games, Activision, CJ games, Glu Mobile and Supercell, to support its primary growth engine – the online gaming market. Alibaba, similarly, has poured large amounts of capital into different e-commerce sites, payment companies, and logistics platforms to support the development of its main business of e-commerce, building partnerships with American online shopping service Shoprunner, Indian online payment system Paytm, and Singapore Post.

Second, shopping globally can also help these Chinese tech giants to further diversify their business structures. For instance, apart from various deals with mobile game makers, Tencent has also participated in the social media (with Spotify and SnapChat), ride-sharing (with Ola and Go-Jek), e-commerce (with Flipkart) and electronic vehicle (with Tesla) markets. Alibaba, on the other hand, has accomplished large deals in social media (with TangoMe and SnapChat) and online gaming (with Kabam), increasingly encroaching on Tencent's home turf.

Finally, outward capital projection has played an important role for the BATs with respect to finding profitable outlets to reinvest the money capital they have accumulated over the years. It is reported that in 2013, Alibaba held \$7 billion in cash reserves while Tencent had \$5 billion.<sup>15</sup> This large amount of money capital needs to be reinvested in order to generate new profits. Probably for this reason, the BATs have also started to partner with transnational venture capital firms to explore lucrative emerging markets outside of China. In April 2010, for example, Tencent injected \$300 million into Digital Sky Technologies, a Russian investment firm that is well known for its investments in Facebook, to build a "long-term strategic partnership".<sup>16</sup> In January 2015, Tencent and another Chinese social media

---

<sup>14</sup> Lulu Yilun Chen, Pavel Alpeyev and Yuji Nakamura, "Tencent Leads \$8.6 Billion Deal for Clash of Clans Studio," *Bloomberg*, 22 June 2016, <http://washpost.bloomberg.com/Story?docId=1376-O949KV6KLV701-44DR9M9STL12JECOAD2GQQLPSP>.

<sup>15</sup> Alistair Barr, "Just How Much Cash Does Alibaba Have," 6 May 2014, *The Wall Street Journal*, <http://blogs.wsj.com/digits/2014/05/06/just-how-much-cash-does-alibaba-have/>; Evelyn M. Rusli and Paul Mozur, "China Buys Its Way into Silicon Valley," 4 November 2013, *The Wall Street Journal*, <http://www.wsj.com/articles/SB10001424052702303843104579171963801529056>.

<sup>16</sup> Tim Bradshaw and Kathrin Hille, "Tencent to invest \$300m in DST," *Financial Times*, 12 April 2010, <https://next.ft.com/content/5364d9c2-464d-11df-9713-00144feab49a>.



company, Renren, invested \$100 million in Singulariteam, an Israeli venture capital firm. This \$100 million, according to Singulariteam, would be used to fund local start-ups.<sup>17</sup> In other words, instead of merely receiving global venture capital investments, China-based internet companies, represented by the BATs, have now started to form collaborative relationships with transnational financial capital to project money *outward*.

Despite growing outward capital projection, there is still a long way for the BATs to go to conquer the international market. In 2017, the overseas revenues of Alibaba, Tencent, and Baidu only accounted for 11%, 5%, and 1% of their annual revenues, respectively. In contrast, in the same year, overseas revenue was 53% for Google, 56% for Facebook, and 32% for Amazon.<sup>18</sup> Indeed, the BATs have not become “global” internet giants yet – at least for now.

## THE NEW JOURNEY

In March 2015, reporting to the National People’s Congress, Chinese Premier Li Keqiang announced that China had adopted an “Internet Plus” strategy, which aims to link the internet, especially next-generation network technologies such as Big Data and Internet of Things, with almost all the sectors of the Chinese political economy.<sup>19</sup> A few months later, on 5 July, China’s State Council, the top decision-making body of the government, formally promulgated the “Internet Plus Action Plan,” calling for further deepening of the integration of network technologies with 11 targeted sectors, including entrepreneurship and innovation, manufacturing, agriculture, energy, finance, public services, logistics, e-commerce, transportation, green ecology and Artificial Intelligence.<sup>20</sup> With various state agencies and local governments issuing their own versions and interpretations of this central strategy, “Internet Plus” has officially become a hallmark policy under the Xi Jinping-Li Keqiang administration.

---

<sup>17</sup> Ingrid Lunden, “Israel VC Singulariteam Raises 2nd Fund, \$102M Backed by Tencent, Renren Founders,” *TechCrunch*, 28 January 2015, <https://techcrunch.com/2015/01/28/singulariteam-vc-fund>.

<sup>18</sup> Rebecca Fannin, “China’s BAT Won’t Battle the FANGs in the US Anytime Soon,” 21 May 2018, *Forbes*, <https://www.forbes.com/sites/rebeccafannin/2018/05/21/dont-count-on-chinas-baidu-alibaba-tencent-to-go-mainstream-in-the-u-s/#191319745f28>.

<sup>19</sup> Xinhua News Agency, “Internet Plus Set to Push China’s Economy to Higher Level,” 15 March 2015, *Xinhua Net*, [http://news.xinhuanet.com/english/2015-03/15/c\\_134067831.htm](http://news.xinhuanet.com/english/2015-03/15/c_134067831.htm).

<sup>20</sup> State Council, “Guiding Opinions on Actively Promoting the ‘Internet Plus’ Action Plan,” [http://www.gov.cn/zhengce/content/2015-07/04/content\\_10002.htm](http://www.gov.cn/zhengce/content/2015-07/04/content_10002.htm).

"Internet Plus" has also taken the BATs onto a new journey as it has officially opened up many previously highly regulated sectors in China for internet capital to permeate, from healthcare to education, from banking to public services. Indeed, riding the tide of the "Internet Plus," there have been many "first times" in the three tech giants' business adventures. In the area of banking and finance, Alipay and WeChat Pay were among the first non-banking payment providers that received a license from China's central bank. In 2014, Alibaba's affiliate bank, Zhejiang Internet Commerce Bank, was one of the two privately owned commercial banks – another one belongs to Tencent – to be allowed to operate in the highly regulated state-owned banking industry.<sup>21</sup> A number of local governments have also reached agreements with Alibaba and Tencent to develop smart cities initiatives, linking public services such as hospital appointments or payment of utility bills with Alipay and WeChat Wallet, the two companies' payment platforms.<sup>22</sup> Probably most significantly, tech giants have also started to cultivate strong collaborative relationship with China's state-owned behemoths: In 2016, Alibaba teamed up with China's largest automaker, the state-owned SAIC Motor Corporation, to jointly develop driverless cars. The same year, it also announced its plan to help the state-owned oil giant Sinopec on big data analytics and information security, officially stepping into the highly sensitive energy sector.<sup>23</sup> Through all these new initiatives, the BATs have extended their tentacles into various aspects of China's political economy.

This trend is expected to continue with China's new push toward 5G mobile networks, the Internet of Things, and probably most prominently, Artificial Intelligence (AI). In 2017, the BATs were collectively recruited by the state as the first members of China's AI "national team," with Baidu's focus on driverless cars, Alibaba's focus on smart cities, and Tencent's focus on computer vision and medical AI.<sup>24</sup> How this new journey will unfold, however, remains to be seen.

---

<sup>21</sup> Gabriel Wildau, "Alibaba affiliate Wins approval for Bank License," *Financial Times*, 29 September 2014, <http://www.ft.com/cms/s/0/605c26bc-47d3-11e4-ac9f-00144feab7de.html#axzz4KvOySat4>.

<sup>22</sup> Xinhua News Agency, "Tencent, Alibaba in race to snap up smart city deals with local gov't," *China Daily*, 16 April 2015, [http://www.chinadaily.com.cn/bizchina/tech/2015-04/16/content\\_20450793.htm](http://www.chinadaily.com.cn/bizchina/tech/2015-04/16/content_20450793.htm).

<sup>23</sup> Brian Spegele and Alyssa Abkowitz, "China's Tech Leaders Try Teaching Dinosaurs to Dance," *The Wall Street Journal*, 24 April 2016, <http://www.wsj.com/articles/chinas-tech-leaders-try-teaching-dinosaurs-to-dance-1461526201>.

<sup>24</sup> Meng Jing and Sarah Dai, "China recruits Baidu, Alibaba and Tencent to AI 'national team'," *South China Morning Post*, 25 September 2018, <https://www.scmp.com/tech/china-tech/article/2120913/china-recruits-baidu-alibaba-and-tencent-ai-national-team>.

## AFTER THE BATS, WHAT? THE NEW UNICORNS

Despite their dominant status in the Chinese market, the BATs are by no means without competitors. The next generation of digital unicorns – i.e., tech start-ups with more than \$100 billion valuation – are already approaching. Thanks to the aforementioned supportive government policies, China now reportedly has 164 tech unicorns, worth more than \$600 billion, according to the 2017 *China Unicorn Enterprise Development Report* published by the Ministry of Industry and Information Technology.<sup>25</sup>

Among these newly emerged tech companies on the list, the TMDs – news and information content provider Toutiao, online food delivery-to-ticketing services giant Meituan-Dianping, and ride-hailing platform Didi-Chuxing – are arguably the three most powerful ones in the web applications sector.<sup>26</sup> Toutiao is currently valued at more than \$20 billion, after its most recent fund raising in August 2018. Based on using machine learning algorithms to create highly personalised news feeds, it has quickly become one of the most popular news and social media apps in China, increasingly encroaching on Tencent’s and Baidu’s territories. Meituan-Dianping, the Chinese food delivery unicorn, went public in Hong Kong in September, raising \$4.2 billion in a single deal. Aggressively expanding its businesses from group buying to food delivery to ride-hailing, it is currently directly confronting Eleme, the Alibaba-backed online food ordering platform. Finally, Didi-Chuxing, after defeating and acquiring Uber China in 2016, has effectively become a monopoly in China’s growing ride-hailing market. Backed by funding and market entries from both Alibaba and Tencent, it offers a wide range of transportation options for 550 million users in China, ranging from taxi to bike sharing, and is currently competing with Meituan-Dianping in the food delivery sector as well.<sup>27</sup>

The rise of this full-range of Chinese tech companies on the global stage has raised serious questions not only for the Chinese, but also for the international internet. For a long time, popular media stories have shaped the conventional wisdom about China’s relationship with the global internet. For many, China is only interested in building a national “intranet” that is sealed by the “Great Firewall,” or

---

<sup>25</sup> Xie Yu and Maggie Zhang, “At the heart of China’s techno-nationalism is a hit list of 200 unicorns,” *South China Morning Post*, 31 March 2018, <https://www.scmp.com/business/companies/article/2139684/heart-chinas-techno-nationalism-hit-list-200-unicorns>.

<sup>26</sup> Other top units of Internet capital on the list include Ant Financial (Alibaba-affiliated financial arm, with a valuation of \$75 billion) and Xiaomi (consumer electronics company, with a valuation of \$46 billion).

<sup>27</sup> “About Didi,” <https://www.didiglobal.com/about-didi/about-us>.

a “giant cage” that is unplugged from the international network.<sup>28</sup> This conventional wisdom, however, has become more and more inadequate – and even misleading – in the face of the growing cyber expansion of China-based entities. Has the Chinese internet started to move across the “Great Firewall”? Will the future structure of the global internet be significantly shaped by China-based business actors – not only the BATs but also the TMDs, and many other unicorns to come? If so, for whom and to what ends?

**Hong Shen** is a Systems Scientist at the Human-Computer Interaction Institute at Carnegie Mellon University. She received her PhD in media and communications from the University of Illinois at Urbana-Champaign in 2017. Her research focuses on internet industry and policy (with an emphasis on China) as well as the social and policy implications of emerging technologies.

---

<sup>28</sup> Gady Epstein, “China’s Internet: A Giant Cage,” *The Economist*, 6 April 2013, <http://www.economist.com/news/special-report/21574628-internet-was-expected-help-democratise-china-instead-it-has-enabled>.



# Japan's Innovation Systems at the Crossroads: Society 5.0

*René Carraz and Yuko Harayama*

## INTRODUCTION

This paper intends to address the changes that have occurred in Japan's innovation system at large, and how they have impacted the formulation and implementation of the country's Science, Technology and Innovation (STI) policies in particular. It can be argued that Japan's industrial system after the Second World War has emerged at the crossroads between the old and new technological paradigms (Imai, 1992). The old paradigm is an extension of the mechanisation process, familiar since the second industrial revolution; the mass production of standardised technologies and innovation processes was orchestrated by large companies, which relied on vertically organised technological and industrial developments (Fransman, 1999; Goto and Odagari, 1997). In the new paradigm, a more decentralised process fuelled by a strong and ever-expanding base linked to the digital economy emerged; multiple actors such as universities, public research institutions, public sector agencies, entrepreneurial companies and citizens play a more decisive role (Motohashi, 2005; Okamuro et al., 2011; Fukugawa, 2016).

In a narrow sense, innovation policies often tend to mitigate market failure consequences by providing government support for business research and development (R&D), and government investments in basic R&D, knowledge infrastructures, education and skills. Nevertheless, innovation often goes beyond the mobilisation of science and technology as it involves a wide range of assets that extend beyond R&D (Von Hippel, 2006). In that respect, the *OECD Innovation strategy 2015* suggests that the improvement of the governance and implementation of innovation policies is one of the five priorities for policymakers for a comprehensive and action-oriented approach to innovation (OECD, 2015). While framing innovation policies, policymakers need to recognise that they operate in a complex, dynamic and uncertain environment, where governments are increasingly asked to act as

facilitators in the face of these constantly changing conditions. Their mission therefore is to enable closer coordination between individual economic agents as well as foster greater experimentation in the wider economy and society. This includes greater emphasis on building networks, improving coordination and regulation, as well as promoting guiding strategies to deal with global challenges through STI policies and actions.

This paper suggests that, while the Japanese system of innovation is still dominated by a centralised culture where big companies and ministries have a central position in the decision making process, their influence over national innovation policy since the 1990s has been supplemented with new actors and mechanisms. The system moved away from an emphasis on supporting domestic industrial capacities through a “big science” research agenda. Instead the focus was to strengthen budgets and public infrastructure for publicly supported research while fostering university-industry collaborations. In the latest phase, the policy orientation saw a shift away from a traditional technology-driven approach to a more society-centred and challenge-driven innovation policy. A signpost to this trend is the creation and deployment of the concept of “Society 5.0” as a foundation for future economic growth and the basis for a multi-level innovative ecosystem. Broadly defined, Society 5.0 is an STI policy proposed by the Japanese government to gather momentum around Japan’s unique position and role in mastering the challenges of digitalisation and connectivity to raise economic growth prospects and solve societal challenges. The goals are not solely technological. The moves should rather be seen as a way to push for fundamental reforms of Japanese economic and social institutions by giving more weight to society in the innovation process.

This paper is structured in three sections. The first section analyses the change of paradigm that the Japanese innovation system has undertaken. The second section presents the evolutionary path of the Japanese STI policy framework strategy laid out by the government since the enactment of the Science and Technology Basic Law in 1995. The third section shows the steps that led to the introduction of Society 5.0, and outlines its conceptual definition.

## **1. HISTORICAL PERSPECTIVE ON THE JAPANESE INNOVATION SYSTEM**

### **“Big project” research agenda**

From an innovation perspective, Japan has been successful from the 1960s through to the 1980s when it was trying to catch up with more technologically advanced

nations; “big project” research programmes initiated by the government were an important part of the story. One of the most successful examples is the Very Large Scale Integrated circuit (VLSI) project, designed to help Japan catch up in semiconductor technology. The project, conducted between 1975 and 1985, had a budget of ¥130 billion (EUR 1.01 billion) of which 22% was financed by the government. All of the major national industrial players were part of the project, and gained world leadership as a result (Sigurdson, 1998). But as many industries caught up to and reached the technological frontier in the 1980s, the need for changes in STI policies became apparent. Indeed, it is often argued that the closer a country is to the technological frontier in a given field, the more difficult it is to tap the technological pool of knowledge. A result of this is that it becomes harder for the government to design and manage new research projects.

A good example of this issue is given by Fransman’s (1995) account of the Fifth Generation Computer Project, a large-scale programme devised by the Japanese government in the 1980s to develop a totally new kind of computer, allowing Japanese companies to undermine IBM’s supremacy. However, in strictly scientific terms, the outputs of the programme were meagre as the beliefs on what computing was all about were changing during the Project’s realisation driven by breakthroughs in microprocessor technology. This rapidly rendered the Project’s goals obsolete, showing the limitations of the “big project” research agenda model. Since the 1990s, Japan’s R&D projects display a decline in the government’s direct interventionist capabilities as many sectors of the country’s industry moved from follower position to technological pioneers. Sakihara (1997) concluded, in his large-scale survey of government-sponsored R&D consortia in Japan, that in the 1990s the government lost its edge in signalling and directing the development of important research fields, as the goal was no longer to transfer and adapt Western technologies.

## **Prioritisation of science-based technologies**

Moving up the technological ladder, the Japanese government has been increasingly targeting “science-based” industries to counteract the “hollowing out” of manufacturing jobs in more labour-intensive sectors, such as the machinery industry, which lost 750,000 jobs in the 1990s (MEXT, 2004). Essentially, science-based industries are characterised by strong linkages with scientific knowledge. In these sectors, the main source of technology resides in the R&D activities of the firms. Meanwhile this R&D relies on the development of science in universities and public laboratories, with which these firms maintain close collaboration (Niosi,



2000). This new framework was a challenge for domestic firms, as they had to move from a catch-up strategy to a search for innovative technologies and outside knowledge partners. This orientation shift implied changes not only in R&D-targeted fields, but also in the way R&D was conceived, planned and managed, so that the “big project” agenda, the reference point of the Japanese research system, had to be restructured.

Firms have coped with this demand for “science-based” technologies not only by building up substantial research capacities, but also by increasing research cooperations with universities and other external research institutions. As a consequence industrial research in these sectors is linked with the increased contribution of academic research to industrial R&D and product developments. What is new here is that the decentralisation of the innovation process became apparent in these industries with a growing reliance on external partners.

## 2. PARADIGM CHANGE: A NEW POLICY PERSPECTIVE

Since the bursting of the financial and property bubble in the 1990s the Japanese economy has been confronted by an economic slowdown, the hollowing out of some of its production facilities, demographic challenges, and increased economic and technological competition from other countries, especially in other parts of Asia. In order to address these issues, one of the main strategies mobilised by Japanese policymakers has been to concentrate efforts on STI policies and increase public expenditures in that area as part of a long-term strategy to support economic growth.

### Science and Technology Basic Law

In its search for a novel growth model, the Japanese government has emphasised the need to promote domestic science and technology (S&T) since the 1990s. The first step was the revision in 1992 of the “General guideline for science and technology policy” of 1986 based on the recommendation of the Council of Science and Technology (CST). The enactment of the *Science and Technology Basic Law* on 15 November 1995 (hereinafter referred to as “the Basic Law”) symbolised a firm commitment towards the promotion of R&D, determined its basic principles, and required the Japanese administration to raise science and technology-related spending. The Basic Law requires the Japanese government to develop and implement a five-year *Science and Technology Basic Plan* (hereinafter referred to as “Basic Plan”). Looking at the successive Basic Plans, it is clear that they are not intended

to define priorities in R&D on a detailed level. Rather they can be seen as the government's broad identification of important research fields, actors and framework conditions, hence framing the domestic aspirations and expectations of the actors of the system.

## Science and Technology Basic Plans

The First Science and Technology Basic Plan (1996-2000) expressed the goal to energetically promote a "new R&D system for the country". This goal was achieved mainly through an expansion of the existing research apparatus. Major measures that were implemented are the strengthening of university-industry linkages, the expansion and financial support for international exchange programmes, the commercialisation of "intellectual assets", support to young researchers (especially post-doctoral fellows) and increased funding of competitive research grants, all at a total budget of ¥17 trillion (EUR 132 billion). The expansion continued with the second Basic Plan (2001-2005). Competitive funding was doubled, the commitment to basic research was strengthened, and societal goals were included such as improving the communication between society and science. For all this the government assigned a budget of ¥24 trillion (EUR 187 billion), a 36% increase over the First Basic Plan. More importantly, from a policy perspective, the second Basic Plan offered a vision to apprehend technological and societal changes.

The vision lies in the prioritisation of a limited number of research fields and subjects. The objective was to promote R&D activities that are in line with policy priorities in resolving national and social issues. These include the enhancement of international competitiveness, countermeasures against environmental problems, ageing and the low birth-rate of Japanese society. The ambitious Plan aimed to foster emerging S&T fields that were expected to be developed rapidly in the future, while at the same time, secure proper resources to promote basic research. In practice, four priority domains were to be encouraged by the government: life sciences (including biotechnology), IT, environmental sciences and nanotechnology and new materials. R&D funding was to be mobilised to promote these four domains.

The third Basic Plan's (2006-2010) design reflected the need for Japan to put in place an environment more inclined to help scientists to achieve high-quality research results, to cultivate a highly competitive research environment, and to advance science while continually promoting innovation. For instance, measures were put in place to support the autonomy of young researchers, reform graduate education, and increase competitive funding. Despite the stringent fiscal climate,

the Plan continued to push for a slightly increased budget and proposed to allocate ¥25 trillion (EUR 194 billion) in total R&D investment over its five-year duration.

The Fourth Basic Plan (2011-2015) laid the foundation for an issue-driven formulation of the innovation strategy that pushed forward the use of STI to address social and economic challenges. A large portion of the Plan targeted initiatives for the “recovery and revitalisation” of Japan as a response to the 2011 Great East Japan Earthquake as one of its four major challenges to be overcome for sustainable growth and prosperity. It was a departure from previous Plans, where the focus had been on strengthening particular fields of S&T, a technology-driven approach.

### **3. A MORE COMPREHENSIVE INNOVATION STRATEGY, TOWARDS SOCIETY 5.0**

#### **Empowerment of the Council dedicated to Science, Technology and Innovation**

In terms of supervision of the Japanese S&T policy, the Council of Science and Technology passed the responsibility to a new Council for Science and Technology Policy (CSTP), which was situated in the cabinet office above individual ministries. Thus the CSTP was equipped with wider competences in 2001, just before the launch of the second Basic Plan. As stated by the second Basic Plan, “The CSTP will act as a control tower and direct the multi-fold processes of S&T policy implementation. In addition to formulating promotion strategies on prioritised areas, principles of resource allocation, and guidelines for project evaluation, the Council will strive to promote S&T activities.”<sup>1</sup> The CSTP formulated and coordinated all of the nation’s S&T policies.

In 2013, under the newly formed Abe Cabinet, the CSTP was assigned to formulate the so-called “Science, Technology and Innovation Comprehensive Strategy” (hereafter “STI Comprehensive Strategy”) by the Prime Minister, in view of the formulation of Japan’s New Growth Strategy. The first STI Comprehensive Strategy was adopted at a Ministerial Meeting in June 2013, and it was revisited the following year, to take into account the changing environment surrounding innovation and to better respond to policy challenges. Thus, Japan acquired a new framework for STI, alongside its overarching five-year Basic Plan, which provides basic orientation for S&T policies. Indeed, the STI Comprehensive Strategy was expected to function as a complement to the five-year Basic Plan, by providing actionable policy

---

<sup>1</sup> Second Basic Plan, <http://www8.cao.go.jp/cstp/english/basic/index.html>, accessed 24 October 2018.

recommendations, which could take into account the country's evolving societal and political needs.

The STI Comprehensive Strategy 2013 was guided by three principles: (i) act smart; (ii) implement a thinking system; (iii) think global, and is composed of the following three pillars:

1. Grand policy challenges
2. Structural reforms of the national innovation system
3. Empowerment of the CSTP

Regarding the third pillar, the CSTP proposed to equip itself with a new competency, by designing and implementing programmes promoting innovation with its budget, with the aim to better drive efforts made at the ministerial level. It required a revision of the Act for Establishment of the Cabinet Office, the legal basis of the CSTP. In May 2014, the Parliament voted on proposed amendments to enlarge CSTP's competencies and to change the name of the CSTP to "Council for Science, Technology and Innovation (CSTI)". Thus the mainstreaming of "Innovation" became apparent, with CSTI as a guiding body.

The CSTI moved one step further in 2014 with its STI Comprehensive Strategy. The roadmaps of grand challenges to be addressed were updated and consolidated around the newly created programme "Cross-Ministerial Strategic Innovation Promotion Programme (SIP)". With regard to the structural reforms, CSTI proposed to take action to enlarge opportunities for "challenges" and "interactions", by bridging ideas, facilitating the mobility of people, and creating different types of innovation hubs. The CSTI also tried to promote disruptive thinking, putting a newly created programme, "Impulsing Paradigm Change through Disruptive Technologies Programme (ImpACT)", at the heart of its policy tools. ImpACT aims to generate ground-breaking innovation, which will bring drastic changes to industries and society if realised. Through ImpACT, the CSTI expected next-generation innovations to be created by investing in high-risk, high-impact R&D. Through these two programmes, the CSTI became equipped for policy experimentation, and this capacity will play an essential role for the forthcoming "Society 5.0", by trying to trigger paradigm changes through disruptive research.

## **Fifth Basic Plan and the inception of Society 5.0**

The preparation of the Fifth Basic Plan was initiated with a new methodological approach, which consists of brainstorming discussions among CSTI's executive members, with a view to identifying shared guiding principles upon which the Fifth

Basic Plan will be founded. This runs in parallel to a formal assessment of 20 years' worth of experiences of Basic Plans and benchmarking exercises of STI policies around the world.

Recognising that the world is increasingly becoming interconnected beyond traditional borders at a pace we have hardly experienced before, and evolving at an accelerated rate fuelled by digital transformation, the executive members have identified the "preparedness" for this unpredictable and unforeseeable near future as the most fundamental challenge to be addressed throughout the Fifth Basic Plan. The capacity to design future industry and society will be instrumental, and to this end, investing in people and providing the space to test their ideas will be the key. What we observe here is the shift from the traditional technology-driven to a more society-centred and challenge-driven innovation policy.

Four pillars have been identified to structure the Fifth Basic Plan:

1. Preparing the next generation: Future industry and society
2. Addressing socio-economic and global challenges
3. Investing in "fundamentals": People and excellence
4. Better-functioning STI systems

The first pillar naturally became the nursing ground for the inception of Society 5.0. Behind the eye-catching titles and programme initiatives – such as Third Industrial Revolution (Rifkin, 2011), Fourth Industrial Revolution (Schwab, 2017), Industry 4.0 (Kagerman et al. 2013), "e-Estonia" Programme, "Smart Nation" (Singapore), or the FIWARE open source platform supported by the European Union – lies a fundamental shift in how economies may be structured in the future as industries, academia and governments create, store and integrate various data streams into daily production processes to provide goods and services.

Society 5.0 is not an exception. But beyond this shift, Japan is facing a set of pressing challenges, such as its ageing population, labour shortages and weak nominal growth prospects. Just as Industry 4.0 was a tentative response to the digital transformation of manufacturing, Society 5.0 emerged from the need to master the challenges of digitalisation and connectivity across a wide range of platforms in particular and more generally across all levels of the Japanese society to achieve the digital transformation of society itself.

Indeed, in today's information society, the weight of added values generated by connecting intangible assets is likely to surpass the added value generated by the manufacturing sector (Haskel and Westlake, 2017). Also we may expect that this ongoing digital transformation will have an amplified impact on economic and social

systems and even on our social values. In fact, Society 5.0 is an attempt to capture this expectation by inviting all citizens – including game changers such as entrepreneurs and non-government organisations (NGOs) and a wide variety of actors that in the past have only participated in non-visible ways in the innovation process – to take part in shaping our future society, while respecting the values of openness, sustainability and inclusiveness, and acting accordingly and in a responsible manner. Therefore, Society 5.0 has to be nurtured, tested and developed in order to become an operational concept. This approach implies the need to secure a space for accommodating various bottom-up ideas, which has proven to be a big challenge for formulating the Fifth Basic Plan.

## Definition of “Society 5.0”

Officially the term “Society 5.0” was introduced and coined in the Fifth Basic Plan by the CSTI and approved by Cabinet decision in January 2016. In the Fifth Basic Plan, Society 5.0 is defined as follows:

a society that is capable of providing the necessary goods and services to the people who need them at the required time and in just the right amount; a society that is able to respond precisely to a wide variety of social needs; a society in which all kinds of people can readily obtain high-quality services, overcome differences of age, gender, religion, and language, and live vigorous and comfortable lives.<sup>2</sup>

The outline of the Fifth Basic Plan described Society 5.0 as “an initiative merging the physical space (i.e. the real world) and cyber space by leveraging ICT to its fullest, where we are proposing an ideal form of our future society” with “a series of initiatives geared toward realising this.” Society 5.0, by proposing to further the potential of data-driven technology and application while enhancing the quality of life of all citizens through a “super smart society”, has the potential to be a core notion of Japan’s STI and growth strategy.

It could be argued that this wide-ranging STI policy goal is a departure from the traditional technology-driven approaches pursued so far, and it relates to the strategic planning orientation taken by the CSTI. Rather than setting rigid Plans centred on how technology is likely to evolve in the next five years, the essence of the Fifth Basic Plan is rather to prepare the Japanese STI system for an unforeseeable technological future. This should be achieved by securing public investment in

---

<sup>2</sup> 5th Basic Plan, <http://www8.cao.go.jp/cstp/english/basic/5thbasicplan.pdf>, accessed 24 October 2018.

R&D to a target level of 1% of GDP, by investing in the development of high-quality human resources, and promoting an open-innovation framework and open science to facilitate the exchange of intellectual assets. Additionally, technological domains considered as fundamental for the promotion of interconnected systems that facilitate the use of data should be promoted and aligned with fundamental technological fields where Japan is in a leading position, such as robotics and human interface technology, or where it should build up technological strengths, such as cybersecurity, Internet of Things (IoT) system architecture technology, and big data analytics, as these fields are considered critical to implementing secure and reliable data platforms. In order to implement this vision, a common platform called “Society 5.0 Service Platform”, through collaboration between industry, academia and the relevant government ministries, is envisaged by the CSTI.

This systemic approach for the development of an innovation ecosystem is in our view pivotal to the overall strategy. It is necessary to incorporate these new technologies and data usages in all industries and social activities in order to promote parallel economic development and bring about solutions to social problems. For instance, in order to create value in the field of “intelligent transport systems”, with the prospect of autonomous driving, it is important to promote a standardisation of technological interfaces and data formats, and to develop common security technologies shared by all actors, human and non-human. Additionally, collaboration between industry, academia, government and society is of the utmost importance as usage and acceptance of the systems developed is likely to be shaped by users and citizens.

## **Acceptance and usage of “Society 5.0”**

The concept of Society 5.0 has been incorporated in the Ministry of Economy and Trade’s (METI) “New Industrial Structure Vision”, which projects the evolution of industry up to 2030 by identifying and finding ways of overcoming systemic challenges to the realisation of Society 5.0. In March 2017, METI announced the policy concept of “Connected Industries” where industrial players will integrate the various technologies needed for the realisation of a “human-centred” Society 5.0.

From the private sector, Keidanren, Japan’s most important business federation, endorsed the concept of Society 5.0 in its policy proposal “Toward realisation of the new economy and society” as early as April 2016. In February 2017, Keidanren published a comprehensive action plan to rebuild Japan with Society 5.0 as its key concept. Also, industrial players such as Hitachi, NEC, Fujitsu, Toyota and Panasonic, among others, integrated Society 5.0 as part of their overarching strategies.

Moreover, Society 5.0 plays a pivotal role in the recently updated growth strategy of the Japanese government. The Prime Minister's Office released Japan's Growth Strategy 2017, which lays out a strategic blueprint for Japan's Society 5.0, including specific plans for the deep integration of cutting-edge technologies to solve economic and social problems. Approved by the Cabinet in June 2017 under the title "Future Investment Strategy", the government sees the efforts undertaken towards Society 5.0 as "the key to break secular stagnation and achieve mid- and long-term growth."<sup>3</sup> Japan is promoting Society 5.0 by introducing digital technologies in a variety of platforms, as well as accelerating its implementation to achieve a society in which all citizens have the potential to be engaged in the system.

## CONCLUDING REMARKS

The role of governments is no longer confined to identifying promising technologies, but to improving the overall environment for innovation. This assertion can help us to apprehend the changes that occurred in the governance of science and innovation in Japan. As Japan moved up the technological ladder, it had to reorganise its innovation system. Pursuing incremental innovation based on imported technologies was not a solution anymore. Challenged by the economic crisis of the 1990s, the Japanese government had to find a way to regain momentum. One of the paths followed was to invest massively in R&D spending and to revise its S&T policies. These changes can be traced back to the 1995 Basic Law, which stated the strong commitment of the government toward S&T with the aim of positioning the Japanese economy at the forefront of science-based industries, and more recently to the Fifth Basic Plan structured around the concept of Society 5.0.

Looking at the strengths of its innovation system, Japan seems capable of taking the lead in the realisation of Society 5.0 due to its abundance of well-documented physical data, advanced manufacturing technologies and pressing societal issues. The question then is whether the concept will gather enough traction to gain commitment from key stakeholders and help to induce societal transformation to achieve the government's vision of Japan being the "most innovation-friendly country".

Japan, having experienced the effects of mechanisation and industrialisation, and now under the sway of digitalisation, has an imperative to find ways to gain maturity as an open, innovation-friendly society, reaching beyond the sole pursuit

---

<sup>3</sup> [http://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/miraitousi2017\\_summary.pdf](http://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/miraitousi2017_summary.pdf), accessed 24 October 2018.



of economic growth. As such, the inception of Society 5.0 can be seen as an invitation to all stakeholders to think about the future of Japanese society, in an inclusive manner, with a particular eye on the advancement of STI. By and large, the latter is expected to bring prosperity to the society; however, economic and technological historical accounts demonstrate that this is not always the case. The creative destruction dynamic of innovation, dystopian technological changes and unintended scientific consequences may all be the collateral of a new economic system based on and nourished by the ever-increasing digitisation trend envisioned by Society 5.0. Therefore all stakeholders of the innovation process are expected to assume social responsibility when moving in that direction, in order for Society 5.0 to thrive and gain public acceptance. Under the flagship programme of Society 5.0, a society-wide experimentation is underway in Japan, putting the transformative power of STI policy to the test. The key to the success of Society 5.0 may lie in the learning capacity of Japanese society to embark on this innovative journey.

**René Carraz** is a Lecturer at Tokyo University, Japan. He holds a PhD in Economics and teaches and researches on science, technology and innovation, creative cities and urban studies using an economic perspective. His recent work includes studies of university-industry linkages in Japan and Asia, innovation, and urban creativity.

**Yuko Harayama**, Professor Emeritus of Tohoku University, is the former Executive Member of the Council for Science and Technology Policy, Cabinet Office of Japan. She is the former Deputy Director of the Directorate for Science, Technology and Innovation, OECD. She combines academic and policy expertise on the topics of innovation policies.

## References

- Fransman, M. 1999. *Visions of innovation: The firm and Japan*. Oxford University Press on Demand.
- Fukugawa, N. 2016. "Knowledge spillover from university research before the national innovation system reform in Japan: localisation, mechanisms, and intermediaries". *Asian Journal of Technology Innovation*, 24: 100-122.
- Goto, A. and Odagiri, H. 1997. *Innovation in Japan*. Oxford, England; New York: Clarendon Press.
- Haskel, J., and Westlake, S. 2017. *Capitalism without capital: the rise of the intangible economy*. Princeton University Press.
- Imai, K. I. 1992. "The Japanese pattern of innovation and its evolution". *Technology and the wealth of nations*. Stanford University Press, Stanford.
- METI, Ministry of Economy Trade and Industry, 2004. *White Paper on International Economy and Trade 2007*. METI, Tokyo.
- Motohashi, K. 2005. "University-industry collaborations in Japan: The role of new technology-based firms in transforming the National Innovation System". *Research policy*, 34: 583-594.
- Niosi, J. 2000. "Science-based industries: a new Schumpeterian taxonomy". *Research Policy*, 22: 429-444.
- OECD, 2015. *The Innovation Imperative: Contributing to Productivity, Growth and Well-Being*. OECD Publishing, Paris.
- Okamuro, H. and Honjo, Y. 2011. "Determinants of R&D cooperation in Japanese start-ups". *Research Policy*, 40: 728-738.
- Sakihara, M. 1997. "Evaluating government-sponsored R&D consortia in Japan: who benefits and how?". *Research Policy*, 26: 447-473.
- Sigurdson, J. 1998. "Industry and State Partnership: The historical role of engineering research". *Industry & Innovation*, 5: 209 - 41.
- Von Hippel, E. 2005. *Democratizing innovation*. MIT press.



# Taking Stock of Smart Nation Development in Singapore

*Teck-Boon Tan*

## THE ROAD TO HYPER-CONNECTIVITY

In late 2014, Singapore rolled out the Smart Nation initiative – a mega-digitalisation project to transform the city-state into a hyper-connected nation infused with cutting-edge digital and computing technologies. The basic idea is this: harness the power of these technologies to remediate policy problems and by doing so, deliver to citizens tangible improvements in the quality of life. Four years into the Smart Nation, quite a few projects have been implemented. Underlining the vast complexity involved in using modern technology to improve the human condition, roadblocks have also surfaced on the road to hyper-connectivity. To accelerate Smart Nation development, this paper argues that getting citizens to embrace the related technology is crucial. Because privacy is a major concern, smart technology can be made more acceptable through effective product communication and information. Enhancing digital security will also make a difference. It concludes by suggesting that a finer appreciation of the obstacles encountered so far will inform other Smart Nation projects in the pipeline and even the path ahead.

## The Smart Nation unpacked

Singapore is undergoing an unprecedented digital transformation into a Smart Nation – a hyper-connected city-state where digital and computing technologies are weaved into everything from public infrastructures and offices to homes and everyday objects. In the years ahead, these cutting-edge technologies will be appropriated ever more to help set the country on a more sustainable development path. Heading into its fifth year, the Smart Nation is well into the implementation phase. But roadblocks have slowed its progress intermittently. With that in mind, this article attempts to shed light on what some of these obstacles are. A stronger

understanding of these impediments will not only reveal possible ways to overcome them but also offer valuable lessons for other Smart Nation projects in the pipeline. But first, it is useful to have a sense of where the Smart Nation, as a mega-digitalisation project, is situated in the broader context.

By all accounts, Singapore was never a stranger to digitalisation, having rolled out quite a few digital masterplans since the early 1980s, just as the digital age was starting.<sup>1</sup> Even so, the Smart Nation does differ from past digitalisation efforts in that its core emphasis is on life in the city-state made better by the pervasive application of digital and computing technology. Gone is the emphasis on an economy elevated by computerisation and related manufacturing. In its place are visions of urban spaces made cleaner, safer and more efficient by modern technologies. In the Smart Nation narrative, the city-state is no longer just a place where technology is produced but a nation where it is taken onboard to enhance the quality of urban living. In other words, insofar as Singapore has been a manufacturer of digital and computing technology, it is now also a beneficiary of its many applications. If anything, the idea of being a receptacle for technology goes to the heart of what a smart city is.<sup>2</sup>

In the last decade, the smart city concept has emerged as the much-sought-after answer to many of the policy problems brought on by rapid urbanisation. As more people flood into cities in search of better economic opportunities, health-care and education, the overall quality of life has also deteriorated due to, *inter alia*, stressed infrastructures, inadequate housing, rising crime and elevated levels of pollution. With a high availability of digital and computing technology, the smart city has been held up as the panacea to these urban woes. Specifically, through the extensive application of cutting-edge technologies like the Internet-of-Things (IoT), big data and cloud computing, city managers can now have a better sense of the urban problems they face daily, respond to them faster and in some cases, even detect them before they surface.<sup>3</sup> Signs of this high-tech urban future can already be seen as more progressive cities start to line their streets with multi-functional intelligent streetlights, optimise bus routes with crowd-sourced mobile phone data, automate waste collection and recycling, harness video analytics to fight crime, and more.

---

<sup>1</sup> Kong, Lily, and Orlando Woods, 2018, "The ideological alignment of smart urbanism in Singapore: Critical reflections on a political paradox," *Urban Studies*, 1-23.

<sup>2</sup> Glasmeyer, Amy, and Susan Christopherson, 2015, "Thinking about smart cities," *Cambridge Journal of Regions, Economy and Society* 8, 3-12.

<sup>3</sup> Townsend, Anthony, 2014, *Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia*, New York: W. W. Norton & Company.

At a time when city planners across the world are struggling to cope with today's urban challenges it is no wonder that the smart city concept, with its futuristic vision of a more sustainable urban future, is gaining more appeal globally.<sup>4</sup> From North America to Europe to Asia, municipal governments are eagerly jumping onto the smart city bandwagon. But even as smart cities appear in almost every corner of the world, Singapore is still the sole country to embrace it at the national level. Governments around the world may be scrambling to build smart cities but Singapore is the only one looking to turn the entire country into a mega-smart city. Even Estonia – the former Soviet Republic most often associated with extreme digitalisation – has yet to do so and perhaps, for good reasons. For one thing, the public investment needed for such a mega-project would be massive, not to mention the technical complexity involved.<sup>5</sup> A more digitalised economy is also more vulnerable to cyberattacks, as the Estonians and others have found out over time. That raises the question: why is Singapore embarking on this mega-digital transformation then?

The answer has to do with sustainable development. With few exceptions, the weight of the evidence suggests that the Smart Nation is really a platform to remediate key policy issues of the day. Indeed, post-industrialised Singapore is not without its fair share of challenges – issues that not only cut across different policy domains but also defy easy resolution. Although the country has one of the highest standards of living in the world and regularly tops global rankings in education, safety, life expectancy and so forth, it still faces complex policy issues that, if left untouched, threaten to upend the country's many achievements.<sup>6</sup> The most serious is arguably demographic transition; Singapore is ageing rapidly and to make matters worse, current measures like nursing homes and foreign maids to care for the elderly do not scale very well. While there are certainly other hot-button issues around, demographic ageing is possibly the most severe as it has far-reaching consequences for the country's sustainable development. It is noteworthy that the country has no natural resources whatsoever except its human capital, and an ageing population means that the country will soon find it tougher to sustain economic growth, among other consequences.

---

<sup>4</sup> Albino, Vito, Berardi, Umberto, and Dangelico, Rosa M., 2015, "Smart Cities: Definitions, Dimensions, Performance, and Initiatives," *Journal of Urban Technology*, 22:1, 3-21.

<sup>5</sup> The Smart Nation, as a case in point, is expected to cost an estimated US\$1 billion each year for the next ten years until it is completed.

<sup>6</sup> Tan, Kenneth P., 2017, *Governing Global-City Singapore: Legacies and futures after Lee Kuan Yew*, New York: Routledge.

## DELIVERING SUSTAINABLE DEVELOPMENT

This section explains how the Smart Nation will set Singapore on a more sustainable developmental path. Particularly, it looks into how the initiative tackles an ageing society by harnessing smart technology for senior care. Two enabling technologies form the backbone of this high-tech drive: smart homes and telemedicine.

### Smart eldercare

By 2030, one in four Singaporeans will be aged 65 and above; in absolute terms, the country is looking at roughly 900,000 senior citizens in about a decade's time. In 2017, that number stood at just above 516,000.<sup>7</sup> The reasons behind this rapid demographic change are highly complex but it is essentially the by-product of a high life expectancy and a low birth rate. More importantly, the policy implications of this dramatic demographic trend for the country's development will be profound.

At issue is really how to take care of the sheer number of seniors in the coming years without overwhelming the country's eldercare system. Compounding the challenge is the fact that building many more nursing homes to house the aged would not be feasible in the city-state as scarce land must be set aside for other things like housing and industry. One practical solution to this conundrum is ageing-in-place, the idea of senior citizens living out their twilight years in their own homes while drawing on the support of their loved ones and communities. Needless to say, if ageing-in-place works as it should, then there will be less pressure on the country's eldercare system ahead. Moreover, the idea complements the wish of most Singaporeans to stay put as they age. So, for obvious reasons, a major aspect of the Smart Nation is harnessing the power of so-called smart homes to help Singaporeans age-in-place.

Built by the Housing Development Board (HDB), the government agency responsible for public housing in Singapore, smart homes are essentially apartments infused with a gamut of digital sensors and gadgets to make them safer for elderly occupants. They are, for all intents and purposes, public housing designed and built with seniors' wellbeing and safety in mind. For instance, since the elderly are prone to falls, these next-generation homes are outfitted with smart motion sensors that detect prolonged periods of inactivity – as in when the occupant has fainted after falling. But unlike run-of-the-mill motion sensors, these sensors are sophisticated enough to send an alert to caregivers and emergency services when

---

<sup>7</sup> <https://www.population.sg/articles/older-singaporeans-to-double-by-2030>, accessed 22 November 2018.

something amiss is detected. Other similar enhancements include portable panic buttons and door-contact sensors to help caregivers better monitor the condition and movement of elderly occupants. The former allows elderly occupants in need of immediate assistance to quickly alert their caregivers by just pressing a portable button. Meanwhile, the latter is designed to automatically alert caregivers when elderly occupants (especially those suffering from dementia) leave their apartments and fail to return after an extended period.

But what happens when a senior citizen falls ill and requires long-term continuous medical care at home?

Telemedicine, a term referring to medical care delivered remotely with the aid of information and telecommunication technologies, has been taken onboard to address just that. Originally created to treat patients located in rural areas, the medical technology is now being adapted to deliver healthcare to patients in their homes. Thanks to the advent of Internet-enabled medical devices, teleconferencing equipment and wearable health trackers, doctors can now treat and monitor patients round-the-clock remotely. In addition to these high-tech devices, simple home-use medical devices that let patients collect additional medical information at their doctor's request mean that they only visit the hospital when necessary. Apart from convenience, another major advantage of telemedicine is that with fewer non-essential visits to the hospital, the pressure on the healthcare system as a whole will be reduced. With the aid of webcams and video chat apps, physiotherapists can even conduct online therapy sessions for patients in their homes.

The potential for telemedicine to help ease Singapore's ageing pains is tremendous. Seniors who require medical attention can now receive treatments from healthcare professionals without having to set foot in the hospital. Those requiring physiotherapy can now receive it over the Internet. The technology is especially beneficial for bedbound seniors who require regular visits to the hospital. Fewer hospital visits also lower the risks of hospital-acquired infections. Moreover, because telemedicine typically costs less than medical care delivered in a clinical setting, it is expected to keep healthcare affordable as spending jumps in an ageing population.

As futuristic as smart homes and telemedicine may seem, these technologies are now actually in various stages of implementation to help care for the rapidly growing number of senior citizens in Singapore. Coming together under the umbrella of smart eldercare, these technologies will enable more Singaporeans to not only age safely in-place but also receive medical attention in the comfort of their high-tech homes when illnesses strike. One initial concern was that smart homes, with their sophisticated array of sensors and gadgets, would be priced beyond the



reach of most Singaporeans. That worry turned out to be misplaced when a 2015 smart home project actually priced these apartments at about US\$20,000 for a two-room unit in a popular housing estate, making them affordable for the average Singaporean.<sup>8</sup>

There is no room here to discuss the Smart Nation's extensive list of digital and computing technologies. But from the discussion above on smart eldercare, the use of technology to remediate policy issues and deliver tangible benefits is clearly visible. If anything, it is a recurring theme in the Smart Nation narrative that harks back to the earlier point about how smart cities are not just urban spaces where modern technology is born but also its receptacles and beneficiaries. That being said, as with previous attempts to use technology on a mega-scale to improve the human condition, vast complexities are involved and, accordingly, unexpected impediments – many of which surface only during the implementation phase – are not uncommon. In that regard, the Smart Nation is no exception.

## SMART NATION ROADBLOCKS

This section looks into some of the impediments that have slowed the Smart Nation's progress. As unpleasant as these roadblocks might be, they do offer valuable insights into the complex nature of technology implementation. Indeed, a deeper and more situated understanding of these obstacles can help inform other projects in the pipeline and accelerate the Smart Nation's progress.

### Privacy concerns

At the time of writing, it is generally believed that Singaporeans are not exactly embracing smart homes. Suggestive of the level of interest Singaporeans have for the technology, a pilot project that sought to bring it into 3,000 homes in a HDB housing estate had only about 50 sign-ups.<sup>9</sup> This low uptake is even more puzzling given the country's rapidly ageing population. If anything, there should be strong demand for smart homes.

---

<sup>8</sup> Yeo, Sam Jo, 2015, "First smart HDB homes in Punggol to go for as low as \$28,000," *The Straits Times*, 25 May 2018, accessed 2 December 2018, <https://www.straitstimes.com/singapore/housing/first-smart-hdb-homes-in-punggol-to-go-for-as-low-as-28000>.

<sup>9</sup> Tham, Irene, 2017, "Untangling the way to a Smart Nation," *The Straits Times*, 26 March 2018, accessed 27 November 2018, <https://www.straitstimes.com/singapore/untangling-the-way-to-a-smart-nation>.

Based on information obtained exclusively for this article, the low uptake has little if anything to do with the technology itself as earlier trials – albeit at a smaller scale – had demonstrated that it worked exactly as expected. Neither does the level of technological sophistication of Singaporeans explain it. As a matter of fact, Singapore is among the most wired nations in the world with mobile, Internet and social media penetration rates of about 85 percent, 82 percent and 77 percent respectively in 2017.<sup>10</sup> With those figures, it should be obvious that the level of technological sophistication of Singaporeans and, implicitly, their ability to adopt digital and computing technology, cannot fully account for the low uptake. Even assuming that some senior citizens are not tech-savvy enough to take up smart home technology, their often-younger caregivers should be if there is real interest. Then how might one explain the low interest in smart homes?

A crucial factor is evidently trust or more appropriately, the lack of it vis-à-vis the technology. Indeed, there is evidence indicating that people perceive – though erroneously – the technology as a potential violation of their privacy. This was manifested in the behaviour of seniors taking it upon themselves to cover the sensors in their smart homes with towels during trials. Even though the sensors were designed to detect nothing but motion, the common misperception was that they somehow recorded video and images too. That is to say, the concern was that the technology was operating in a way it was never intended to. Consequently, the sensors were covered up and never given the chance to work. And to be clear, the fear was not even about state surveillance, but rather that the sensors were recording occupants as they changed out of their clothes or went to the bathroom. So, it seems that the cultural context in which the technology was situated in also came into play as older Singaporeans are generally more conservative.

Leaving aside the question of why a tech-savvy population like Singapore's would fall for such misguided notions, the effect of this misperception of smart home technology is obvious and tangible. More importantly, unless a way is found to correct these faulty conceptions, smart homes will likely remain confined to the realm of technological imagination in the Smart Nation as citizens continue to shun the technology – for the wrong reason notwithstanding.

---

<sup>10</sup> <https://wearesocial.com/sg/blog/2017/01/digital-in-2017-global-overview>, accessed 27 November 2018.

## Digital insecurity

Increasingly, it is becoming apparent that smart cities – or more specifically, the extensive array of digital sensors that support them – are vulnerable to cyberattacks and digital manipulations.<sup>11</sup>

Part of the reason is that many of these sensors lack even the most basic protection from malwares. With limited computing, memory and power resources, these so-called resource-constrained devices typically do not come with anti-virus protections, encryptions and firewalls baked into their minimalistic designs. Another reason is that the widespread application of Wi-Fi has exposed these sensors to so-called man-in-the-middle attacks. During such attacks, data flowing between devices can be intercepted and compromised devices can be corrupted into platforms for launching attacks on other systems. It is also entirely possible that the ever-increasing number of Internet-enabled sensors will open up more pathways for malicious hackers to exploit. The worst-case scenario is when hackers wrestle control of critical infrastructures by subverting connected subsystems. As smart infrastructure systems rarely exist in isolation, an attack and subsequent crash in one system could cause a ripple effect and lead to near-simultaneous shutdowns in others.

Since the Smart Nation also utilises a plethora of digital sensors, there are grounds to believe that it too is susceptible to cyberattacks. But exactly how vulnerable the Smart Nation is remains a mystery at this point. One reason is that it is still a work-in-progress with many related projects still in the pipeline and various sensors – to collect real-time data on traffic and environmental conditions, for example – are still not in place. Hence, it is difficult to conclude to what degree the country is vulnerable to large-scale cyberattacks. Furthermore, the government has taken preventive measures like establishing a dedicated cybersecurity agency and air-gapping the entire civil service to better secure the Smart Nation architecture.<sup>12</sup> Even so, the nation got a hint of the pitfalls of extreme digitalisation in July 2018 when it was revealed that the medical records of many patients under SingHealth – the nation's largest healthcare provider – had been stolen by hackers. Indicative of the severity and, to an extent, the sophistication of the attack, the lengthy list of victims included the Singapore Prime Minister himself. Like it or not, the unfortu-

---

<sup>11</sup> Joo, Yu-Min, and Tan Teck-Boon, 2018, "Smart Cities: A New Age of Digital Insecurity," *Survival*, Vol. 60(2), 91-106.

<sup>12</sup> Air-gapping is a digital security measure that involves isolating work computers from unsecured networks like the Internet.

nate fact is that as a country becomes more digitalised, it also turns into a bigger target for malicious hackers.

Beyond the attention-grabbing headlines, incidents like the SingHealth hack can have a chilling effect on the Smart Nation – particularly, on the speed with which it can be implemented. For one, telemedicine will never be as popular if it were shown to leak revealing medical data of users. It is one thing to have plain information like names, birth dates and contact details stolen; it is another to have stolen images of one hooked up to life-sustaining medical devices posted online for all to see. Since public confidence is a key determinant of technology adoption, citizens must have trust in the technology before they bring it into their lives and telemedicine will not be able to deliver tangible benefits – let alone tackle the problems of an ageing society – if citizens shun it.

## **ACCELERATING SMART NATION DEVELOPMENT**

Since Singapore Prime Minister Lee Hsien Loong's remark last year that the country was not moving as fast as it should to realise the Smart Nation, steps have been taken by the government to accelerate plans for its development.<sup>13</sup> They include the formation of the Smart Nation and Digital Government Group in the Prime Minister's Office to drive Smart Nation development and the launch of new projects like the Smart Nation Sensor Platform to fast-track the deployment of much-needed sensors that would help direct autonomous vehicles and improve traffic flows. But apart from those actions, what more can be done, especially in terms of getting citizens to embrace Smart Nation technology?

For starters, more can be done to address the smart home's low uptake. Since the key factor is a flawed conception of the technology – that the sensors in smart homes are violating the privacy of occupants when they are not – better product communication and marketing should help to dispel that wrongful notion. By underlining the function of these sensors to homeowners and drawing their attention to product-specific details, service providers can help drive home the message that these sensors do not violate privacy in any way. Additionally, it will help if positive user experiences are shared more widely since public confidence plays a vital role in technology adoption.

It is also necessary to enhance digital security for devices used in telemedicine if the technology is to gain broader public acceptance. There is no easy answer to how this can be accomplished, not least because cyberattacks are growing in

---

<sup>13</sup> Tham, *op. cit.*, p. 8.

sophistication as they are becoming common. One way, in light of the SingHealth cyberattack, is to adopt strong encryption. If implemented, medical data would be more secure as it cannot be easily read even when stolen by hackers. But the implication of extensive encryption is that resource-constrained devices can no longer be included in telemedicine. So, a trade-off between convenience and security is expected with across-the-board encryption.

Roadblocks are never pleasant. But in the Smart Nation's case, there is a silver lining to them in that they provide an opportunity to gain valuable insights into the complex nature of using technology to improve the human condition. On a more pragmatic note too, a deeper and more situated understanding of the obstacles encountered during the implementation of smart homes and telemedicine can help inform other Smart Nation projects in the pipeline and ultimately, accelerate Smart Nation development. In that sense, as the Smart Nation heads into its fifth year, it is also beneficial to take stock of the last four.

## **FINAL THOUGHTS**

In the beginning of this article, the globally shared problem of rapid urbanisation was underlined. Searching for a better life, people from the countryside are flooding into cities and their actions have paradoxically led to a deterioration in the quality of urban life. The smart city concept, by promising a solution to the assortment of problems brought on by rapid urbanisation, is embraced globally as a result. Taking the smart city concept further than anyone, Singapore has taken it upon itself to become the world's first smart nation. As a first-mover in the pervasive application of cutting-edge digital and computing technology at the national level, Singapore has positioned itself not just as a leader but also as a model for others. With smart cities rising across the globe, it is not a hyperbole to say that the world is watching the Smart Nation. So, proving that smart technology can deliver tangible benefits is not just about realising a vision but also Singapore's chance to inspire many others. And by developing a more refined understanding of the impediments, the path ahead should become easier.

**Dr. Teck-Boon Tan** is Research Fellow and Coordinator of the Science and Technology Studies Programme (STSP) in the Office of the Executive Deputy Chairman, S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore. His research covers science and technology policy, smart urbanism and disruptive technology. He received his PhD from the Lee Kuan Yew School of Public Policy, National University of Singapore.



# Redefining Parity at Work in India

*Terri Chapman*

## 1. INTRODUCTION

Technological adoption and digitisation are changing production processes and business models in India. Workers are shifting out of agriculture and into services and manufacturing by the millions each year. The geographic distribution of employment opportunities is increasingly urban, while 70 percent of the population resides outside of cities.<sup>1</sup> The skills and know-how required of workers are changing with the introduction of new technologies. Simultaneously, the contracts, salaries and benefits that most individuals have come to expect are increasingly rare.

There are a multitude of questions that remain with regard to how the future of work in India will unfold. This paper outlines three trends in employment relations in India driven in part by technology adoption and digitisation: (1) a rise in contractual labour, (2) an increase in platform and on-demand workers, and (3) a rise in freelancing work. In this context, the paper considers the ways in which these trends are creating new forms of inequality at work. These include: a protection gap between traditional and non-traditional workers, a disparity in opportunities for upward mobility and career progression, and greater inequality of opportunity, particularly for women.

The paper proceeds as follows: *section two* discusses the contours of disruption and work in India, focusing on trends in employment relations. *Section three* outlines three dimensions of inequality that must be considered in the context of observed and expected workforce change in India. *Section four* concludes.

---

<sup>1</sup> 2011 Census. The urbanisation rate as of 2011 stood at 31.6 percent.



## 2. THE REORDERING OF WORK IN INDIA

### Background

The vast majority – 92 percent – of employment in India is informal.<sup>2</sup> There are an estimated 42 million small and medium-sized enterprises (SMEs), accounting for 95 percent of firms and 40 percent of total employment.<sup>3</sup> By sector, agriculture remains the largest employer, accounting for 42.7 percent of workers. This is followed by services at 33.4 percent and manufacturing at 23.7 percent of employment.<sup>4</sup>

Wages remain relatively low at an average of 247 INR (3.10 EUR) per day.<sup>5</sup> While the unemployment rate is just 3.5 percent,<sup>6</sup> the labour force participation rate stands at 53.8 percent. Strikingly, the female labour force participation rate is just 23.3 percent.<sup>7</sup> Furthermore, India has seen stagnation in manufacturing employment,<sup>8</sup> and is experiencing a demographic shift in which 1.3 million youth are entering the workforce each month.<sup>9</sup>

At the same time, technological adoption and digitisation are reshaping the nature of industries, jobs, workplaces and work itself. While a significant amount of uncertainty remains with regard to the future, a number of trends can be observed. This section outlines three such trends related to changing employment relations in India: an increase in contract work, the rise of the platform and on-demand economy, and an increasing number of freelance workers. Definitions of these terms are provided in *Table 1*; while these definitions help to highlight the differences between these work arrangements, there are some overlaps and ambiguities between them.

---

<sup>2</sup> A. Srija and Shrinivas V. Shirke, "An Analysis of the Informal Labour Market in India," *Confederation of Indian Industry: Economy Matters* (Year Unknown).

<sup>3</sup> Evoma, <https://evoma.com/business-centre/sme-sector-in-india-statistics-trends-reports>, accessed 21 October 2018.

<sup>4</sup> National Sample Survey Office (NSSO), EUS round 2011-12.

<sup>5</sup> Reserve Bank of India (RBI), 2011-12, <https://rbi.org.in/scripts/PublicationsView.aspx?id=18621>, <https://indianexpress.com/article/explained/meaning-urp-mrp-mmprp/>, accessed 20 October 2018.

<sup>6</sup> World Bank database, year 2017, <https://data.worldbank.org/indicator/SL.UEM.TOTL.ZS?locations=IN>.

<sup>7</sup> World Bank database, year 2012, <https://data.worldbank.org/indicator/SL.TLF.CACT.FE.NE.ZS?locations=IN>.

<sup>8</sup> Radhicka Kapoor, "Creating Job's in India's Organised Manufacturing Sector," *ICRIER*, 2014.

<sup>9</sup> World Bank, "Jobless Growth?," *South Asia Economic Focus*, Spring 2018: 30.

**Table 1: Definition of terms.**

Term	Definition
Contract workers	Contract workers are hired by companies through a third-party contractor to perform a specific job for a fixed period of time. Contract workers typically work onsite alongside permanent employees.
Platform and on-demand workers	Platform workers use online platforms to connect with organisations or individuals that require services in exchange for payment. Like contract work, three parties are involved; in this case it is the online platform, the worker and the client. Jobs are typically broken down into specific tasks carried out by workers and are provided on-demand.
Freelance workers	Freelance workers are self-employed and do not necessarily sit with their client company. Instead, they have tasks and activities outsourced to them directly from the client. While freelance workers may use an online platform to find work, they are not hired through a third-party agency. Freelance workers can be hired for lower skilled tasks, but generally perform high-skilled activities.
Permanent employee	A permanent employee is either a full or part-time employee in a company with an open-ended agreement with the employer.
Temporary employee	A temporary employee is either a full or part-time employee in a company with a fixed-term agreement with a company.

Source: Adapted from The Observer Research Foundation and the World Economic Forum (2018) and Eurofound (2018).

## 2.1 The contractualisation of labour

The overall share of informal workers in India saw a very slight decline between 2004-05 and 2011-12 from 92.7 percent to 91.9 percent. At the same time, however, the share of informal workers in registered/formal firms increased from 13 percent to 17.3 percent as illustrated in *Table 2*.<sup>10</sup> This can in part be explained by the simultaneous increase in contract workers.

<sup>10</sup> A. Srijā and Shrinivas V. Shirke, "An Analysis of the Informal Labour Market in India," *Confederation of Indian Industry: Economy Matters* (Year Unknown).

**Table 2: Formal-informal employment in organised and unorganised firms (%).**

	2004-05		
	Organised	Unorganised	Total
<b>Formal</b>	52	0.3	7.3
<b>Informal</b>	48	99.7	92.7
<b>Total</b>	13	87	100
	2011-12		
	Organised	Unorganised	Total
<b>Formal</b>	45.4	0.4	8.1
<b>Informal</b>	54.6	99.6	91.9
<b>Total</b>	17.3	82.7	100

Source: Adapted from A. Srija and Shrinivas V. Shirke. Data source: Various rounds of NSSO.

Contract workers are individuals hired through a third party to carry out a job, rather than being hired as an employee of a firm. While they are called contract workers, an estimated 68 percent of contract workers in India work without a contract.<sup>11</sup> Kapoor (2016) finds that in the organised manufacturing sector, the share of contract workers rose from 15.7 percent to 26.5 percent between 2000 and 2010. During the same time period, the share of permanent workers declined from 61 percent to 51 percent.<sup>12</sup> The trend towards contractualisation has also been observed in the services sector in India, particularly in the IT and financial industries.<sup>13</sup>

A recent survey by the Observer Research Foundation (ORF) and World Economic Forum (WEF) found that of the 774 surveyed companies, nearly a quarter – 24 percent – hire contract workers. On average, 20 percent of surveyed firms' employees are contract workers. For 59 percent of these companies, the hiring of contract workers is a new trend in the last five years.<sup>14</sup>

The main reasons studies have suggested for the hiring of contract workers compared to permanent employees are: (1) the desire of firms to avoid labour

<sup>11</sup> "Emerging technologies and the future of work in India," *ILO and Tandem Research*, June 2018: 17, ISSN: 2227-4391.

<sup>12</sup> Radhicka Kapoor, "Technology, Jobs and Inequality: Evidence from India's Manufacturing Sector," *ICRIER: Working paper 313* (2016): 8.

<sup>13</sup> "Emerging technologies and the future of work in India," *ILO and Tandem Research*, June 2018: 17, ISSN: 2227-4391.

<sup>14</sup> Terri Chapman, Samir Saran, Rakesh Sinha, Suchi Kedia and Sriram Gutta, "The Future of Work in India: Inclusion, Growth and Transformation," The Observer Research Foundation and the World Economic Forum, 2018.

regulations and the costs associated with compliance,<sup>15</sup> (2) the wage differential in labour cost between permanent employees and contract workers, (3) the lack of bargaining power of contract workers,<sup>16</sup> and (4) the need for a nimble workforce in the face of market and technological uncertainty.<sup>17</sup> The contractualisation of labour is not all bad, as it provides firms with needed flexibility in the context of technological and business uncertainty, but it also creates risks and uncertainty for the workforce that must be addressed through new policies and a reconceptualisation of social security and safety nets.

## 2.2 The rise of platform and on-demand work

Just 15.6 percent of India's workforce are regular salaried workers, compared to 51 percent who are self-employed and 33.5 percent who are casual labourers.<sup>18</sup> Self-employment is therefore already an important characteristic of the Indian economy. On-demand work in India has in many ways emerged as a natural extension of what exists. What is relatively new is the emergence of online platforms such as Ola, India's ride hailing app, and UrbanClap, a platform that matches clients with a wide range of service providers from cleaning to party planning. The emergence of such platforms has been aided by improved digital infrastructure, increasing internet connectivity, and rising mobile phone and device ownership. McKinsey Global Institute (MGI) estimates that between 700,000 and 900,000 technology-enabled jobs were created in India between 2014 and 2017.<sup>19</sup>

Digitisation has in some ways formalised informal micro entrepreneurship in India by linking self-employed workers to online platforms and to government, financial and other services. This has both expanded markets for individuals and created new kinds of income-generating opportunities. Digitally enabled on-demand workers carry out a wide range of activities such as driving, home repair, food delivery and beauty and wellness, typically doing multiple part-time activities at any given time.

---

<sup>15</sup> Radhicka Kapoor and P. P. Krishnapriya, "Informality in the formal sector: evidence from Indian manufacturing," International Growth Center: Working paper, 2017.

<sup>16</sup> Chaurey, Ritam, "Labor Regulations and contract labor use: Evidence from Indian firms," *Journal of Development Economics* 114, 2015, pp. 224-232.

<sup>17</sup> "Emerging technologies and the future of work in India," Ilo and Tandem Research, June 2018: 17, ISSN: 2227-4391.

<sup>18</sup> NSSO Employment-unemployment round 2011.

<sup>19</sup> McKinsey Global Institute, "India's Labour Market: A New Emphasis on Gainful Employment," McKinsey, 2017, p. 10.

## 2.3 The rise of freelancing work

Across the skill-distribution, individuals are finding opportunities as self-employed freelance workers. Firms in India are showing an openness towards engaging freelance and independent workers, with an estimated 20 percent of firms reporting that they hired at least one freelance worker in the last year.<sup>20</sup> The industries most commonly hiring freelance workers in India are professional services, IT services, banking and finance, e-commerce, retail and fast-moving consumer goods (FMCG).<sup>21</sup>

Most freelancing work is concentrated in India's largest cities, Delhi, Mumbai and Bangalore. Freelancing projects are relatively short term, with approximately 61 percent lasting between 1-3 months, and 83 percent between 1-6 months. This points to a likely need for highly qualified or skilled workers to undertake short-term and specialised tasks. It also appears that in India, it is not just start-ups that are hiring freelancers, but also large and multinational companies. The main reasons reported by companies for hiring freelance workers include the cost and difficulty in finding permanent employees.<sup>22</sup>

This section provided a brief overview of three transformations in employment relations in India. These are: a rise in contractual labour, the emergence of platform and on-demand work and increasing freelancing employment.

## 3. THE DIGITAL DIMENSIONS OF PARITY

Labour market transformations driven by technological disruption present opportunities for reducing barriers to access and redefine economic participation in India. The emergence of online platforms, freelancing and remote working, for example, are creating income-generating opportunities that may have been previously unavailable. There is also some evidence pointing to a rising interest in non-standard and flexible work arrangements among India's youth.<sup>23</sup>

---

<sup>20</sup> Terri Chapman, Samir Saran, Rakesh Sinha, Suchi Kedia and Sriram Gutta, "The Future of Work in India: Inclusion, Growth and Transformation," The Observer Research Foundation and the World Economic Forum, 2018.

<sup>21</sup> FlexingIt, "Indian Companies Say I Do to the Freelance Economy," FlexingIt, 2016: 3.

<sup>22</sup> Terri Chapman, Samir Saran, Rakesh Sinha, Suchi Kedia and Sriram Gutta, "The Future of Work in India: Inclusion, Growth and Transformation," The Observer Research Foundation and the World Economic Forum, 2018.

<sup>23</sup> Vidisha Mishra, Terri Chapman, Rakesh Sinha, Suchi Kedia and Sriram Gutta, "Young India and Work: A Survey of Youth Aspirations," *The Observer Research Foundation and the World Economic Forum* (forthcoming).

In the context of the above trends this section argues that with changing labour relations, the dimensions of parity and work are also changing. The section sets forth three dimensions of equality that are increasingly important: a deepening divide in access to social security and protections, rising disparity in career progression and upward mobility, and greater inequality of opportunity, particularly for India's females.

### 3.1 The social security and protection divide

The predominant point of provision for social security is employers. In India, however, the vast majority of workers are not employed in firms that are required to provide protections and benefits. Several of the main labour regulations in India are applicable only to large-sized firms, which account for a small fraction of the nation's companies and overall employment.<sup>24</sup> The rise in non-standard forms of work such as contractual employment also means a deepening protection divide. For instance, 37 percent of companies in India report providing permanent employees with paid annual leave, and 36 percent, paid sick leave. Among contract workers, however, these numbers drop to 15 and 16 percent respectively. Similarly, 24 percent of companies report providing maternity leave to permanent employees, and 11 percent, retirement plans. This is compared to 10 and 5 percent respectively provided to contract workers.<sup>25</sup>

The gap in social security and protections between traditional and non-traditional workers in the formal and informal economies in India persists. The changing nature of work, employment relations and digitisation demand new forms of protections, new points of provision, and new mechanisms for delivery. Without a significant overhaul, inequality in access to and quality of protections and social security will widen.

In order to deliver better coverage to workers that are primarily informal and independent, and increasingly digital, the provision of social security should be linked to the individual rather than to employers. Similarly, the predominant model of place-based protections needs to be reconsidered in the context of remote and digital employment. The types of security and protections against harassment in the workplace need to be redesigned to account for increasing digital engagements

---

<sup>24</sup> Radhicka Kapoor and P. P. Krishnapriya, "Informality in the Formal Sector: Evidence from Indian Manufacturing," *International Growth Center: Working Paper*, 2017.

<sup>25</sup> Terri Chapman, Samir Saran, Rakesh Sinha, Suchi Kedia and Sriram Gutta, "The Future of Work in India: Inclusion, Growth and Transformation," The Observer Research Foundation and the World Economic Forum, 2018.

between workers and employers. Moreover, the types of protections and benefits that are provided need to be adapted, as the protections and benefits needed among independent workers are likely to vary from those of workers in large organised firms.

### 3.2 Horizontal stagnation, not upward mobility

The on-demand economy, freelancing work and contractual work provide much-needed opportunities for generating income. However, the rise in non-standard employment risks increasing income inequality. There is a significant disparity in wages between permanent and contract workers in India, with permanent workers on average making 1.5 times more than contract workers.<sup>26</sup> Today, the top 1 percent of income earners in India hold 21.3 percent of national income, compared to the 14.7 percent owned by the bottom 50 percent of the income distribution.<sup>27</sup> The distribution of wealth is even more unequal. Individuals in the on-demand economy and contractual work not only earn less, but will likely not see major income increases in the medium and long term.

Freelancing and on-demand work also provide few opportunities for career progression and upward mobility. The kinds of jobs and tasks carried out, particularly among contractual and on-demand workers, are unlikely to change significantly over time. That is, the activities and subsequently the required skills of individuals driving for Uber, or subletting their home on a platform such as Airbnb will remain relatively static over time and will have few opportunities to progress upwards. While the ambitions of India's workforce are growing, many of the jobs being created are unlikely to meet their labour market aspirations. This is creating a greater divide between those in the few formal and traditional jobs, and those stagnating in on-demand jobs. In a recent survey, India's youth report that opportunities for upward career mobility, salary and job security are the three most important factors when considering a job. While India's youth have indicated an openness towards new formats of employment, they have a strong desire for upward mobility and the security of traditional jobs.

Research also reveals that workers with non-standard arrangements have significantly less access to training than permanent workers.<sup>28</sup> In the context of technological adoption and digitisation, skilling and upskilling throughout the life

---

<sup>26</sup> NSSO Employment and Unemployment 2004-05.

<sup>27</sup> World Inequality Database, 2015, <https://wid.world/country/india/>.

<sup>28</sup> Andrea Broughton et al., "Precarious Employment in Europe, Part I: Patterns, Trends and Policy Strategy," July 2016, *Directorate General for Internal Policies, European Parliament*, 85.

course are becoming increasingly important. With less access to training, non-standard workers will also face greater barriers in adapting to technological change and subsequent changes in skill demand.

A balanced policy approach will be needed in order to allow for the emergence of new job-creating business models, while at the same time protecting the welfare of workers. Mechanisms for increased income and occupational mobility will also need to be prioritised.

### 3.3 Rising disparities in opportunity

Many argue that freelancing and other flexible employment options provide a gateway for greater female labour force participation. In reality, they may deepen rather than reduce barriers to equal participation. The assumption that part-time or temporary work are desirable for women who need to balance multiple responsibilities will likely reinforce existing inequalities. Approximately 75 percent of freelancing work in India is part-time and 60 percent is remote.<sup>29</sup> Among females surveyed in the *Youth Aspirations in India Survey*, 85 percent report wanting a full-time job. Females also report a strong preference for employment contracts signed directly with their employer, rather than a contract with a third party.<sup>30</sup>

Further, the wages, protections, security and career progression of many non-standard jobs do not avail themselves to lifting females to parity with their male counterparts who occupy the few traditional and secure job opportunities available. India has a significant and persistent gender wage gap of 34 percent.<sup>31</sup> It is greatest among casual urban workers at 39 percent, followed by regular rural workers at 38 percent, casual rural workers at 31 percent and regular urban workers at 22 percent.<sup>32</sup> This gap persists among freelancers, with highly experienced male freelancers commanding remuneration that is 50 percent higher than their female equivalents.<sup>33</sup>

Moreover, an estimated 75 percent of freelancing professionals in India are male, pointing to the fact that new work formats are already replicating existing labour market realities. This also points to the fact that women in India have

---

<sup>29</sup> FlexingIt, "India's Top Tier Freelancers: What They Earn," FlexingIt, November 2017: 9.

<sup>30</sup> Vidisha Mishra, Terri Chapman, Rakesh Sinha, Suchi Kedia and Sriram Gutta, "Young India and Work: A Survey of Youth Aspirations," *The Observer Research Foundation and the World Economic Forum* (forthcoming).

<sup>31</sup> ILO, "India Wage Report: Wage Policies for Decent Work and Inclusive Growth," 2018: 19.

<sup>32</sup> ILO, "India Wage Report: Wage Policies for Decent Work and Inclusive Growth," 2018: 20.

<sup>33</sup> FlexingIt, "India's Top Tier Freelancers: What They Earn," FlexingIt, November 2017: 8.



significantly less access to the internet and mobile devices. Just 30 percent of internet users in India are female.<sup>34</sup> The gender divide is mirrored in access to mobile phones, whereby 33 percent of females have access to a phone compared to 67 percent of males.<sup>35</sup>

The socio-cultural, financial and fluency barriers to accessing and using the internet and mobile devices among women need to be addressed. If the opportunities presented by new formats of work are going to be leveraged, women need equal access to those opportunities. The onus for achieving this is on individuals, households, and the public and private sectors alike. Further, the new digital and remote nature of work presents an opportunity for anonymising freelance and platform workers; this could lead to a reduced bias in hiring and remuneration.

#### 4. CONCLUSION

The employment landscape in India is changing. India is experiencing a demographic shift as its bulging young population enters the working-age population. Employment in manufacturing has stagnated at the same time that individuals are shifting by the millions out of agriculture. At the same time, technological adoption and digitisation are reshaping industries and production processes, business models, and the skill requirements of the workforce.

Digitisation is also enabling the emergence of new formats of work. This paper highlighted three trends in employment relations in India: the increase in contract workers, driven in part by technological disruption and an uncertain business environment; the emergence of the platform and on-demand economy, which is digitally connecting an already independent workforce; as well as an increase in freelancing workers.

Further, this paper argues that with these trends, there are three increasingly important dimensions of inequality that must be at the centre of discussions about the future of work. These are: an increasing social security and protection gap between formal-sector regular workers and non-standard workers; increasing disparity in opportunities for career progression and upward mobility; and finally, increasing inequality of opportunity, particularly for India's females, who have significantly less access to the internet and mobile devices. While new formats of work are creating opportunities for people to earn an income, they are also reinforcing

---

<sup>34</sup> Brian Keeley et al., "Children in a Digital World," *UNICEF*, December 2017: 1.

<sup>35</sup> Rohini Pande and Simone Schaner, "The Mobile Phone Gender Gap: Why does it matter and what can we do?," *EPoD*, 2017.

persistent inequalities, and creating new forms of inequality in the labour market. Without concerted efforts, inequality of access to social security and protections, and inequality in upward mobility and labour market opportunities and outcomes are likely to rise in India.

**Terri Chapman** is an Associate Fellow at the Observer Research Foundation in India, where she leads research on the future of work, education and skills. Her research focuses on the impacts of technology and digitisation on labour markets, employment and social protections. More broadly her research interests include social mobility, welfare, and inequality. Prior to joining the Observer Research Foundation, Terri worked as a management consultant advising public sector clients on regional economic development.



# Dissecting the Rise and Plateau of Digital Payments in India

*Bedavyasa Mohanty*

## INDIA'S DIGITAL PROMISE

In many ways the past decade can be considered the golden age of India's digital transformation. As a nation that bypassed manufacturing-led growth and leapfrogged into a service-driven economy, India has significant expectations from technology and its promise of social and economic development. The recent years have therefore witnessed an unprecedented push towards digitisation and increasing access to both basic technologies and government services. The "Digital India" programme – Prime Minister Narendra Modi's flagship project – encompasses these goals by striving to provide reliable and secure digital infrastructure which can act as a conduit for government services. The programme aims to empower citizens through digitisation of government services while concurrently increasing literacy among many of India's first-generation adopters of technology.

In an effort to remedy India's high levels of income inequality, a significant portion of this push for digitisation is geared towards economic and financial inclusion – towards ensuring that Indian citizens have access to formal means of savings, credit facilities and investment opportunities. Digitisation has also created the opportunity to build an ecosystem that supports more economic activity in cyberspace, not only generating additional value and contributing to the country's growth but also creating incentives for Indian innovation.

In this endeavour, digital payments systems have emerged as a primary indicator of India's technology-led growth – serving previously underrepresented communities<sup>1</sup> and encouraging the growth of disruptive startups. In many ways,

---

<sup>1</sup> Pranav Mukul, "Digital payment push: 1 in 3 rural persons enrolled under DigiDhan Abhiyan opts for Paytm," The Indian Express, 29 December 2016, <https://indianexpress.com/article/business/economy/digital-payment-push-rural-persons-digidhan-abhiyan-paytm-demonetisation-4449410/>.

the success of digital payments represents a maturing of an economy on its way to being truly cashless while also displaying a trust in technology that has so far been missing globally. To be sure, this is no small task. Technological adoption is replete with many challenges that are uniquely Indian. While many of these have been surmounted in recent years, maintaining the momentum of digitisation and growth would truly indicate that the country is moving towards achieving economic parity and perhaps creating an ecosystem that can be replicated in other parts of the emerging world.

These difficulties associated with digital growth can be broadly categorised as those of infrastructure, capacity and regulation. The success of this story depends on reconciling these multifarious challenges while ensuring adequate safeguards for user rights. This paper begins with an overview of India's digital payments landscape. It examines which regulatory principles have spurred the growth of payments and which ones have hindered it. It also takes stock of institutional safeguards currently in place to ensure the security of digital payments in India and offers recommendations to make this growth sustainable.

## A NEW DIGITAL ECONOMY

India's current regulatory push towards a cashless society is mindful of the realities around the lack of digital literacy and lack of access. The Digital India programme hopes to extend banking facilities to the unbanked while simultaneously allowing users to operate their accounts remotely and virtually authenticate their identities and transactions.

This ambitious goal is centred on the Indian government's JAM trifecta (*Jan Dhan-Aadhaar-Mobile*). However, implementation of the programme is often hindered by the aforementioned challenges. The *Jan Dhan* programme<sup>2</sup> is aimed at bringing about comprehensive financial inclusion by ensuring universal access to banking facilities for every household in India. Launched in 2014, it enables access to financial services such as savings accounts, insurance and pension by allowing citizens to open zero-balance accounts. For ease of access, these accounts can be opened by submitting an identity document issued by any government department or a letter issued by a gazetted officer. For those without any valid legal identity, the Aadhaar programme seeks to provide a unique digital identity to all Indian residents – giving those living at the fringes of society the ability to participate in the formal economy. Aadhaar issues a unique 12-digit number to every enrolled citizen

---

<sup>2</sup> Pradhan Mantri Jan Dhan Yojana, "Scheme Details," <https://www.pmjdy.gov.in/scheme>.

that is matched with their biometrics – fingerprint and iris scan – and demographic information – such as address, registered phone number etc. The lynchpin of the JAM programme though is access to a mobile phone that users need to operate these services.

Official sources claim that the JAM trinity has resulted in the opening of as many as 295 million bank accounts since 2014.<sup>3</sup> Up until a few years ago, a significant portion of the Indian population did not have access to banking, thus restricting their ability to conduct high-volume transactions. Although this has significantly improved over the past few years – with almost 80% of adult Indians now having access to financial institutions – many problems persist. Nearly 38% of all Indian bank accounts remain inactive, indicating that their owners are not yet integrated into the formal economy.<sup>4</sup> Even for those that own bank accounts, access to ATMs and commercial bank branches remain woefully inadequate.<sup>5</sup> While the Digital India programme has leveraged technology to create pathways to basic services, the true goal of inclusion is often foiled by the lack of supporting infrastructure.

It was thought that these limitations could be overcome by bypassing institutions such as banks and ATMs. In this regard, mobile payments have been considered a panacea to the physical limitations of the formal economy. And yet, in spite of India's relatively high cellular penetration<sup>6</sup> only about 5% of users access a financial institution over a mobile phone or the internet in 2017.<sup>7</sup> Moreover, while 44% of urban customers have adopted digital payments services, the number drops to a meagre 16% in rural areas. This would indicate that in addition to the infrastructural shortcomings discussed above – such as access to secure smartphones and the lack of network infrastructure – other factors like inadequate digital literacy also cloud schemes meant to increase financial inclusion.

---

<sup>3</sup> Surabhi, "Jaitley sees JAM Trinity ushering in a 'financial inclusion' revolution," Hindu Business Line, 27 August 2018, <https://www.thehindubusinessline.com/economy/policy/jaitley-sees-jam-trinity-ushering-in-a-financial-inclusion-revolution/article9832227.ece>.

<sup>4</sup> Tish Sanghera, "Record Number Of Indians With Bank Accounts. So Why Is Financial Inclusion Low?," India Spend, 22 May 2018, <https://www.indiaspend.com/record-number-of-indians-with-bank-accounts-so-why-is-financial-inclusion-low-13223/>.

<sup>5</sup> For every 100,000 Indian adults there are only 13.3 ATMs and 12.2 commercial branches. See, Abheek Barua, Rajat Kathuria, and Neha Malik, "The Status of Financial Inclusion, Regulation, and Education in India," ADBI Working Paper No. 568 (April 2016), <https://www.adb.org/sites/default/files/publication/183034/adbi-wp568.pdf>.

<sup>6</sup> Ananya Bhattacharya, "Internet use in India proves desktops are only for Westerners," Quartz India, 30 March 2017, <https://qz.com/india/945127/internet-use-in-india-proves-desktops-are-only-for-westerners/>.

<sup>7</sup> World Bank Findex Report 2017.

These setbacks, however, have not dampened New Delhi's enthusiasm and the government continues to steer an administration with "Digital India" as its flagship programme. But in a marketplace where the immediate need is structural overhaul and capacity creation, India remains committed to solving systemic challenges through regulatory intervention. Indeed, what perhaps distinguishes India's digitisation approach from that of western nations is the fluidity of its marketplace – where the government in addition to being a regulator has also assumed the role of an innovator, developing applications and services like the Bharat Interface for Money (BHIM) and the Aadhaar Enabled Payment System (AEPS).

While Aadhaar with its centralised database of over a billion Indians' biometric information remains the current administration's crown jewel, equally noteworthy is the creation of the Unified Payments Interface or UPI.<sup>8</sup> The UPI is a single window payment framework that allows users to transact with banks, mobile wallets or applications. Once connected with a user's bank account through a linked smartphone, the UPI ID allows a user to send and receive money across platforms. The UPI application program interface (API) has also allowed companies like Google<sup>9</sup> and Whatsapp<sup>10</sup> to introduce peer-to-peer payment systems in India. The adoption of UPI has also enabled transactions over Indian digital payment startups like PhonePe to skyrocket.<sup>11</sup> The success of the UPI – marked by the emergence of numerous private payments apps – is partly due to the regulatory ecosystem. However, ongoing developments indicate that a slowdown in this growth may be imminent.

---

<sup>8</sup> IndiaStack, "ABOUT UPI API," <http://indiastack.org/upi/>.

<sup>9</sup> Kul Bhushan, "Tez rebranded as Google Pay: Top features of the UPI-based payment app," Hindustan Times, 30 August 2018, <https://www.hindustantimes.com/tech/tez-is-now-google-pay-here-are-top-features-of-upi-based-payment-app/story-CDZOIW3Es12Mxo1Sx4kj7L.html>.

<sup>10</sup> Arun Mohan Sukumar, "WhatsApp's Integration of UPI-Based Payments Has Strategic Consequences for India's Digital Economy," The Wire, 9 August 2017, <https://thewire.in/banking/whatsapp-upi-bhim-digital-economy>.

<sup>11</sup> Binu Paul, "PhonePe Claims it's the New King of UPI Transactions," TechCircle, 1 August 2018, <https://techcircle.vccircle.com/2018/08/01/phonepe-claims-it-s-the-new-king-of-upi-transactions>.

## REGULATING THE NEW MARKETPLACE

At the heart of India's digital payments infrastructure lies a body called the National Payments Corporation of India (NPCI). While the NPCI self-defines as an "umbrella organisation"<sup>12</sup> for retail payments in India, the body escapes easy classification. Established as a Non-Profit Company and under the provisions of the Payment and Settlement Systems Act, 2007, the NPCI started out as an operator of inter-bank ATM transactions. Today, it manages instant electronic transfers between banks, owns and operates the UPI along with a suite of other digital payment apps, issues the RuPay card, which is a direct competitor to Visa and Mastercard, and drafts guidelines for digital payments in India. It is simultaneously a payments network, a payments app developer and a quasi-regulator.<sup>13</sup>

While the overwhelming majority of shareholding of the NPCI is held by big banks, the body itself answers to the Reserve Bank of India (RBI), the Ministry of Electronics and Information Technology and the Indian Government's think tank, the NITI Aayog.<sup>14</sup> The Reserve Bank of India, which has the overarching mandate of regulating all financial and payment ecosystems in India, approves policies that are drafted by the NPCI, and issues its own guidelines.

This regulatory murk, coupled with the fact that the rate of adoption of digital payments has fallen well below expectations,<sup>15</sup> has raised questions on the competence of the RBI to manage the digital payments ecosystem. Consequently, after 10 months of deliberations, an inter-ministerial committee (that included the RBI) has recommended removing digital payments from under the ambit of the central bank. All members of the committee, with the exception of the RBI, recommended the creation of an independent Payments Regulatory Board so that regulatory institutions can keep up with evolving technologies.<sup>16</sup>

---

<sup>12</sup> National Payments Corporation of India, "About Us," <https://www.npci.org.in/about-us-background>.

<sup>13</sup> Arundhati Ramanathan, "NPCI, The God of Many Things," *The Ken*, 26 February 2018, <https://the-ken.com/story/npci-god-many-things/>.

<sup>14</sup> Arundhati Ramanathan, "Rock. NPCI. Hard Place.," *The Ken*, 11 May 2017, <https://the-ken.com/story/rock-npci-hard-place/>.

<sup>15</sup> Rupa Subramanya, "India is adopting digital payments like never before, but cash too seems here to stay," *Observer Research Foundation*, 16 February 2017, <https://www.orfonline.org/expert-speak/india-digital-payments-cash-here-to-stay/>.

<sup>16</sup> Inter-Ministerial Committee for Finalisation of Amendments of the PSS Act, 2007, "Recommendations to Consolidate and Amend the Law Relating to Payments," Ministry of Finance, Government of India August 2018, <https://dea.gov.in/sites/default/files/Payment%20and%20settlement.pdf>.



## SECURITY VERSUS GROWTH

A large part of the slowdown in the adoption<sup>17</sup> of digital payments in India can be attributed to the overly cautious approach adopted by the Indian regulatory ecosystem – specifically the RBI. Take for instance, the insistence of the central bank on mandatory two-factor authentication (2FA) for all digital transactions. The 2FA requirement, which India has adopted for nearly a decade, is being seen as a model that causes unnecessary friction in payments – especially subscription-based payments – thus hindering the adoption of digital payment systems by businesses.<sup>18</sup> The only consolation that the RBI has provided in this regard is the relaxation of 2FA for card-not-present transactions for less than INR 2000 or approximately 30 US Dollars.<sup>19</sup>

Although the author has previously argued<sup>20</sup> that even this relaxation has the potential to lessen the security of digital transactions across the country, it is undeniable that certain payment models are entirely foreclosed by a mandatory 2FA requirement.

This point was driven home when the UPI 2.0 launched by the NPCI earlier this year also failed to introduce automatic payments. Automatic or recurring payments are what all subscription-based payments rely on and have the potential to increase the number of payments made over UPI manifold. In fact, they were being seen as such an obvious step in the evolution of digital payments that many payment service operators had already designed new payments packages before the UPI 2.0 was released.<sup>21</sup> This too was seemingly a result of the RBI's insistence.

---

<sup>17</sup> Abhishek Waghmare, "Digital Transactions Recede, Threaten 'Digital India'," IndiaSpend, 21 March 2017, <https://archive.indiaspend.com/cover-story/digital-transactions-recede-threaten-digital-india-77955>.

<sup>18</sup> Ranjani Ayyar and Rachel Chitra, "Two-factor authentication hurting subscription business," The Times of India, 22 March 2018, <https://timesofindia.indiatimes.com/business/india-business/two-factor-authentication-hurting-subscription-business/articleshow/63404794.cms>.

<sup>19</sup> ET Tech, "RBI relaxes 2FA norms for online card transactions up to Rs 2,000," Economic Times, 6 December 2016, <https://tech.economictimes.indiatimes.com/news/internet/rbi-relaxes-norms-for-online-card-transactions-up-to-rs-2000/55842254>.

<sup>20</sup> Bedavyasa Mohanty, "Pitting e-customer 'convenience' against cyber security is a dangerous precedent to set," Economic Times, 22 December 2016, <https://economictimes.indiatimes.com/opinion/poke-me/poke-me-pitting-e-customer-convenience-against-cyber-security-is-a-dangerous-precedent-to-set/articleshow/56118896.cms>.

<sup>21</sup> Arundhati Ramanathan, "UPI, India's massive fintech nudge, misses a step: automatic payments," The Ken, 1 August 2018, <https://the-ken.com/story/upi-indias-massive-fintech-nudge-misses-a-step-automatic-payments/>.

While there is an increasing apprehension that these regulatory impulses might deny India the promise of digital transformation, the RBI's approach is not entirely misplaced. In spite of boasting the world's second largest internet user base, internet penetration in India remains under 30% and is restricted mostly to urban centres. The next wave of people coming online will not only be first-generation internet users but will also be relatively lacking in digital literacy. Given these realities, it is not difficult to imagine that relaxation of security standards will adversely affect this very demographic. These threats are only exacerbated when one considers the low institutional capacity among Indian law enforcement authorities to adequately tackle cyber-crimes.<sup>22</sup>

Taken together these issues make the resolution of the digital payments problem in India a complex one. At first it may seem that the answer lies in solving the chicken and egg riddle: should the institutional security architecture be strengthened before increasing adoption of payments or will the opportunity to harvest digital payments-driven growth disappear if regulatory issues are not addressed? The problem may in fact lie in the dichotomous framing of the issue.

## **INCLUSIVE GROWTH AS THE FUTURE**

The reason why the growth of digital payments in India seemed transformative – at least for a while – was because it relied on unnatural market impulses to surge ahead. In the wake of demonetisation<sup>23</sup> of nearly 80% of India's currency, the UPI, for example, saw a 1,540% rise in transaction volumes.<sup>24</sup> This rate of growth is naturally unsustainable. As multiple analyses have subsequently shown, although

---

<sup>22</sup> By one estimate, nearly 98% of cyber crimes in India go unsolved. See, Madan M. Oberoi, "National Capacity Strengthening to Combat Cybercrime," Digital Policy Portal, 21 July 2016, <http://www.digitalpolicy.org/national-capacity-strengthening-to-combat-cybercrime/>.

<sup>23</sup> On 8 November 2016 at 20:15 hrs, in a televised address to the entire nation, Prime Minister Narendra Modi announced that all ₹500 and ₹1000 bank notes would be demonetised and no longer considered valid legal tender effective from midnight. Citizens were given a 50-day window to deposit cash in hand into their bank accounts. The move was expected to reduce the circulation of fake currency in the country, address tax evasion and stop illicit cash-based transactions. However, with the Reserve Bank of India later reporting that 99.3% of demonetised notes had been returned into the banking system, the move failed to achieve its goals.

<sup>24</sup> Shekhar Lele and Arushi Jain, "Demonetisation effect: Digital payments gain new momentum," Pricewaterhouse Coopers, <https://www.pwc.in/consulting/financial-services/fintech/fintech-insights/demonetisation-effect-digital-payment-gain-new-momentum.html>.

digital payments are on the rise, cash-based transactions (a staple of the Indian marketplace) have normalised to pre-demonetisation levels.

The post-demonetisation behaviour also holds important lessons for the Aadhaar programme that has primarily relied on coercive measures for speedy adoption; that Indians may play by new rules when they are forced to, but will likely resort to natural behaviour when the pressure is eased. In addition to the structural complexities of transacting online, this is indicative of a wider distrust that Indians share of internet-based payment systems. Sustainable growth of the sector, therefore, is only possible when wider trust is built in the medium and questions around ease of access are addressed.

The creation of best-in-class standards for network, information and data security can go a long way in addressing some of these trust issues. A familiar refrain from India's security establishment has always been that cyber security is not seen as a board-level priority by technology companies while the companies themselves bemoan non-involvement in standard-setting processes.<sup>25</sup>

To address this, India's standard-setting processes must be harmonised with increased private sector involvement. This can be achieved through continued multistakeholder consultations with the industry, allowing institutions to adopt self-regulatory frameworks wherever possible and increasing transparency in the rule-making processes of institutions like the RBI and NPCI.

When apprehensions around the relaxing-security-for-growth issue arise, Indian regulators can adopt a sandbox approach where market-friendly policies are adopted until enough data can be obtained to make regulatory decisions one way or another.

## CONCLUSION

The one thing that becomes clear is that if India aspires to become a model of digital growth and development for the rest of the emerging economies, then it cannot just rely on exporting Indian technology and solutions to these markets. There are two significant strengths that the Indian marketplace offers. First, the large market size makes it an arduous proving ground for any technology-led innovation. If a digital solution is able to adapt to and scale in the Indian market with its linguistic and structural barriers then the model of growth for that solution is more likely than not sustainable in other parts of the world. Second, despite its

---

<sup>25</sup> Observer Research Foundation, "Securing Digital Payments in India: A Primer," Special Report No. 45, October 2017.

manifold problems, Indian innovation operates within the bounds of a democratic ring-fence. Therefore, the digital solutions exported out of an Indian market will have necessarily demonstrated adherence to strong institutional safeguards.

These expectations also place an additional burden on Indian policymakers. For an economy that to a large part defines its growth in opposition to the Chinese model, India must ensure that it does not bow to the same market pressures (and compromises) that have defined its eastern neighbour.

**Bedavyasa Mohanty** is an Associate Fellow with Observer Research Foundation's Cyber Initiative. His current work focuses on encryption and the regulation of lethal autonomous weapons systems. Bedavyasa coordinates ORF's cyber security capacity building for Indian law enforcement officials and is the convenor of CyFy, ORF's flagship conference on technology, security and society. He is a lawyer by training and completed his BA LLB (Hons) from the National University of Juridical Sciences, Kolkata. Bedavyasa's latest paper, "Hitting Refresh", analyses elements in the data sharing process between law enforcement agencies in India and the US and offers reforms to address them.



# Promoting Prosperity and Providing Protection: Australia's International Cyber Engagement Strategy

*Damien Spry*

## INTRODUCTION

The launch of Australia's International Cyber Engagement Strategy (the Strategy)<sup>1</sup> in October 2017 followed the appointment of that nation's first Ambassador for Cyber Affairs, Dr Tobias Feakin, in early 2017 and updates and expands upon the 2016 Cyber Security Strategy – a flurry of activity reflecting the role that digital networks increasingly play in Australian international relations, trade and investment, and security and strategic concerns. This chapter discusses the Strategy, its priorities and progress to date, in the context of Australian foreign policy, with an emphasis on cyber security, governance and cooperation, and human rights and democracy online.

Australia's Strategy is partly a response to current developments and partly a consequence of persistent geo-strategic realities. Australian foreign policy is based on three pillars<sup>2</sup>: the security alliance with the United States, including the 1951 ANZUS Treaty; the pragmatic (if at times wavering) commitment to middle-power multilateralism through international and including regional institutions; and a deepening, broadening economic and cultural connectivity with the Asia-Pacific (or Indo-Pacific) region. These foreign policy pillars, and the 2017 Foreign Policy White Paper which is the most recent expression of how Australia pursues its security and prosperity in contemporary circumstances, are the essential background for understanding and evaluating the Strategy.

---

<sup>1</sup> Commonwealth of Australia, Department of Foreign Affairs and Trade (DFAT), *Australia's International Cyber Engagement Strategy* (October 2017), accessed 20 July 2018, <https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/index.html>.

<sup>2</sup> Allan Gyngell, *Fear of Abandonment: Australia in the World since 1942* (Carlton: La Trobe University Press, 2017).

Australia is, and has been since colonial days, highly dependent on international networks of capital, trade, people and information. This outward-looking global connectivity remains a source of Australia's prosperity and enriches the country culturally. However, these connections are also potential pathways for unwelcome or malevolent actors. Thus, the Strategy seeks to enhance Australia's advantageous participation in global markets and governance, including through support for the technological and multi-stakeholder governance systems that underwrite the Internet, while protecting Australia from those same systems' apparent risks and emerging threats.

Australia's place in the Asia-Pacific means the Strategy must include and prioritise engagement in a region that is large and diverse – from micro-states in the Pacific to continental powerhouses – as well as being dynamic, turbulent, and potentially dangerous. The re-emergence of China as a global power is the dominant feature of this region's trading and security landscape. For Australia, this is keenly felt: for the first time in its history, Australia's major trading partner, China, is an authoritarian state while Australia's major security partner, the United States, is China's strategic rival. Cyber security, including cyber warfare, and the threat of malicious interference with national political systems, have prompted legislative responses in Australia and rank high among national security priorities. China's use of digital means of surveillance and control is also at odds with Australia's commitment to a free and open internet. Other nations, notably Cambodia and Myanmar, are similarly exploiting online methods of state control that place democracy and human rights at risk. Non-state actors, from terrorist networks to growing cyber-criminal threats, pose increasingly alarming risks for Australia and her partners in the region.

In its Strategy, Australia has outlined how it perceives these risks, threats and opportunities, as well as how it will address them. This paper situates Australia's Strategy in these contexts, outlining the rationale for its approach. It also charts some of its progress to date by considering programs and achievements from the first year of its implementation.

## **THE STRATEGY AND ITS CONTEXTS**

The Strategy is structured around eight related themes: digital trade; cyber security; cybercrime; international security and cyberspace; internet governance and cooperation; human rights and democracy online; technology for development; and comprehensive and coordinated cyber affairs. Each of these themes contains a key goal and a number of related aims (see Table 1).

**Table 1: Australia’s Cyber Engagement Strategy: Themes, goals, aims.**

Theme	Goal	Aims
<b>Digital trade</b>	Maximise the opportunity for economic growth and prosperity through international trade	<p>Shape an enabling environment for digital trade, including through trade agreements, harmonisation of standards, and implementation of trade facilitation measures</p> <p>Promote trade and investment opportunities for Australian digital goods and services</p>
<b>Cyber security</b>	A strong and resilient cyber security posture for Australia, the Indo-Pacific and the global community	<p>Maintain strong cyber security relationships with international partners</p> <p>Encourage innovative cyber security solutions and deliver world leading cyber security advice</p> <p>Develop regional cyber security capability</p> <p>Promote Australia’s cyber security industry</p>
<b>Cybercrime</b>	Stronger cybercrime prevention, prosecution and cooperation, with a particular focus on the Indo-Pacific	<p>Raise cybercrime awareness in the Indo-Pacific</p> <p>Assist Indo-Pacific countries to strengthen their cybercrime legislation</p> <p>Deliver cybercrime law enforcement and prosecution capacity building in the Indo-Pacific</p> <p>Enhance diplomatic dialogue and international information sharing on cybercrime</p>
<b>International security and cyberspace</b>	A stable and peaceful online environment	<p>Set clear expectations for state behaviour in cyberspace</p> <p>Implement practical confidence building measures to prevent conflict</p> <p>Deter and respond to unacceptable behaviour in cyberspace</p>
<b>Internet governance and cooperation</b>	An open, free and secure Internet, achieved through a multi-stakeholder approach to Internet governance and cooperation	<p>Advocate for a multi-stakeholder approach to Internet governance that is inclusive, consensus-based, transparent and accountable</p> <p>Oppose efforts to bring the management of the Internet under government control</p> <p>Raise awareness across the Indo-Pacific of Internet governance issues and encourage engagement of regional partners in Internet governance and cooperation discussions</p>
<b>Human rights and democracy online</b>	Human rights apply online as they do offline	<p>Advocate for the protection of human rights and democratic principles online</p> <p>Support international efforts to promote and protect human rights online</p> <p>Ensure respect for and protection of human rights and democratic principles online are considered in all Australian aid projects with digital technology components</p>



<b>Technology for development</b>	Digital technologies are used to achieve sustainable development and inclusive economic growth in the Indo-Pacific	<p>Improve connectivity and access to the Internet across the Indo-Pacific, in collaboration with international organisations, regional governments and the private sector</p> <p>Encourage the use of resilient development-enabling technologies for e-governance and the digital delivery of services</p> <p>Support entrepreneurship, digital skills and integration into the global marketplace</p>
<b>Comprehensive and coordinated cyber affairs</b>	Australia pursues a comprehensive and coordinated cyber affairs agenda	<p>Enhance understanding of Australia's comprehensive cyber affairs agenda</p> <p>Increase funding for Australia's international cyber engagement activities</p> <p>Coordinate and prioritise Australia's international cyber engagement activities</p>

The strategy is in part an expression of how Australia's traditional interests have been transformed by the inexorable rise of digital communications technologies. This is certainly evident in the sections that discuss the importance of international trade and the support for digital industries, including cyber security but extended to encompass the digitalisation of all aspects of commerce, trade and investment. This aligns with Australian moves to diversify its economy, itself a response to the decline of manufacturing and growth in service industries like international education and tourism, and takes advantage of new tech-related opportunities. These sections of the Strategy that promote trade and global governance are therefore logical extensions of pre-existing, largely bi-partisan and long-standing Australian policies that favour and promote the systems of global governance and market conditions that underpin international engagement in trade and investment and bring these up-to-date bearing in mind new opportunities and risks arising out of digitalisation.

The strategy is more noteworthy as an expression of new confluences of national and international, especially regional, interests that arise out of new kinds of security threats associated with digital communications networks. National security interests are traditionally predicated on Australia's close relationship with powerful friends and allies as well as good relations with neighbours. In this Strategy, they are placed in a new context, one that is characterised by the rise of new types of risk and from a wider variety of international actors, using electronic networks that make borders, and thus security, less easily secured.

The security risks the Strategy seeks to confront are three-fold: criminals, operating for profit; non-state actors, motivated by ideological or political interests, including terrorist organisations and similarly motivated individuals; and

foreign states seeking to infiltrate, interfere or threaten national institutions and democratic processes. According to reports from security agencies, affected companies and the Australian Government, concerns about such threats are rising. For example, in May 2018 Australian Security Intelligence Organisation (ASIO) Chief Duncan Lewis described the threat of foreign interference as being at “An unprecedented scale”<sup>3</sup>. In November 2018 the Australian Cyber Security Centre (ACSC) and Austal, an Australian shipbuilder and defence contractor supplying the Australian, American and Omani navies, announced a hacker had stolen personnel information and (non-sensitive) ship drawings in an extortion attempt<sup>4</sup>.

Australian Government efforts to address such threats include the reorganisation of the intelligence community, including placing the Australian Signals Directorate (ASD) with its offensive cyber capabilities into the Defence portfolio<sup>5</sup>, and the introduction of new laws that specifically address foreign interference. In his speech introducing the legislation to parliament, the then Prime Minister Malcolm Turnbull underscored the cyber threat – “The very technology that was designed to bring us together, the internet, is being used as an instrument of division”<sup>6</sup> – and named China and Russia as countries of concern. China in particular has also been identified as involved in cyber espionage, often targeting the intellectual property of companies supplying Australia’s defence forces. China was reportedly behind cyberattacks on the Australian National University in 2018 and Australia’s Bureau of Meteorology as far back as 2015<sup>7</sup>. And Chinese telecommunications giant Huawei has twice had bids rejected by Australian governments because of concerns about security, the most recent being the effective banning of Huawei from

<sup>3</sup> Bevan Shields, “ASIO chief Duncan Lewis sounds fresh alarm over foreign interference threat,” *The Sydney Morning Herald*, 24 May 2018, accessed 2 November 2018, <https://www.smh.com.au/politics/federal/asio-chief-duncan-lewis-sounds-fresh-alarm-over-foreign-interference-threat-20180524-p4zhdk.html>.

<sup>4</sup> Brett Worthington, “Explainer: Here’s what you need to know about Austal cyber attack and extortion attempt,” Australian Broadcasting Corporation News, 1 November 2018, accessed 2 November 2018, <https://www.abc.net.au/news/2018-11-02/austal-ship-cyber-attack-and-extortion-attempt-national-security/10458982>.

<sup>5</sup> Patrick Walters, “Spies, China and Megabytes: Inside the overhaul of Australia’s intelligence agencies,” *Australian Foreign Affairs* 4 (2018).

<sup>6</sup> Malcolm Turnbull, “Second Reading: National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017,” accessed 1 November 2018, <https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22chamber/hansardr/716f5e71-dee3-40a3-9385-653e048de81b/0193%22>.

<sup>7</sup> Patrick Walters, “Spies, China and Megabytes: Inside the overhaul of Australia’s intelligence agencies,” *Australian Foreign Affairs* 4 (2018).

Australia's 5G network due to the likelihood that it could be required, under Article 7 of China's 2017 National Intelligence Law, to secretly collaborate with Chinese intelligence services<sup>8</sup>.

For its own part, Australia's hands are not entirely clean when it comes to the use of cyber espionage capabilities. Past allegations include spying on then Indonesian President Susilo Bambang Yudhoyono, his wife and other senior officials in 2009<sup>9</sup>, bugging the Timorese Cabinet offices during negotiations over a maritime boundary in 2004<sup>10</sup>, and monitoring mining giant Rio Tinto's negotiations with a Chinese bank during the 2008 financial crisis<sup>11</sup>. Despite these indiscretions, Australia has positioned itself as a trusted partner.

The rising threat to security, whether from criminals, terrorists or countries, is the context for the Strategy and helps explain its sense of urgency and thoroughness. However, the Strategy's emphasis is less on naming cyber attackers – China is included as a potential partner, its statements in support of agreements against cyber theft highlighted – and more on the role that Australia can play in promoting and assisting with cyber security in Asia and especially the Pacific. The logic is clear: under-resourced Pacific Island Nations may prove a weak link in the chain of security required to keep the internet safe. Australia can and in its own interest should address this as a matter of national security, as well as a matter of international diplomacy and development.

## **CYBER SECURITY, CYBER CRIME, AND INTERNATIONAL SECURITY IN CYBERSPACE**

These three closely interconnected themes are the areas where the Strategy is at its most innovative and internationally connected – a measure of how the issues

---

<sup>8</sup> Danielle Cave, "Huawei highlights China's expansion dilemma: espionage or profit," *The Strategist*, 15 June 2018, accessed 25 October 2018, <https://www.aspistrategist.org.au/huawei-highlights-chinas-expansion-dilemma-espionage-or-profit/>.

<sup>9</sup> Michelle Grattan, "Phone spying rocks Australian-Indonesian relationship," *The Conversation*, 18 November 2013, accessed 25 October 2018, <https://theconversation.com/phone-spying-rocks-australian-indonesian-relationship-20445>.

<sup>10</sup> Jonathon Pearlman, "Spy row a threat to Australia's ties with Timor-Leste," *The Straits Times*, 15 August 2018, accessed 25 October 2018, <https://www.straitstimes.com/asia/se-asia/spy-row-a-threat-to-australias-ties-with-timor-leste>.

<sup>11</sup> Angus Grigg and Lisa Murray, "Revealed: How Australian spooks 'spied' on Rio during 2008 debt crisis," *Australian Financial Review*, 25 July 2018, accessed 25 October 2018, <https://www.afr.com/news/policy/foreign-affairs/revealed-six-governments-on-rio-tintos-it-network-during-2008-debt-crisis-20180725-h134my>.

around crime and security are prompting significant transformations in approaches, resourcing and relationships.

Australia defines cyber security as “measures relating to the confidentiality, availability and integrity of information that is processed, stored and communication by electronic or similar means”, and nominates it as “the foundation for the achievement of Australia’s entire cyber affairs agenda”<sup>12</sup>. The fundamental elements of this theme and its goal and aims speak to the core of the entire strategy, firstly in outlining the seriousness of the threat and the consequent need for robust and resilient responses, and secondly in the intrinsic interconnections between national, regional and global actions required.

Australia’s strategic response to cyber threats, therefore, is a combination of robust domestic defensive – and offensive – capabilities and a forward-defence through international engagement. Australia’s cyber security efforts are in concordance with their overall security and strategic positions in that, more than the other themes, they are related to the alliance with the US and the close relationships with their fellow members of the “Five Eyes” intelligence sharing network. The ANZUS Treaty is affirmed in the Strategy<sup>13</sup> as applying to cyberattacks. Since April 2016, Australia has acknowledged that it has an offensive cyber capability and in November 2016, Australia’s then Prime Minister Malcolm Turnbull confirmed that these offensive capabilities were used to target the Islamic State. In 2017, Australia became the first nation to disclose that its offensive cyber capabilities would be directed at “organised offshore cyber criminals”<sup>14</sup>.

Australia’s international engagement prioritises the Asia-Pacific because that is where it has identified threats and vulnerabilities but also because that is where it can have the greatest impact. As with Australia’s aid programs, the closer to home, the more engaged Australia is. Papua New Guinea (PNG), a growing, resource-rich nation with considerable social and political challenges separated from Australia at its closest point by a mere five kilometre stretch of water, is a clear priority. Australia has already committed AU\$14.4 million (US\$10.4 million) for an advanced cyber

<sup>12</sup> Commonwealth of Australia, Department of Foreign Affairs and Trade, *Australia’s International Cyber Engagement Strategy* (October, 2017), accessed 20 July 2018, <https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/index.html>, p. 23.

<sup>13</sup> Commonwealth of Australia, Department of Foreign Affairs and Trade, *Australia’s International Cyber Engagement Strategy* (October, 2017), accessed 20 July 2018, <https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/index.html>, p. 47.

<sup>14</sup> Fergus Hanson and Tom Uren, *Policy Brief: Australia’s Offensive Cyber Capability* (Australia Strategic Policy Institute, 2018), accessed 30 October 2018, <https://www.aspi.org.au/report/australias-offensive-cyber-capability>.

security package for PNG (encompassing technical, policy and training elements, and the establishment of a cyber security operations centre) as part of its focus on cyber-resilience in the Pacific through its Cyber Cooperation Program (CCP)<sup>15</sup>.

Elsewhere in the Pacific, Australia is also supporting the Solomon Islands to establish a cyber security operations centre, and Vanuatu and Tonga to establish national Computer Emergency Response Teams, and has assisted Tonga to develop stronger cybercrime laws, a model approach to more robust legislation for other countries in the region.

More widely, throughout the Asia-Pacific, the CCP includes support for the Asia-Pacific Network Information Centre (APNIC), the Forum of Incident Response and Security Teams (FIRST) to provide cyber security training, including incident response training across the Pacific, and the Pacific Cyber Security Operational Network (PaCSON), launched in April 2018<sup>16</sup>, comprised of government-designated cyber security incident response officials, which shares information, tools, techniques and ideas. The Australian Cyber Security Centre was re-elected as Chair of the Asia-Pacific Computer Emergency Response Team (APCERT) Steering Committee in Shanghai in October 2018<sup>17</sup>, indicating Australia's commitment to, and the region's acceptance of, its leadership in Asian cyber security.

At the ASEAN Regional Forum in August 2017, with Malaysia, Australia co-sponsored a proposal to establish a cyber Point of Contact database to facilitate communication in times of crisis – one of the Strategy's goals – and will pilot the concept in 2018-19. In August 2018, Australia and Indonesia signed a Memorandum of Understanding, with an associated Action Plan, regarding cooperation over the next two years. A Cyber Capability Engagement Program, which has provided training to 20 Indonesian government officials in partnership with the Australian National University's National Security College, is already underway<sup>18</sup>. The ASD's

---

<sup>15</sup> Information provided by email from DFAT.

<sup>16</sup> Sara Barker, "The Pacific Cyber Security Operational Network is now in action," 14 May 2018, accessed 1 November 2018, <https://securitybrief.com.au/story/pacific-cyber-security-operational-network-now-action>.

<sup>17</sup> Australian Government: Australian Signals Directorate, "Australia maintains a key role in international cyber security community," accessed 2 November 2018, <https://cyber.gov.au/about-this-site/media-newsroom/aus-role-in-cyber/>.

<sup>18</sup> Information provided by email from DFAT.

*Essential Eight*<sup>19</sup>, a checklist of strategies to mitigate cyber risks, is scheduled for translation into the ten official ASEAN languages.

Beyond the Asia-Pacific, Australia has established key working-level partnerships to confront cybercrime. The Five Eyes Cyber Crime Working Group shares best practices and operational resources and an Australian Criminal Intelligence Commission (ACIC) Cybercrime Analyst is posted at the FBI International Cyber Crime Coordination Cell in the United States. Another is posted at the National Cybercrime Unit at the United Kingdom's National Crime Authority<sup>20</sup>. Diplomatically, Australia participated in coordinated action to protest unacceptable behaviour by North Korea WannaCry ransomware (December 2017) and Russia (*inter alia*, US Democratic National Committee email hack, 2016 NotPetya malware, February 2018; and cyber operations against the Organisation for the Prohibition of Chemical Weapons<sup>21</sup> and the investigations in the Malaysian Airlines plane shot down in the Ukraine, October 2018<sup>22</sup>). Australia also works closely with the International Telecommunications Union (ITU) and is at the time of writing standing for re-election to the ITU council.

Australia's approach to cyber security demonstrates a combination of international cooperation through leadership and modelling responsible practice, and a capacity and robust willingness to confront threats.

---

<sup>19</sup> Australian Government: Australian Signals Directorate, "Essential Eight explained" (March 2018), accessed 30 October 2018, <https://acsc.gov.au/publications/protect/essential-eight-explained.htm>.

<sup>20</sup> Commonwealth of Australia, Department of Foreign Affairs and Trade, *Australia's International Cyber Engagement Strategy* (October, 2017), accessed 20 July 2018, <https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/index.html>, pp. 42-3.

<sup>21</sup> <https://www.theguardian.com/world/2018/oct/04/how-russian-spies-bungled-cyber-attack-on-weapons-watchdog>.

<sup>22</sup> Senator the Hon Marise Payne, Minister for Foreign Affairs, and The Hon Scott Morrison, Prime Minister, "Attribution of a pattern of malicious cyber activity to Russia," *Media Release*, 4 October 2018, accessed 4 November 2018, [https://foreignminister.gov.au/releases/Pages/2018/mp\\_mr\\_181004.aspx](https://foreignminister.gov.au/releases/Pages/2018/mp_mr_181004.aspx); additional information provided by email from DFAT.

**Table 2: Main Australian and international agencies, networks and programs addressing cyber security/cybercrime.**

<b>Agencies</b>	<b>Role</b>
<i>Australian agencies</i>	
<b>Australian Criminal Intelligence Commission (ACIC)</b>	Australia's national criminal intelligence agency.
<b>Australian Cyber Security Centre (ACSC)</b>	Coordinates cyber security capabilities across the Australian Government. Engages with international partner organisations to share threat information, to cooperate on operational responses to major incidents and to work collaboratively on best practice mitigations. Run by the ASD.
<b>Australian Federal Police (AFP)</b>	Australia's Federal police force, with major emphases on counter terrorism and national security, and interagency cooperation on transnational crime.
<b>Australian Security and Intelligence Organisation (ASIO)</b>	Australia's national security agency responsible for defence against espionage, illegal acts of foreign interference, and terrorism.
<b>Australian Signals Directorate (ASD)</b>	Monitors and intercepts foreign communications. Defends against cyber threats. Conducts offensive (counterterrorism and military) cyber operations.
<b>Computer Emergency Response Team Australia (CERT Australia)</b>	Australia's expert group that handles computer security incidents, now part of the ACSC.
<b>Department of Foreign Affairs and Trade</b>	Australia's government department managing foreign affairs, diplomacy, international trade (through Austrade) and development assistance programs (through AusAID)
<i>International institutions, networks and programs</i>	
<b>Asia Pacific Computer Emergency Response Team (APCERT)</b>	A grouping of leading and national CERTs and Computer Security Incident Response Teams dedicated to the protection of national infrastructure in the Asia Pacific.
<b>Asia Pacific Network Information Centre (APNIC)</b>	The Regional Internet address Registry for the Asia-Pacific region, providing registration services that support the Internet's operation.
<b>Cyber Cooperation Program (CCP)</b>	A program facilitating the development of policies, legislative frameworks and cyber governance institutions to empower Australia's regional partners to safely embrace the benefits of connectivity.
<b>Cyber Security Pacifica (CSP)</b>	Program partnering the AFP with law enforcement agencies in the region to enhance capacity to address cybercrime.
<b>Forum of Incident Response and Security Teams (FIRST)</b>	Network of internet emergency response teams from over 78 countries, promoting cooperation among CERTs through developing and sharing technical information and best practices
<b>Pacific Cyber Security Operational Network (PaCSON)</b>	A network of Pacific governments' technical experts, supported by not-for-profit organisations and academia, with operational cyber security points of contact. Launched April 2018.
<b>"Five Eyes" network</b>	Intelligence sharing arrangement between Australia, Canada, New Zealand, the United Kingdom and the United States.

## HUMAN RIGHTS, DEMOCRACY AND DEVELOPMENT

The human rights and democracy platforms of the Strategy are based on Australia's proclaimed commitment to international human rights standards. It aims to meet its human rights commitments and to promote human rights internationally through advocacy and capacity building. It does this in part through collaboration with the Australian Human Rights Commission, an independent statutory body, and its equivalent national human rights bodies in the region. Australia's engagement with and support for human rights includes participation in the Freedom Online Coalition<sup>23</sup>, a network of 30 governments promoting internet freedoms, and the Digital Defenders Partnership<sup>24</sup>, which provides emergency funding for human rights defenders who are under threat because of their online activities. A key achievement to date is supporting the Human Rights and Technology Conference in Sydney in July 2018, bringing together ten representatives from ASEAN and Pacific nations. The conference produced an issues paper, with an aim to invite participation and feedback and to publish a final report in 2020 – an indication that this area is one still requiring extensive consultation and leadership.

In this context, the Strategy's approach taken toward human rights online has some weaknesses. Foremost among these is the assertion that "human rights apply online as they do offline"<sup>25</sup> and that democratic debates occurs online "just as it does offline"<sup>26</sup>, which occludes – perhaps inadvertently – the specific and new types of threats to human rights because of changes in the techno-social landscape. While making mention of the capacity for governments to use digital means to monitor, harass, intimidate, censor and even persecute citizens (often in the name of national security), the strategy does not adequately consider how information and communications technologies pose additional risks. These risks include, *inter alia*, the potential for Artificial Intelligence and Big Data systems to make discriminatory decisions; the rights of privacy relating to data access, ownership and use; the role of the internet in spreading hate speech and violent extremism; the debate between protection and participation online with respect to child's rights; and the

---

<sup>23</sup> <https://freedomonlinecoalition.com>.

<sup>24</sup> <https://www.digitaldefenders.org>.

<sup>25</sup> Commonwealth of Australia, Department of Foreign Affairs and Trade, *Australia's International Cyber Engagement Strategy* (October, 2017), accessed 20 July 2018, <https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/index.html>, p. 64.

<sup>26</sup> Commonwealth of Australia, Department of Foreign Affairs and Trade, *Australia's International Cyber Engagement Strategy* (October, 2017), accessed 20 July 2018, <https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/index.html>, p. 65.



labour rights of those involved in the extractive and manufacturing industries that are part of the supply chain for digital devices<sup>27</sup>. Access Now, a digital human rights Non-Governmental Organisation, has directly criticised the Strategy on the basis that the explicit right to privacy is not afforded an adequate level of consideration and connects this to Australian governmental efforts to access private citizens' data in the name of policing efforts and national security<sup>28</sup>.

Notable also through omission are sufficient considerations given to the role that the major social network platforms play in undermining human rights and democracy, and what Australia's interventions should be, and should aspire to achieve, in this regard. There are good reasons to believe that engagement with digital media companies, especially Facebook, is desirable and feasible and would promote human rights and democracy in the region. A recent human rights impact assessment of Facebook use in Myanmar, commissioned by Facebook and undertaken by BSR<sup>29</sup>, a business consultancy and research network, makes several recommendations as to how the social media platform could address underlying systemic problems which lead to abuses being facilitated by social media in Myanmar and elsewhere, especially in the ASEAN countries. Because of Australia's ongoing engagement with ASEAN on cyber security matters, this is an area in which Australia could provide assistance through advocacy, networking, and provision of expertise and program funding.

Australia's efforts to promote technology for development include the provision of technical expertise and financial resources to improve digital infrastructure and access. Examples of this include fibre-optic submarine cables for Fiji, Samoa and the Republic of Palau and improved mobile phone coverage in the Solomon Islands and Kiribati<sup>30</sup>. Through the Department of Foreign Affairs and Trade's innovationXchange, Australia collaborates with private sector and university partners to identify and develop projects aimed at upskilling populations in the Asia-Pacific, with a focus on young people, women and girls, and people with disabilities.

---

<sup>27</sup> BSR, "10 Human Rights Priorities for the Information and Communications Technology Sector," 6 December 2017, accessed 1 November 2018, <https://www.bsr.org/en/our-insights/primers/10-human-rights-priorities-for-the-ict-sector>.

<sup>28</sup> Access Now, "Human rights in the digital era: An international perspective on Australia," accessed 25 October 2018, <https://www.accessnow.org/cms/assets/uploads/2018/07/Human-Rights-in-the-Digital-Era-an-international-perspective-on-Australia.pdf>.

<sup>29</sup> BSR, "Human Rights Impact Assessment: Facebook in Myanmar," October 2018, accessed 5 November 2018, <https://newsroom.fb.com/news/2018/11/myanmar-hria/>.

<sup>30</sup> Commonwealth of Australia, Department of Foreign Affairs and Trade, *Australia's International Cyber Engagement Strategy* (October 2017), accessed 20 July 2018, <https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/index.html>, p. 72.

## CONCLUSIONS

The Strategy provides a clear articulation of Australia's priorities, intentions and capabilities. In part, it is an expression of how the country will continue to pursue its national interests in the new techno-social trading and strategic environment. The key pillars of Australian foreign policy, in one sense, have not changed much: the US alliance, its position as a middle-power engaged in and supporting global cooperation through multilateral institutions, and its key relationships in the Asia-Pacific region.

In another sense the Strategy clearly sets out a new purposefulness to Australia's engagement, especially with its near neighbours. Its clarity is also a conscious effort at putting into practice one of its core values: transparency. Together with the 2016 Cyber Security Strategy<sup>31</sup> and successive Foreign Policy White Papers<sup>32</sup>, the Strategy explains Australia's intentions and outlines its capabilities in an effort to reduce the risk of miscommunication with, and to encourage greater candidness from, other international actors. This is one of the Strategy's most laudable objectives.

All nations, governments and policies are faced with the conflict between pragmatism versus principles. The strategy has elements of this in the scant attention to privacy rights. The omission of certain state actors as risks – either to their own people (Myanmar, Cambodia) or to other nations (China, Russia) – can be chalked up to diplomatic prudence. And the shortage of due attention given to digital platforms such as Facebook may be a product of timing – the abuses in Myanmar and the risks to democratic processes both being associated with social media only quite recently. These are, however, areas which Australia's Cyber Ambassador and his department may wish to give further attention to.

Despite these slight concerns, Australia's combination of good standing and comparatively hale resources make its leadership feasible, the interconnectedness of the issues at stake makes its engagement necessary. The purposefulness and thoroughness of the Strategy are in large part cause for confidence; its implementation thus far, likewise.

---

<sup>31</sup> Commonwealth of Australia, Department of the Prime Minister and Cabinet, "Australia's Cyber Security Strategy" (2016), accessed 20 October 2018, <https://cybersecuritystrategy.homeaffairs.gov.au>.

<sup>32</sup> Commonwealth of Australia, Department of Foreign Affairs and Trade, "2017 Foreign Policy White Paper" (2017), accessed 20 October 2018, <https://www.fpwhitepaper.gov.au>.

**Dr. Damien Spry** is a Lecturer in Media and Communications at the University of South Australia and a Visiting Fellow at the Digital Media Research Centre at the Queensland University of Technology. He has previously held academic positions in Hong Kong, Japan, South Korea and the United States of America. His scholarly research focuses on digital media impacts on international politics and diplomacy. He has developed the Facebooking diplomacy database for this purpose. He is a regular contributor to think tanks, including the Lowy Institute and the Australian Strategic Policy Institute, and has consulted for several multinational companies, including Google, Facebook and Amnesty International, as well as to several governments.

# Asia Pacific Contributions to International Cyber Stability

*Caitríona Heint*

## INTERNATIONAL CYBER STABILITY

This article examines activities in the Asia Pacific related to normative proposals for restraining self-interested state activity in the field of cyber.<sup>1</sup> In the absence of a global agreement for international cybersecurity in the immediate future, this article outlines the potential for other multilateral efforts and regional activities in the Asia Pacific to promote common views, and universalise norms as stepping-stones to progress for an international governance framework. More research is needed now to address issues of stability and escalation control, which some scholars believe is arguably more important (or achievable) than seeking military superiority.<sup>2</sup>

While there did not seem to be consensus within the 2016-2017 United Nations Group of Governmental Experts (UN GGE) for new norms, nor does there seem to be an appetite for new norms in Asia Pacific discussions, new norms could potentially develop in other forums. In any case, this article is timely given the recent increase in attention on regional activities as a means to forge progress beyond the UN GGE.

Many states in the region recognise their self-interest in ensuring that cooperation in this field continues to support market interdependence, as well as regional economic and social growth. This is particularly the case where many

---

<sup>1</sup> The author explored similar questions surrounding the cyber-world order nexus for a panel session, "World disorder, cyber norms and grand strategy: the search for peaceful equilibrium", MIT-Harvard International Conference on Cyber Norms 5.0, March 2017. This article is adapted to focus on the Asia Pacific from the author's subsequent article: Caitríona Heint, "Cyber dynamics and world order: Enhancing international cyber stability", *Irish Studies in International Affairs*, Royal Irish Academy, 2018.

<sup>2</sup> Jason Healey, "Triggering the New Forever War, in Cyberspace", *The Cipher Brief*, 1 April 2017, <https://www.thecipherbrief.com/triggering-new-forever-war-cyberspace>, accessed 11 June 2018.

Asian countries' digital strategies consider the digital economy to be essential to their visions for future prosperity. Even where there are worries that international cybersecurity negotiations are currently stalling, economic self-interest that is often linked to the digital economy or smart city concepts (such as Singapore's "Smart Nation" ambitions) can sometimes explain why progress has already been made – and may continue to be made – in the field of cyber compared to other domains. Moreover, such delays can be part of the natural course of deliberations in a relatively new field where international discussions first began twenty years ago when Russia tabled a draft resolution in the First Committee of the UN General Assembly. It will continue to take time for this field to develop over the longer term. Indeed, the 2015 GGE consensus report specifies that the 11 voluntary non-binding norms' implementation may not be immediately possible.<sup>3</sup>

The need for political willingness, especially among the major powers, will continue to be a key factor in progressing with the development and implementation of norms of state behaviour and confidence-building measures (CBMs). A key concern raised following the 2016-2017 UN GGE is that the previous GGE meetings and work within regional bodies such as the Organisation for Security and Cooperation in Europe (OSCE) and ASEAN Regional Forum (ARF) took place in a more favourable international security environment. Many recent and ongoing geopolitical tensions do not bode well for such political willingness, and economic self-interest may not always outweigh such tensions. Nonetheless, leaders in countries like Singapore, while recognising this challenge, still advocate that although all 11 norms of the 2015 GGE are not ideal, they are practical and it is better to move forward by focusing upon their implementation.<sup>4</sup>

Given that state competition and self-interest can often have greater influence on state practice than norms, a number of trends such as intensifying major power rivalry, rising nationalism as well as challenges to the rule of law and international human rights obligations are making it even more difficult to find common ground on state behaviour in cyberspace. While these are trends that are being witnessed globally, many Asian countries such as Myanmar, Cambodia and the Philippines, among others, are now criticised for regressing. Asian countries can be significantly

---

<sup>3</sup> UN General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", A/70/174, 22 July 2015, pgh. 14, p. 8, <http://undocs.org/A/70/174>, accessed 12 June 2018.

<sup>4</sup> Author observations, United Nations Institute for Disarmament Research (UNIDIR) and CSIS, "International security cyber issues workshop: Preserving and Enhancing International Cyber Stability-Regional Realities and Approaches", September 2017. Experts, including the author, explored these questions in preparation for the workshop.

diverse in terms of cultural and political sentiments where, for instance, Japan, India, and Korea are rather different to China or Southeast Asia when it comes to openness and democracy. This difficulty is exacerbated by different conceptions of world order and conceptual understandings of cybersecurity and information security, including disruptive state behaviour in multilateral cyber efforts. China and Russia have been criticised for sometimes playing a disruptive role in multilateral cyber efforts on CBMs and transparency in forums like the UN GGE, ARF, and OSCE. Given calls at the highest levels in the Asia region for reform of the multilateral order and recognition of multi-polarity, scholars must therefore continue to consider the potential impact of these developments on cyber conflict and stability. This includes, for instance, the ambitions and need for more states in the region to become involved in shaping the agenda.

Given the palpable levels of dissatisfaction with the current post-World War Two order that is perceived by some Asian countries as Western-centric, states seem more willing to engage in cyber-enabled influence operations and low-level activity below the threshold of armed conflict to bring about change in the international security architecture. In other words, state parties and their proxies are more willing to pursue their ambitions to change the current order and undermine democracies with cyber-enabled tools without resorting to the use of military force, and without fear of major retaliatory consequences. While liberal democracies are particularly vulnerable to these types of activities, state espionage and political influencing will most likely continue, which means that states must develop more robust cyber defences and strengthen the resilience of their citizenry to these types of activities. The majority of attention is currently focused on Russian influence and information operations, yet rising global powers in the Asia region such as China also have ambitions in order building. Several national strategies delineate that cyber operations also include information operations – information security and hybrid conflict are aspects of national strategies in powers like China that have different conceptions of world order. This will then continue to have implications for the development of international cyber norms vis-à-vis liberal democracies' understanding of cybersecurity. This point is captured well in the following analysis of the recent 2018 election in Cambodia where “[j]ust as various countries in the developing world – including Cambodia – served as locations for proxy wars between the US and the Soviet Union and their respective allies during the Cold War,

Cambodia is once again functioning as the location for a new proxy war, this time with China leading the alternative to the US-led liberal world order.”<sup>5</sup>

This article therefore argues that it is important to persist with ongoing endeavours at national and bilateral levels as well as among like-minded groupings, regional bodies, and informal mechanisms to create a regime for international cyber stability.

## NATIONAL ENDEAVOURS

Regional policymakers’ understanding of cyber-related issues has become far deeper and more nuanced in recent years. Not so long ago, many of these countries did not even hold national views on these questions. This means that current and future discussions on international security cyber issues will become more complex and require more time given that more experts, actors and agencies will be involved. Even in 2016, it was clear then that there is now a “new negotiating dynamic, driven by broader participation and by contending concepts of cybersecurity”, which was considered likely to make reaching consensus in the 2016-2017 GGE more challenging.<sup>6</sup> Likewise, progress in forums such as the ARF and ASEAN will likely be affected by such broader participation. While this is likely to delay progress, it is also a positive indicator when more states continue to become involved in shaping the development and implementation of cyber norms and CBMs. For example, states such as Brunei and Singapore, which were not highly active previously in their international cyber engagement activities, submitted national views on how to implement norms to the UN Office for Disarmament Affairs (UNODA) in 2017.

Such endeavours thus provide opportunities for these states to take ownership of the agenda, especially where they may not have been members of previous GGEs. Prime Minister Modi earlier argued that the voices of many rather than the few should shape the agenda.<sup>7</sup> This type of thinking resonates in the cyber stability agenda where more countries should ideally become involved in this process of developing rules of responsible state behaviour. Even with an uptick in state sub-

---

<sup>5</sup> Alvin Cheng-Him Lim, “The Spiral Repetitions of Cambodia’s 2018 General Election”, Asia Dialogue, <http://theasiadialogue.com/2018/08/09/the-spiral-repetitions-of-cambodias-2018-general-election/>, 9 August 2018, accessed 10 August 2018.

<sup>6</sup> James Lewis and Kerstin Vignard, “Report of the International Security Cyber Issues Workshop Series”, UNIDIR and CSIS, 2016, 11.

<sup>7</sup> Author observations, Raisina Dialogue, “The New Normal: Multilateralism with Multipolarity”, Observer Research Foundation, New Delhi, 17-19 January 2017.

missions from the region (such as Singapore and Brunei) to UNODA, more states, including smaller states, can hopefully become more involved.

A number of countries in the Asia Pacific continue to make considerable efforts to champion aspects of the international cybersecurity. Malaysia was a member of two GGEs, and for many years it has advocated regionally for transparency as a means to contribute to confidence building as well as support for CBMs. It has done so through efforts such as co-hosting several ARF workshops on CBMs and capacity building, as well as publishing new cybersecurity strategies that outline how it intends to position itself internationally and regionally. Countries like Japan, the United States, Australia, and China, among others, are particularly active in terms of international engagement (although US diplomatic engagement in multilateral forums has lessened in the wake of the Trump administration). The United States and Australia have devoted much time to regional engagement through, for example, workshops on CBMs and capacity building endeavours. Once Japan organised itself nationally, it too has become highly active in international and regional engagement. In particular, the country has shown regional leadership in its work on technical capacity building, cyber capacity building and norms, including work with ASEAN members on capacity building. The Japan Computer Emergency Response Team (JPCERT) is also considered to be a leader in the region.

Indonesia and Korea have both been members of former GGEs on a number of occasions. Korea participated in the last four GGEs, and it hosted the Global Cyber Space Conference in 2015. The country continues its work in this space through initiatives such as driving regional awareness of the latest GGE proceedings in East Asia, and interregional workshops. Smaller states such as Singapore became highly active in their international engagement in recent years – launching, for example, a regional cyber capacity building programme in support of norms and CBMs implementation as well as leveraging regional institutional mechanisms like ASEAN for global influence.

Likewise, while India has become more engaged with broader global order issues in recent years, scholars note the country's ambitions to be a stabilising influence in the world system by being a rule-setter and security provider in contested spaces such as cyberspace and sensitive technologies.<sup>8</sup> It was, for instance, a member of the 2016-2017 GGE, and it hosted the 2017 iteration of the Global Conference on Cyber Space (GCCS). India also became a Co-Chair of the Global Forum on Cyber Expertise (GFCE). These types of activities are important given that countries like

---

<sup>8</sup> Ibid.



India and China have such large populations that they can have a significant effect on the global digital ecosystem.

Even with a swell of regional activities in this field in recent times, it is still the case, however, that cybersecurity and information security may not be a priority issue in other countries in the region such as Cambodia. There is a well-known regional developmental and digital divide, which means there is significant diversity in terms of cyber maturity (there is even an urban-rural digital divide within countries like India and China). This divide between countries like Cambodia, Myanmar, Laos and Vietnam and other Asian countries is particularly evident in regional institutional groupings like ASEAN and the ARF. Several Southeast Asia countries are still figuring out how to communicate effectively domestically (between government ministries and agencies) which can thus impact international cooperation. This situation is exacerbated by the ongoing need to continue coordinating national level policymaking and the integration of fast-developing technologies within those policies. These uneven levels of capacity could also affect the consensus required for future progress within regional institutional mechanisms such as ASEAN, thus affecting its collective ability to inform the global cyber norms discussion. Moreover, debates continue about the impact of such digital divides and lack of capacity to address attacks upon states' international obligations.

As it stands, Asian states' varying understanding of cybersecurity and what they perceive to actually constitute a cyber threat will continue to shape their domestic priorities (security interests also vary widely between countries in the region). This will continue to impact attempts to find common ground and different interpretations of norms. In addition, infrastructure needs, concerns about non-interference in internal affairs, geopolitical support, and regime changes are factors that can impact international and regional cybersecurity developments such as capacity building, or the consensus needed in forums like ASEAN. For instance, the Duterte regime seems more willing to realign towards China in exchange for infrastructure investment at the expense of America (even with the state's traditional alliance with the United States).<sup>9</sup> The Philippines has been Co-Chair of the ASEAN Defence Ministers' Meeting-Plus Expert Working Group on cyber, and there have been occasions where officials were not authorised to attend regional cyber events. This could impact regional efforts to enhance transparency and trust by building communities of interest through regular meetings and conferences. Indonesia, too, has been willing to receive infrastructure investment and diplomatic support from

---

<sup>9</sup> See "The Rise of Duterte: A Populist Revolt against Elite Democracy" by Richard Heydarian for more information about the impact of the rise of China.

China. In return for geopolitical support (such as Cambodia's advocacy in ASEAN for China's position on the South China Sea dispute) China has apparently provided aid and investment as well as support when Cambodia faced United States and European sanctions for human rights violations.<sup>10</sup> The country also apparently received from China "US\$20 million worth of support for the 2018 election, 'including polling booths, laptops and computers.'"<sup>11</sup>

Furthermore, while concerns about terrorism and fake news have heightened globally in recent years, those regional states which understand cybersecurity as including risk to their political, military, social and cultural landscapes in addition to risk to infrastructure are particularly worried about social stability and Internet control. The heightened concerns about terrorism, and more recently fake news, have brought about an increase in the introduction of counter-terrorism and cyber legislation in the region. A key concern is whether this legislation could sometimes be introduced as a means for illegitimate content control. For example, Malaysia's introduction of a "fake news law" in 2017 just before the election is criticised as being designed to suppress criticism of former Prime Minister Najib and the ruling party at that time.<sup>12</sup> Another key question is how cyber capacity building should be conducted where values may not be compatible, particularly where there might be valid capacity building requests for assistance, including technical training and programmes to investigate in order to tackle violent extremism online, but a risk that these skills could be then used for surveillance.<sup>13</sup> Large democracies like India have the potential to provide a model for other countries where there are genuine concerns about countering violent extremism online and "fake news".

The ways in which states in Europe and the United States now choose to tackle these types of trends as well as nationalism, hate speech, freedom of expression and anti-democratic sentiments are watched closely by states in this region. Even where there is parliamentary oversight in liberal democracies to provide a system of checks and balances, they are sometimes accused of hypocrisy. This situation is not helped by the current United States administration, which is so far less attentive to democracy and human rights matters. This is leaving – has already left – a vacuum in the region (even where many countries effectively share, albeit to varying degrees, similar Confucian internal stability and social harmony concerns).

---

<sup>10</sup> Cheng-Him Lim, "The Spiral Repetitions of Cambodia's 2018 General Election".

<sup>11</sup> Ibid.

<sup>12</sup> Austin Ramzy, "Hopes for New Era of Malaysia Free Speech Are High, but Pending", *New York Times*, 18 June 2018.

<sup>13</sup> OSCE and Ministry of Foreign Affairs Republic of Korea, "Inter-regional Conference on Cyber/ICT Security", Background note, Seoul, 2 March 2017.

Others explain that, for now, the Chinese government seems content to quietly push its arguments on cyber sovereignty to receptive leaders, although there is some evidence that this lobbying is becoming more active given the general US retreat across a range of multilateral forums.<sup>14</sup> In other words, there is a perceived risk that China could provide other countries with an attractive example of a successful economic model that continues to align with its own cultural values and conception of world order. China is willing to support capacity building that aligns with its cultural and political values, and Singaporean cyber capacity building programmes also continue to reflect the country's own positions on these subjects. This article concludes that such differences between states on Internet sovereignty and information control are not likely to change in the near future.

## **BILATERAL AND LIKE-MINDED EFFORTS**

Many endeavours at bilateral level and among like-minded groupings such as multilateral memorandums of understanding (MOUs) enable the opportunity to make progress by sharing experience, finding common ground, implementing norms that could extend to larger groups, and capacity building to support OSCE/ARF CBMs. However, such endeavours should ultimately aim to complement global efforts to support international cyber stability (and not add further uncertainty and fragmentation).

Many bilateral MOUs, such as the Singapore-Thailand MOU of 2016 to share experience, have been agreed in recent years. Joint statements such as the United States-Singapore statement in August 2016 were also successful in affirming these states' commitment to the applicability of international law to state conduct in cyberspace and commitments to promote voluntary norms of responsible state behaviour in cyberspace. Bilateral efforts can often be easier for states to make progress where, for example, countries like the Republic of Korea may have found it easier to deal with other states bilaterally rather than regionally due to its difficulties with North Korea.

Similarly, regional countries sometimes find like-minded initiatives useful where progress on cyber issues within regional and international mechanisms such as the ARF and GGE are not seen to work effectively. In addition, steps have been taken to push the international security cyber agenda within like-minded forums

---

<sup>14</sup> Scott Shackelford and Frank Alexander, "China's cyber sovereignty: paper tiger or rising dragon?", Asia & the Pacific Policy Society, 12 January 2018, available at <https://www.policyforum.net/chinas-cyber-sovereignty>, accessed 11 June 2018.

such as the G7 and G20. Multilateral MOUs have also been agreed such as the United States-Japan-Australia-India MOU, as well as joint ministerial statements by Japan, the United States and Australia committing to coordinate in international forums like the UN GGE and ARF.<sup>15</sup> Singapore, too, initiated a Forum of Small States meeting on the sidelines of the previous GGE in 2017. More recently, the coordinated joint United States-United Kingdom statement regarding Russian malicious cyber activities affords an opportunity for other states to join with the goal that a large enough group of nations that feel and act the same way about acceptable and unacceptable behaviour can use that coalition to put pressure on those who are not behaving the way they should.<sup>16</sup> The recent coordination of international attribution is both an example of like-minded groups sending a deterrent message, while also affording other states the opportunity to join them in agreeing upon acceptable state behaviour. Likewise, there are regional calls to bring groups of developing countries together on key issues given the apparent need for a more equitable dispersal of power – this may become even more apparent in the field of cyber where countries like China cite concerns about developing countries in cyber negotiations.

These types of activities further provide an example of broader world order trends identified by intelligence communities whereby a future international environment of competition and cooperation among major powers will probably result in “ad-hoc approaches to global challenges that undermine existing international institutions”.<sup>17</sup> Nonetheless, this article finds that while like-minded initiatives can help to make progress in this field, states should ideally work to ensure that these endeavours do not cause further uncertainty and fragmentation that is “insulting to global norms”.<sup>18</sup>

---

<sup>15</sup> Office of the Spokesperson, “Joint Statement of the Japan-United States-Australia Trilateral Strategic Dialogue”, United States Department of State, 25 July 2016.

<sup>16</sup> Levi Maxey, “Russia Hacks Its Way to the High Ground of the Internet”, The Cipher Brief, 16 April 2018, available at [https://www.thecipherbrief.com/article/tech/u-s-uk-blame-russia-probing-internet-routers-globally?utm\\_source=Join+the+Community+Subscribers&utm\\_campaign=83d511a588-EMAIL\\_CAMPAIGN\\_2018\\_04\\_17&utm\\_medium=email&utm\\_term=0\\_02cbee778d-83d511a588-122471557&mc\\_cid=83d511a588&mc\\_eid=c1f2be183c](https://www.thecipherbrief.com/article/tech/u-s-uk-blame-russia-probing-internet-routers-globally?utm_source=Join+the+Community+Subscribers&utm_campaign=83d511a588-EMAIL_CAMPAIGN_2018_04_17&utm_medium=email&utm_term=0_02cbee778d-83d511a588-122471557&mc_cid=83d511a588&mc_eid=c1f2be183c), accessed 12 June 2018.

<sup>17</sup> United States Office of the Director of National Intelligence, “Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community”, Senate Armed Services Committee, James R. Clapper, Director of National Intelligence, 9 February 2016, available at [https://www.dni.gov/files/documents/SASC\\_Unclassified\\_2016\\_ATA\\_SFR\\_FINAL.pdf](https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf), accessed 8 June 2018, p. 16.

<sup>18</sup> Healey, “Triggering the New Forever War, in Cyberspace”.

## REGIONAL SECURITY ARCHITECTURE

The regional level is sometimes considered to be more suited to implementation of norms and CBMs whereas the global level is more suited to agreements and norms. A robust regional security architecture supported by activities in groupings such as ASEAN, the ARF, East Asia Summit (EAS), ASEAN Defence Ministers' Meeting (ADMM), Shanghai Cooperation Organisation (SCO) and BRICS are often considered important for international and regional stability. The OSCE, Organization of American States (OAS), and ARF have already made some progress in building common understanding and identifying cyber CBMs for regional application – for example, the OSCE's 16 CBMs and the ARF Workplan which aim to operationalise international cybersecurity norms (the ARF has particular strategic importance given the membership of major powers such as the United States, China, Russia, India and Japan, even where this diverse membership could make it more difficult to find common ground).

The Heads of State or Government of the ten ASEAN members and the United States also agreed the Sunnylands Declaration in early 2016 where they committed to promote security and stability in cyberspace consistent with norms of responsible state behaviour. The 2017 ASEAN Cybersecurity Cooperation Strategy was later agreed under Singapore's vice-chairmanship of the ASEAN Network Security Action Council to focus on norms and a cooperation and capacity building framework. The strategy's aim to coordinate cyber policies across the many forums in ASEAN's political-security, economic, and socio-cultural community pillars is significant insofar as it will hopefully support international cooperation. However, it is expected that strategy and international cooperation matters will be examined through the Telecommunications and IT Ministers Meeting (TELMIN). This may not be the best forum to make progress on strategic and security issues, like norms development, especially where the TELMIN and political-security communities can often differ in their understanding of, and approach to, cybersecurity issues. For similar reasons, the ARF Inter-Sessional Meeting (ISM) on cybersecurity was recently established. By continuing to hold these cyber discussions under the ISM on counterterrorism and transnational crime, it could potentially affect how norms and strategy would develop.

Developing and implementing CBMs is considered urgent over the short to medium term in this field to reduce near-term risk by dealing with issues related to misperception and miscalculation. This should ideally reduce the potential for conflict by providing de-escalation mechanisms, especially where it is difficult to assess

or count cyber capabilities.<sup>19</sup> There is an identified need for better communication and coordination between states (as well as across national governments), and a real necessity to move beyond awareness-raising on CBMs to actual implementation and follow-up after meetings.<sup>20</sup> Much awareness-raising has taken place in ARF and ASEAN meetings in recent years, but little progress on concrete implementation. This is particularly important where CBMs and capacity building can assist states to find common understanding of their normative commitments.

Regular meetings and practical exercises (such as the table-top exercises previously held in ARF, OSCE and ASEAN meetings) can continue to assist this process of building capacity and confidence.<sup>21</sup> In terms of capacity building, many states in the region are still challenged by the speed of technological changes, they often lack technical capacity and gaps in the law persist, which is hindering international cooperation and exchange of good practice. GGE experts agree that capacity building is essential for both cooperation and confidence building.<sup>22</sup> Singapore's ASEAN Cyber Capacity Programme has thus included a number of regional workshops on CBMs, capacity building and norms, including the first formal ASEAN workshop on norms in May 2017. The goal is to provide resources, expertise and training to enable ASEAN members to more proactively participate in the international cybersecurity agenda. The country also launched the annual ASEAN Ministerial Meeting on Cybersecurity in 2016 to identify ways to increase cooperation and continue the development of norms in ASEAN states. These initiatives seem to have helped to pave the way for Singapore to present ASEAN's perspectives at the global level through the ASEAN statement to the UN at the end of 2017, thus contributing to the international cyber stability agenda.

Some of the OSCE and OAS work on CBMs could also provide good practices for other regional bodies such as the ARF, while successful ARF confidence building table-top exercises were introduced within OSCE meetings. There is space to further increase such examples of cross-regional exchange of good practices and interregional cooperation (although the work within these regional forums is far from done). Interregional cooperation can work towards ensuring complementarity

---

<sup>19</sup> Author observations, "ASEAN Cyber Norms Workshop", Singapore Cyber Security Agency, 8-9 May 2017.

<sup>20</sup> Ibid.

<sup>21</sup> Author observations, "Australia-Singapore Cyber Risk Reduction Workshop", Singapore Cyber Security Agency and Australian Department of Foreign Affairs, 6-7 December 2017.

<sup>22</sup> UN General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", A/70/174, Summary.

globally so that measures within regional bodies like the ARF and ASEAN do not evolve in such different directions that they cause further fragmentation. Some recent examples of efforts to identify and promote synergies between different regional efforts in order to promote global cyber stability include the joint OSCE and Ministry of Foreign Affairs of the Republic of Korea Inter-regional Conference on Cyber/ICT Security in 2017, where Korea and Thailand offered to be bridges between the OSCE and Asia region.

Such interregional efforts (and even bilateral capacity building) could be hampered by incompatible state views on cyberspace governance though, particularly where ASEAN states often hold different perspectives on internal stability, content control and sovereignty. It is unlikely that such views would affect intra-ASEAN cooperation or engagements with countries like China, which continues to promote its notions of cyber sovereignty. Rather, such views could impede capacity building efforts with the EU, for example, or bilaterally with countries like Australia.

Lastly, informal regional mechanisms such as academia, research institutes and Track 1.5/Track 2 diplomatic mechanisms have played a fruitful role to date in forging progress in the region. These informal mechanisms can continue to enable progress where formal international and regional mechanisms such as the GGE or ARF may not be successful or are slow to make progress. Such initiatives can sometimes provide the space for policymakers to increase their understanding of key questions, and it can help to build networks and communities of interest in an informal environment. Findings within academia and informal deliberations can often inform the Track 1 decision-making process further down the line. There is still room for more independent insights and fresh ideas that can be produced through papers, and informal roundtables or workshops with concrete scientific questions about ways to transition to the next phase of international and regional security discussions. However, governments should avoid politicising institutes and analysts in order to avoid the criticism of the previous GGE where experts were described as proxies for negotiations rather than expert consultations. In short, as Richard Haass surmises, in order to forge further progress in this field currently, smaller consultations with critical governments, companies and NGOs are likely to achieve more than large formal gatherings of countries.<sup>23</sup>

---

<sup>23</sup> Richard Haass, *A World in Disarray: American Foreign Policy and the Crisis of the Old Order*, (New York, New York 2016), 247.

## CONCLUSION

This article examines the contribution of Asia Pacific states to a regime for international cyber stability, including promoting common views and implementation of norms of responsible state behaviour in cyberspace, CBMs and capacity building. It argues that it is important to persevere with ongoing endeavours at national and bilateral levels as well as among like-minded groupings, regional bodies, and informal mechanisms. Recognising, however, that this process will take time. This is particularly the case since more state actors and experts are now involved, differences about the very understanding of cybersecurity persist, and high geopolitical tensions are slowing progress.

Even though regional states are fully cognisant of their economic self-interest in cooperating, ongoing geopolitical tensions are detracting from the political willingness needed to make progress. Both globally and regionally, major power rivalry, rising nationalism as well as challenges to the rule of law and international human rights obligations are making it even more difficult to find common ground on state behaviour in cyberspace. Within the Asia region itself, countries vary in terms of cultural and political values, including different conceptual understandings of world order and cybersecurity. These dynamics will continue to impact international cybersecurity issues. Moreover, there is clear dissatisfaction with the current order and rising powers like China also have ambitions in order building, evidenced by states' willingness to use cyber-enabled influence operations and engage in low-level activities without resorting to the use of military force and without fear of significant retaliation.

The article finds that, although it may lead to delays, it is better that more states in the region are becoming, and continue to become, involved in shaping the regional and global agenda. Several countries are continuing their efforts to create an international regime for cyber stability, and countries such as India and China can have a significant impact on the global ecosystem. Nevertheless, there is a developmental and digital divide, and several countries do not even consider cyber-related issues to be a national priority. Such diverse levels of cyber maturity can make international and regional cooperation more difficult. This is exacerbated by a situation whereby infrastructure needs, concerns about interference in internal affairs, geopolitical support and regime changes further impact the ability to make progress or forge the consensus that is often needed in regional institutional mechanisms like ASEAN.

Moreover, global concerns about terrorism and fake news mean that regional states are also introducing initiatives to address their social stability and Internet



control worries. Even where this has led to concerns about excessive (and illegitimate) content control, the ways in which the United States and European states are dealing with these problems as well as nationalism, hate speech, freedom of expression and anti-democratic sentiments are watched closely for examples of hypocrisy. Although many countries share similar social harmony concerns, the inattentiveness of the current United States administration to democracy and human rights is leaving a vacuum in the region. That said, this article finds that Internet sovereignty and information control differences will likely persist.

Numerous bilateral initiatives such as MOUs and like-minded efforts are helping to make progress where regional and international mechanisms like the GGE and ARF are sometimes ineffective by finding common ground, exchanging experience, and implementing norms that can extend to larger groups. Ideally, these efforts should aim to support global initiatives and avoid causing further fragmentation by creating ad-hoc approaches that undermine existing international institutions.

Given the importance of a strong regional security architecture for international and regional stability, continuing with the ARF and OSCE initiatives to build common understanding and implement cyber CBMs regionally is essential. As is the more recent push in ASEAN for better coordination and greater attention to norms, CBMs and capacity building, which should hopefully also contribute to international cyber stability. A lot of awareness raising has been conducted already, however, with fewer examples of concrete implementation of CBMs and meeting agreements. While these regional forums still have a long way to go, there is also room for more cross-regional exchange of good practices. This can help to avoid a situation where regional bodies evolve in very different directions and thus add more uncertainty and instability (although interregional and bilateral initiatives may be hindered by incompatible state and regional views on issues such as internal stability). Lastly, informal diplomatic mechanisms and academic initiatives can continue to help make progress by examining ways to transition to the next phase of regional and international security discussions.

**Caitríona Heint** is Lead Strategist for Asia Pacific at EXEDEC. She was previously responsible for policy under the NTU Cyber Risk Management project, having transferred from the S. Rajaratnam School of International Studies (RSIS) Centre of Excellence for National Security at NTU Singapore where she worked as Research Fellow on international cybersecurity issues from 2012 to 2018.

# Digital Transformation and Industry 4.0 in Southeast Asia

*Raja Mikael Mitra*

## 1. THE SWEEPING DIGITAL TRANSFORMATION

The sweeping change enabled by advanced information and communication technologies (ICTs), manufacturing (Industry 4.0 and the like) or more broadly the fourth industrial revolution and transformation towards a digital and knowledge-based new economy are major drivers of economic as well as cultural, social and political change. And yet there are fundamental gaps in the knowledge and awareness of the implications of these changes and in the understanding of how to respond to them. Those who respond effectively can benefit greatly while those who falter risk losing out. The velocity, scale and scope of change imply that past models and strategies for social, economic and technological development are becoming increasingly obsolete or ineffective. Southeast Asian economies have common as well as unique features in ICT development and more broadly digital society transformation.<sup>1</sup>

Powered by a large and growing Internet user base it is estimated that the Southeast Asia's internet economy will more than triple in the 2018 to 2025 period: measured in gross merchandise value (GMV) covering Online Travel, e-Commerce, Online Media and Ride Hailing. According to this description the region's internet economy reached USD 72 billion in 2018 (2.8 percent of GDP) and is expected to exceed USD 240 billion by 2025 (about 8 of GDP) with e-Commerce GMV alone increasing from USD 23 billion to USD 100 billion. It should, however, be noted that these numbers underestimate the actual size of the "internet economy" as they do not include all sectors of the "digital economy". These estimates cover the six

---

<sup>1</sup> This chapter draws on various publications by the author, including research covering data and other evidences validating findings outlined here. This presentation is part of a larger research project which the author is working on currently.

largest markets in Southeast Asia: Indonesia, Malaysia, Philippines, Singapore, Thailand, and Viet Nam (Google and Temasek 2018).

The next 5-10 years and beyond will see technology and other innovative developments ranging from new materials to nanotechnology, new ways to produce, distribute and store electric power, biotechnology, genomics and medical science advancement and manifold other technological, business processes and other innovative developments are poised to imply major transformations in technology, economic, social and political ecosystems. The latter is illustrated by ICT developments: artificial intelligence (AI), Internet of Things (IoT), 3D printing, data analytics, cloud computing, blockchain (finance and other sector-specific applications), autonomous vehicles (e.g., drones, ships, trains, cars, trucks, kiwi-robots) and other “new” technologies are driving continuous creative disruption in socio-economic ecosystems. Amongst other things this is reflected in worldwide transformational trends in trade, investment and employment. It has major impact not only on manufacturing, construction, mining, agriculture and other natural resource-based sectors but also in terms of service sectors. Furthermore a large number of jobs will be reshaped or disappear in both goods producing and service sectors, the latter especially impacting routine functions relating to clerical jobs, accounting, banking and financial services, transport and logistics services, retail, hotel and restaurants and social services such as education and health care. At the same time, as demand for certain type of manpower declines, it is equally important to note that new technologies and other forms of innovation result in new or boosted demand for certain products and services, some of which result in higher productivity, income and new jobs (World Bank 2018a).

The conceptual framework applied in this chapter centers around 12 pillars that drive and constrain digital transformation, namely: historical legacy, geography and timing, demand and supply settings in local and external markets, human and social capital, financing, technology and innovation, infrastructure, urban and rural development and institutional and stakeholder eco-systems: government, legal and regulatory-frameworks, the private sector, the Diaspora and the leadership context (Mitra 2012 and 2019a).

## **2. DIGITAL TRANSFORMATION IN SOUTHEAST ASIA**

### **2.1 Asian diversity and catch up trajectories**

The degree of maturity and phases of digital development differs significantly within and between countries. Common to all societies in Asia and elsewhere is,

however, the increasing importance of digital economy transformation, a development which typically is spearheaded by larger cities with the most effective interfaces with international innovation, finance and access to human talent.

Most of the East Asian economies (that is, costal mainland China, Hong Kong SAR, Taipei, China, the Republic of Korea and Japan) are well ahead of the South and Southeast Asian economies (with the exception of Singapore and a few major urban ICT industry centres in other countries) in digital economy developments. This is reflected in the fact that higher GDP per capita levels is also associated with greater use of ICTs in the local economy. Economies which are particularly lagging behind include Cambodia, Laos, and Myanmar as well as backward areas in other countries. It should, however, be noted that all countries (including lagging ones) have launched multiple government vision and planning initiatives relating to ICT development and more recently also digital economy and Industry 4.0 inspired and other broad transformational initiatives. Moreover, it should be noted that ICT industry and application development in ASEAN to a large extent has been driven by foreign and local private companies, the latter including ICT and ICT-enabled micro, small and medium-sized enterprises (MSMEs) as well as startups which have seen a surge in recent years.

Over the past decades ASEAN and other Asian economies have experienced a major surge in the diffusion and use of a wide range of ICTs but the adoption of new technologies has been uneven within and between countries. While the digital divide has been narrowing in many countries if measured in terms of number of TVs, PCs, mobile phones and use of basic ICT services, most countries are significantly behind high-income economies in the application of new sophisticated technologies such as high-end AI, IoT and big data analytics.

Also, it should be noted that internal and cross border migration have played a major role in the development of ICT and other sectors in Asia, prime examples of this being large-scale migration within China and India; and the fact that the Chinese, Indians and other Asians play prominent roles in the ICT-related developments in Singapore and other ASEAN economies.

The international dimension of many new technology developments is further illustrated by close linkages between several Asian economies and the United States. Asia is not only a major market for selling ICT products and services but is also a prominent centre for international sourcing of ICT hardware (especially East and Southeast Asian countries) and since the 1990s also IT and Business Process Management (BPM) services (India being a prime example in IT software and services and BPM and the Philippines in terms of BPM). Much of the ICT industry in Silicon Valley is staffed (and more recently also owned and managed) by

diaspora originating from China, India, the Republic of Korea, the Philippines and other parts of Asia. While this has implied so-called brain drain it has also resulted in brain circulation and other benefits for Asian countries. This and other facts have contributed to inspire Asian nations to develop their own “Silicon Valley” type of industry clustering (Saxenian 2005).

**Table 1. ICT Development Index (IDI): Global and Asia region, 2017**

...Economy	Asia Region Ranking 2017	Global Ranking 2017	IDI Value 2017
<b>High-ranking</b>			
Korea (Rep.)	1	2	8.85
Hong Kong, China	2	6	8.61
Japan	3	10	8.43
New Zealand	4	13	8.33
Australia	5	14	8.24
Singapore	6	18	8.05
Macao, China	7	26	7.80
Brunei Darussalam	8	53	6.75
Malaysia	9	63	6.38
<b>Middle-ranking</b>			
Thailand	10	78	5.67
China	11	80	5.60
Mongolia	14	91	4.96
Philippines	15	101	4.67
Viet Nam	17	108	4.43
Indonesia	19	111	4.33
Sri Lanka	20	117	3.91
<b>Low-ranking</b>			
Bhutan	21	121	3.69
Timor-Leste	22	122	3.57
Cambodia	24	128	3.28
India	25	134	3.03
Myanmar	26	135	3.00
Lao PDR	27	139	2.91
Nepal	28	140	2.88
Bangladesh	30	147	2.53
Pakistan	31	148	2.42
Afghanistan	34	159	1.95

Note: The IDI comprises of three sub-indices, namely, the access sub-index, the use sub-index and the skills sub-index.

Source: ITU 2017. *Measuring the Information Society*. Geneva, ITU.

## 2.2 ASEAN regional developments

Among the members of ASEAN, Indonesia, Malaysia, the Philippines, Thailand and Viet Nam are well ahead of South Asia in most economic development indicators but lag behind most of East Asia in terms of socio-economic indicators for per capita income; education and health; ICT spending per capita; adoption of ICT and the development of the domestic market for services; and international rankings in competitiveness, ease of doing business, e-readiness and so on. Moreover, the region's colonial legacy differs from that of East Asia and is only partly in line with that of South Asia. Malaysia, Myanmar, and Singapore were under British colonial rule and hence are familiar with British culture and legal and business practices. The Philippines was a Spanish colony that came under American rule; Indonesia was a Dutch colony; Cambodia, Laos, and Viet Nam were French colonies; and Thailand was never a colony. These facts have had a significant impact on their legal and education systems and subsequently the scope for developing IT-BPM and other export industries.

Growth opportunities are outlined in two recent reports: According to a report by Bain & Company in 2018 the digital economy<sup>2</sup> currently accounts for 7 percent of GDP (around USD 50 billion) in ASEAN compared to 16 percent in China and 35 percent for the US. Moreover, the report estimates that capitalising on new digital economy growth opportunities could create an additional USD 0.8-1.1 trillion revenue in 2025, that is, close to one-fifth of ASEAN's projected GDP of USD 5.25 trillion in the year 2025. The increased digital economy potential is calculated by considering three factors, namely: i) productivity improvements in offline sectors enabled by digital adoption, such as productivity improvements in the manufacturing sector from adoption of Industry 4.0; ii) expansion of digital markets enabled by digital integration, such as access to new markets through e-commerce or financial inclusion through digital financial services; and iii) growth of enabling sectors that lay the foundation for digital integration, such as growth in ICT or logistics sectors that will support digital integration (Bain & Company 2017 and 2018).

According to a McKinsey report released in 2018, Industry 4.0 is expected to drive productivity increases comparable to those generated by the introduction of the steam engine in the first industrial revolution. Globally, it is expected to deliver

---

<sup>2</sup> *Digital Economy*: A collective term that includes digital infrastructure sub-sectors (such as telecommunications, hardware and software), Internet and platform sub-sectors (such as e-commerce and sharing platforms), and the proportion of traditionally offline sectors and sub-sectors enhanced by digitalisation such as manufacturing adoption of Industry 4.0 (Bain & Company 2018).

between USD 1.2 trillion and USD 3.7 trillion in gains by 2025. Of this, ASEAN, whose member economies have significant manufacturing components, has the potential to capture productivity gains worth USD 216 billion to USD 627 billion by 2025 (McKinsey 2018a).

The increased attention being given to digital economy and Industry 4.0-related developments in ASEAN is illustrated by Singapore's Smart Nation and Committee for the Future Economy initiatives, Malaysia's launch of the world's first digital free trade zone (partnering with Alibaba) and the unveiling of a vision for Industry 4.0 transformation, Indonesia's "2020 Go Digital Vision", the "Thailand 4.0" initiative, the Viet Nam government's Industry 4.0 initiatives and numerous other digital/ICT development initiatives in the region.

While progressing it should be recognised that achieving rapid and sustainable economic transformation is a complex task and that is so especially in countries that are weak in terms of infrastructure, human capital and institutions, the later including "soft states" such as Cambodia, Laos and Myanmar. Furthermore, it should be noted that most politicians tend to focus on short-term objectives while they have limited incentive to give high priority to implementing long-term national economic and technological transformation development.

At the regional level, digital developments manifest in the blueprint for the ASEAN Economic Community (AEC) 2025 and in more detail in the ASEAN ICT Master Plan 2020 as well as the Master Plan on ASEAN Connectivity 2025 and other reports released by the ASEAN Secretariat in Jakarta. Developments in diffusion of ICT technologies and expanded use of broadband connectivity are fostering rapid expansion of logistics, e-commerce, banking, finance and payment systems and other ICT-related developments, and are poised to be major factors driving digital economy transformation within and between ASEAN countries (Mitra 2019b).

While progressing, the Southeast Asian region is characterised by weakness in legal and other aspects of harmonisation needed to boost regional integration in ICT and other areas. Also, it should be noted that multinational corporations (MNCs) and local business interests are key forces in driving or constraining national and regional developments. Effective regional integration implies a strong need for efforts in designing and implementing specific schemes relating to the legal and regulatory system, trade and foreign investment, connectivity and logistics, migration, education and research and specific applications such as payment systems and e-commerce (Severino 2006). Also, it is important to continuously update national and regional plans relating to digital and Industry 4.0 related transformation.

Much of IT and BPM industry development in several ASEAN economies have for some time been directed towards exports (and imports). This reflects the scope

for major growth of exports to high income economies coupled with rapid expansion of foreign investment from these countries. The local markets in ASEAN have also expanded but ICT spending for the domestic market is small on a per capita basis compared to higher income countries.

The Philippines and even more so Malaysia, Thailand and Viet Nam, have made major strides in developing their ICT hardware export industry while the Philippines has emerged as a major centre for export of BPM services as well. Moreover, most ASEAN members have made significant progress in the development of ICT start-ups and national plans for ICT-related development. Inspired by the Republic of Korea, Singapore and other countries, Malaysia, Thailand and Viet Nam have made major progress in terms of broadband connectivity while the Philippines, Laos PDR, Cambodia, Indonesia and Myanmar lag behind other ASEAN countries.

Finally, it should be noted that China and the Chinese diaspora have for centuries had major cultural and economic influence in the region and that fact has re-emerged as increasingly important in recent times. China has become a principal trade partner for ASEAN and many other economies. Indonesia, Malaysia, Thailand and Viet Nam and other countries in the region have attracted more direct investment from China but also from North American, European and Japanese investors (not only in electronics and automobiles but also other sectors); one reason for the latter being interests in diversifying investment in order to avoid singular reliance on China as a production centre and market. As of today, Chinese large enterprises such as Alibaba, Huawei, Lenovo and Tencent are principal competitors to Japanese, South Korean, North American and European firms in spearheading the ICT industry and thereby related digital transformation especially in East and Southeast Asia. Also, it should be noted that Chinese firms have emerged as major investors in the region, e.g., Huawei in ICT infrastructure; Alibaba in e-commerce and ICT local startups. The potential for further developing the scale and scope of China's relations with ASEAN and other countries is clearly manifest in the Chinese government's Belt and Road Initiative (BRI) and other regional cooperation and integration initiatives which also have implications on ICT development, including ICT infrastructure and the development of industry centres.

## 2.3 Country experiences

■ **Singapore.** This highly internationalised city economy has outperformed other ASEAN members in ICT as well as other aspects of economic development. It has given high priority to ICT development since the 1980s with the government acting as a catalyst enabling private sector, government and civil society technology up



take. It has also focused on developing partnerships between government, private industry (both foreign and local), and academia. Early on, the government placed strong emphasis on investing in advanced telecommunication infrastructure and in ICT education, training and research. An examination of all 12 pillars driving digital and more broadly knowledge economy transformation shows that Singapore has been and continues to be a front-runner in responding to new technology, innovation and market developments. Singapore has emerged as a world-class centre in ICT development, logistics, finance, management consulting, education, research, and other knowledge economy services.

Recent government initiatives include the Committee on the Future Economy (CFE), the SkillsFuture and Smart Nation and other visionary initiatives relating to innovation, skill and infrastructure requirements for continued socio-economic transformation. The CFE's vision covers seven mutually-reinforcing strategies:

- Deepen and diversify international connections
- Acquire and utilise deep skills
- Strengthen enterprise capabilities to innovate and scale up
- Build strong digital capabilities
- Develop a vibrant and connected city of opportunity
- Develop and implement Industry Transformation Maps (ITMs)
- Partner each other to enable innovation and growth (Government of Singapore 2017).

Furthermore, the government launched a Services and Digital Economy Technology Roadmap (SDE TRM) in November 2018. This initiative was envisaged to be an important part of Singapore's "Digital Economy Framework for Action". It provides a scan of the digital technology landscape in the next 3 to 5 years, identifying the impact of key shifts and technology trends. "Services 4.0" is identified as a key engine of growth for Singapore's digital economy as the services industry accounts for 72 percent of the nation's GDP. "The SDE-TRM aims at enabling business across sectors to harness technology and innovate, equipping their workers with new skills and capturing opportunities in the digital marketplace to deliver customer-centric experiences." (IMDA 2019).

This and other reforms launched by the Singapore government and its corporate partners are envisaged to have major direct and indirect implications not only for the transformation of Singapore but also for other countries and the international business community in particular. Also, Singapore has been spearheading

various regional initiatives, including the ASEAN Smart Cities Network, the development of industrial parks and promoting education. Nonetheless, the role of Singapore in the region does not merely stem from official government schemes but from the fact that it is a forerunner in ICT development and also a major hub for major corporations, financial, consulting, education and research developments in the region. Moreover, the overall socio-economic ecosystem has especially geared to respond to “new” innovative challenges such as transformations of service sectors (fintech, healthcare, higher education and research, communication and transportation services, etc.) and smart industry/Industry 4.0 developments (Tan Teck Boon et al. 2017).

From the time Singapore became an independent nation (1965) the Singapore government has consistently been committed to learning from its own and others’ experiences in designing, and also to ensure effective implementation of policies and specific technology, infrastructure and other development schemes. The government continues to design and implement new policies to tackle a wide range of future socio-economic challenges such as the need to re-orient and upgrade the legal and regulatory, infrastructure, education, training, entrepreneurial and innovation ecosystems, the latter including digital technologies, Industry 4.0, biotechnology and other areas.

In short, Singapore has outperformed most countries in ICT development. It has done well in anticipating the importance of ICT development right from the late 1970s and it has been good at mobilising government and other resources aimed at supporting the growth of the sector. There is an on-going debate within the industry regarding whether the outcomes have been commensurate with the inputs deployed by the government in the ICT sector and the impact of some government schemes versus other factors such as generally conducive business environment and strong private sector demand pull. The country has attracted a large number of multinational corporations, consulting and other firms which have played a key role in developing ICT and other sectors. As in other parts of the region foreign firms dominate the ICT sector barring a few examples such as SingTel, ICT empowered banks coupled with a growing SME and startup sector. During the 2014-2018 period it has consistently been number one or two in the world in terms of the World Economy Forums Networked Readiness Index (WEF 2018).

**Box 1 - Singapore: Smart Nation Visionary Initiative**

The Smart Nation initiative envisions a Smart Nation that is a leading economy powered by digital innovation, and a world-class city with a Government that gives our citizens the best home possible and responds to their different and changing needs. Singapore's plans to drive transformation across the economy are detailed in the Digital Economy Framework for Action, the Digital Government Blueprint and the Digital Readiness Blueprint. The Digital Economy Framework for Action and the Digital Readiness Blueprint has been released by the Ministry of Communications and Information (MCI). These three plans are key pillars which work together to support Singapore's Smart Nation goals, namely:

I. Strategic National Projects: To drive pervasive adoption of digital and smart technologies throughout key Strategic National Projects:

- National Digital Identity – for citizens and businesses to transact digitally in a convenient and secure manner;
- e-Payments – to allow everyone to make simple, swift, seamless, and safe payments;
- Smart Nation Sensor Platform – deployment of sensors and other IoT devices that will make our city more liveable and secure;
- Smart Urban Mobility – leveraging data and digital technologies, including AI and autonomous vehicles, to enhance public transport;
- Moments of Life – bundling government services, across different agencies, to the citizen at different moments of his life.

II. Enabling a Culture of Innovation & Experimentation: The government will put in place appropriate policies and legislations to facilitate innovations by the public and the private sector, and encourage adoption of new ideas.

III. Computational Capabilities and Digital Inclusion. Smart Nation efforts are underscored by re-skilling and promoting the learning of coding and computational thinking skills, to ensure that all segments of the population benefit regardless of age or digital literacy. Resources are also to be put in place to assist larger as well as smaller enterprises as they seek opportunities in the digital economy.

*Source:* Abstracted from Government of Singapore 2018a. <https://www.smartnation.sg/about/Smart-Nation#sthash.LsvEf1oW.dpuf>.

■ **Malaysia.** This multi-cultural and natural resource rich country has made major strides in developing its ICT industry and is ahead of most ASEAN countries (except for Singapore) in the diffusion of ICT in the local economy. Malaysia developed an electronics industry early on based on multinational corporations' offshoring assembly component manufacturing to serve regional and global markets.

Much of the IT and BPM service industry has been concentrated in Kuala Lumpur and the Klang Valley and Penang areas. The government has made major efforts to attract investment into Cyberjaya, located between the Kuala Lumpur city centre and the international airport, and efforts have also been made to develop the industry in other parts of the country. One example is the Iskandar Malaysia project, a major high-technology industry township close to the Singapore border, with the potential to attract investors and professionals who would have otherwise operated out of Singapore.

Malaysia differs from the Philippines (and many other Southeast Asian countries) in the scale and scope of government interventions to promote and invest large sums to promulgate the use of e-government and other applications in the local economy as well as to foster electronics and ICT hardware and subsequently also ICT service industries. The latter applies also to investment in basic and higher levels of vocational training education. Furthermore, it should be noted that efforts to accelerate adoption of ICTs among the smaller scale and mid-sized homegrown businesses (especially manufacturing) have been sluggish in Malaysia, as is also the case in many other countries in the region. Greater efforts, or different technology adoption business models, need to be explored to catalyse broader-based diffusion of ICT and other technologies in various sectors of the economy.

The Malaysian experience indicates that both the government and the private sector have principal roles in fostering ICT development but the efficacy of government intervention is key. This is illustrated not only in terms of attracting foreign investment but also in establishing industrial parks but the record has been mixed in terms of the ability to solve problems resulting from fragmentation and the poor implementation of government initiatives, some of which have been characterised by ineffective subsidy regimes and corrupt practices. Malaysia's varied results in ICT development suggest that focusing exclusively on government and public-private partnerships for investing in infrastructure and providing generous tax and other incentives may not be enough to enable major IT-BPM industry development, especially if the investments and policies are ineffective. The importance of early and sound investments in human resources and ensuring that such efforts are carefully monitored and managed is paramount. Also, it should be noted that a

large number of skilled and educated Malaysians have opted to leave their country with Singapore being the major beneficiary.

Also, it is imperative to compete for foreign investment and to establish more effective programmes to strengthen local entrepreneurship and innovation. Nevertheless, Malaysia has been an example of bold leadership, as illustrated by its Vision 2020 of a technologically advanced society and a technologically enabled government. The government's 8th, 9th, and 10th plans (2010-2015) along with the Knowledge-Based Economy Master Plan, the Digital Transformation Program and several other government initiatives aim to transform the economy through innovation, knowledgeable and skilled human capital, and the widespread use of technology. By 2020, the Digital Transformation Program is expected to increase the contribution of the digital economy from the current 12.5 percent to 17 percent of gross national income (MOSTI and PIKOM 2012). Furthermore, Malaysia's National Policy on Industry 4.0 or Industry4WRD was launched in 2018. Industry4WRD focuses mainly on digitally transforming the manufacturing sector and its related services to embrace Industry 4.0.

■ **The Philippines.** This island economy has until recently trailed behind most other major Asia economies in GDP, foreign trade and investment growth. But it continues to lag behind not only Singapore and Malaysia but also Indonesia, Thailand and Viet Nam in per capita income, industrial, infrastructure and social development indicators.

The country has developed a major BPM export industry and seen a rapid expansion of social media and some other ICT applications, especially from the 2000s onwards. Manila has emerged as the world's largest centre for offshoring of call centre operations and has also progressed in developing increasingly wide ranges of non-voice BPM services for international markets, the latter including knowledge process management. In addition, it should be noted that the Philippines has a sizeable electronics industry focusing on assembly and more recently also higher value added work. Moreover, in recent years the country has experienced a rapid expansion in the number of ICT-enabled MSMEs, startups and micro-businesses.

The Philippine experience with BPM since the 2000s demonstrates the scope for rapid growth in outsourcing services to developing countries. Most of the growth has so far been at the lower end of service provision such as basic call centres and low-end, BPM non-voice services plus some knowledge process outsourcing and legal service outsourcing, IT services and software, and engineering services. The country has, however, considerable potential to expand the scale and scope of service delivery at the lower as well as the higher end of the value chain,

although recent years' advancement in technology (automation etc.) has begun to have significant impact on the growth and structure of the IT-BPM services as well as prospects for developing ICT hardware and other industries.

The success in developing the BPM export sector can largely be attributed to access to a large pool of service-minded people with English language and other skills coupled with the limited scope for full employment in other sectors. The development of industrial parks in Metro Manila and in other parts of the country have helped due to costing and productivity advantages and increased interest among multinational corporations in expanding the scale and scope of their offshoring and outsourcing operations to a wider range of countries. Much of the ICT-related industries are likely to continue to be located in the Greater Metro Manila area or in Cebu, but significant growth is also expected in the so-called "next wave" cities.

The government has generally been favourable to ICT development. This is reflected in planning documents and the significant expansion of special economic zones and industry parks. Nevertheless, financially and institutionally the scale and scope of the effort to support the ICT industry and more broadly speaking the digital economy transformation, and more recently Industry 4.0, has been moderate if compared to Malaysia, Thailand, Viet Nam and several other Asian countries.

The Philippines lags behind many other countries in improving its education system, investments in science and technology as well as diffusion of quality broadband services. Moreover, it faces general challenges in developing hard and soft infrastructure, the latter including weaknesses in the legal and regulatory system, governance and in educating and retaining technical and managerial talent. More than 10 million Filipinos have opted to work abroad. This includes a large number of unskilled, skilled and well-educated Filipinos working and living in the United States (including in Silicon Valley), Canada, Europe, the Middle East, Singapore, Hong Kong SAR, Thailand and elsewhere.

■ **Thailand.** The country's economic progress since the 1960s is clearly manifest in major investments in infrastructure, education and training coupled with rapid development of tourism and the manufacturing industry, the latter illustrated by successful development of the eastern seaboard (the "Eastern Economic Corridor"). The country has developed a sizable manufacturing industry empowered by foreign investment and access to a large pool of skilled labor and qualified engineers. While Thailand has become a major centre for offshoring electronics, automobiles and other manufacturing, it has only achieved limited success in developing a major IT-BPM service industry, leaving aside recent years' boom in terms of e-commerce, fin tech and ICT enabled startups. Several factors impede the development of a

competitive ICT services export industry, notably limited supply of skilled and experienced technical, managerial, and entrepreneurial human resources with specialised skills in software and other ICT product development and services.

The government is increasingly committed to visions for a digital-economy related transformation. This is manifest in Thailand's 12th Social and Economic Development Plan (2017-2021) and the ICT2020, the latter aiming at developing the country's ICT industry so that it can be a leader in the Southeast Asia region (Wongwuttivat et al. 2018). The government's Third ICT Master Plan (2014 to 2018) focuses on four key strategies, namely: building optimal infrastructure, nurturing vibrant businesses, be a smart government and capitalising on ICT human resources. Also, ageing people are among the prioritised community to pay attention to; thus there is focus in the form of e-Ageing development (Research Gate 2018).

Moreover, a Digital Thailand Plan outlines strategies to expand the use of digital technologies in all socio-economic activities over a 20-year period. Other recent initiatives in support of this goal include the five-year Digital Government Development Plan, which is an operational plan to foster digital economy transformation. From 2016 onward the Thai government has promoted a vision for smart or Industry 4.0 related development in collaboration with Chinese, German and other entities. Under "Thailand 4.0" there is perceived to be limited room for labour intensive manufacturing processes in the future. The main areas of focus are, as per Thailand 4.0, in the food, agriculture, biotechnology, healthcare, biomedicine, smart devices, robotics, automation, digital industry, Internet of Things, better technology, culture and creative industries, as well as a high-value services sector (Jones et al. 2017).

While progressing in adopting modern technologies, the country faces major issues such as limitations in English language, technical and other capabilities, the need to respond to disruptive technology (automation in electronics, automobiles and other), and weaknesses in the investment climate and challenges in implementing stated policy objectives. As in the case of most nations Thailand faces major challenges in focusing on adoption and adaption of existing technologies and progressing towards greater emphasis on creativity and innovation.

■ **Viet Nam.** As in the case of Thailand, Viet Nam has made major progress in developing infrastructure and has become a major centre for electronics and other manufacturing.

Viet Nam is the world's third largest producer of mobile handsets (2017) after China and India (ICA 2018). While the country has made major progress in IT-related development, including penetration of computers, smart phones and access to

broadband and entrepreneurial developments (including a boom in terms of number of startups), rapid ICT-related development is constrained due to shortages of skilled and experienced technical, managerial, and entrepreneurial human resources and persons with strong English-language skills and multinational corporations' concerns about intellectual property rights and e-security. In addition, concerns about the overall quality of the regulatory and business environment have hampered development (WEF 2013).

The government has nonetheless declared plans to develop a sizeable ICT industry along with major investments in ICT infrastructure, training and education, and e-government. Viet Nam is expected to have a complete, stable 4G network in 2018 and aims to introduce 5G networks by 2020 (Oxford Business Group 2017). By 2020, the country's goal is to be well above the average ASEAN member (leaving aside the more advanced Singapore) in terms of ranking as an information society. It aims to change its socioeconomic structure so that it will have an advanced, networked, knowledge-based economy that will contribute significantly to successful industrialisation and modernisation. Achieving continuous growth and upgrading of the manufacturing industry does, however, entail major challenges including responding to the expanding scale and scope of additive technology (3D printing) and automation resulting from the fourth industrial revolution development currently sweeping advanced industrial economies. In 2017 Prime Minister Nguyen Xuan Phuc issued a directive to strengthen the country's ability to access the fourth industrial revolution (Cameron et al. 2018).

Though advancing rapidly in ICT industry and application developments the country faces major economic catch-up issues such as the need to upgrade technical and other capabilities and more broadly to respond to disruptive technology and challenges in implementing stated policy objectives.

■ **Indonesia.** Unlike several East and Southeast Asian countries, Indonesia has not been able to establish a large internationally competitive ICT hardware manufacturing (leaving aside some low end assembly), BPM and software service industry. Also economic growth has slowed down in recent years reflecting demographic development and feeble productivity performance (Felipe 2019). Nevertheless, there is a need to serve the sizeable local market for both ICT services and hardware. Major advancements in broadband connectivity in all parts of the country are critical for integrating and developing the domestic economy as well as its international interface.

The country's major scope of digital economy-related development is highlighted in the McKinsey report "Unlocking Indonesia's digital opportunity" published in



2016. According to this report, if Indonesia embraces digitisation, it can realise an estimated USD 150 billion in growth – 10 percent of GDP – by 2025. “Digital technologies offer ways to boost productivity across sectors and expand participation in the economy to all segments of the population. But accelerating Indonesia’s digital progress will require businesses to step up to the challenge and fundamentally transform themselves. To win in a digital age, Indonesian businesses should pursue five strategic imperatives that will spearhead growth and efficiency: i) define customer-centric experiences to differentiate on design and agility; ii) develop omnichannel engagement to link the online and offline worlds; iii) leverage big data to drive real-time decisions across the value chain; iv) double down on cyber security to protect information capital in a connected world and v) build digital capabilities to develop the organisation of the digital age.” (McKinsey 2016b) Further, according to the report “The digital archipelago: How online commerce is driving Indonesia’s economic development” released by McKinsey in 2018, the size of Indonesia’s online commerce market (a sector comprising about USD 5 billion of formal e-tailing and more than USD 3 billion of informal commerce) is estimated to be about 30 million online shoppers in 2017 in a total population of about 260 million. Moreover the report points to the socio-economic impact of online commerce in Indonesia, today and five years from now, through an evaluation of financial benefits, job creation, buyer benefits, and social equality. It forecasts that online commerce sales will grow substantially, reaching up to USD 65 billion by 2022, out of which 30 percent will be consumption that otherwise would not have occurred. The report claims that in addition to increasing revenue, online commerce can unlock broader positive social impacts (McKinsey 2018b).

In 2015 the Indonesian government launched the “2020 Go Digital Vision” campaign to boost the country’s digital economy. Among key targets are helping one million farmers and fishermen to go digital, and creating 1,000 local tech startups valued at a total of USD 10 billion by 2020. The campaign vision is that the country will become the largest digital economy in Southeast Asia by 2020, a vision which is not astounding given the size of its population and economy (McKinsey 2016b). Furthermore, the government has launched a multi-sector Industry 4.0 related development initiative.

While lagging behind Malaysia, Singapore, Thailand and Viet Nam in composite ICT development indexes (ITU 2017) and Internet readiness indexes (EIU 2018) the country has a fast-growing market for related ICT services. Internet traffic, revenue from cloud services, and connected devices (Internet of Things) are growing fast. The scale and scope of local ICT-empowered entrepreneurs is developing rapidly. This is illustrated by e-commerce major PT Tokopedia and unicorn firms such as

Go-Jek, Traveloka and Bukalapak (all founded by indigenous entrepreneurs focused on the domestic; subsequently also having major foreign shareholders and have begun to invest in other Southeast Asian countries as well) which have created jobs and often also provide better wages and benefits, such as health insurance and access to bank accounts, compared to more traditional jobs (e27 2018). However, while disruptive technologies are perceived as offering benefits, it is also said to pose risks such as loss of job opportunities in certain sectors and increase in inequality. These facts are reflected in the national e-commerce roadmap released in 2016 aimed at supporting the development of the local e-commerce ecosystem, to fund e-commerce startups, to protect consumers, and to double down on cyber security. The e-commerce roadmap has eight major components: funding, taxation, consumer protection, education and human resources, communication infrastructure, logistics, cyber security and the implementing organisation. Also, the government has also started targeted measures and programmes to promote fintech and other technologies as part of its strategy to reduce poverty and inequality in urban as well as rural and remote areas.

Much ICT and other modern economy development is concentrated to few areas, that is, Java in particular, while other areas lag behind. With a large and heterogeneous population spread over a vast archipelago Indonesia faces major challenges in tackling income, education and other socio-economic disparities and developing hard and soft infrastructure, entrepreneurship and governance.

■ **Cambodia, Laos and Myanmar.** Other countries in the region, that is Cambodia, Lao PDR and Myanmar, have for the most part lagged behind other ASEAN members in ICT diffusion and industry development. Especially from the 2000s onward all of these countries have, nevertheless, experienced rapid use of ICT with mobile telephones being the prime example. Given the inadequate infrastructure, the poor education system and other socio-economic weaknesses, it is, however, apparent that these countries (as well as Timor Leste and Papua New Guinea) face major challenges in catching up in ICT-related development, which in turn implies major handicaps in responding to challenges in digital economic transformation and more broadly the fourth industrial revolution.

### 3. COMPARATIVE PERSPECTIVE LESSONS

#### Twelve key strategic imperatives

In conclusion, digital transformation experiences from Southeast Asia illuminates varied sets of feasible development strategies and best practices. Added together,

the lessons from country experiences point to the need for multidimensional understanding of digital economy and Industry 4.0 developments. Moreover, the record highlights the fact that there is little room for complacency in responding to numerous opportunities and challenges relating to technology and other forms of innovation.

The digital transformation strategic lessons from ASEAN (and other countries) need to cover all 12 pillars of digital and Industry 4.0 transformation as noted earlier (Mitra 2019a and 2019b).

## **A. Legacy, supply, demand, investment climate, factor markets and agglomeration**

**1. Historical legacy, geography and timing.** The colonial past and different periods in the post-independence era including the political economy, cultural and geopolitical settings, matters significantly in terms of the opportunities and challenges in technology, industry and entrepreneurship development.

**2. Swift response to change in demand and supply.** Timely and effective responses to new demand and competitiveness conditions are essential as illustrated by local IT-BPM industry growth opportunities in a wide range of vertical and horizontal market segments and local and international geographies. The investment climate needs to be perceived as sound and stable by both indigenous and foreign firms. Business models grounded in local and international competition as well as cooperation and partnerships are beneficial.

**3. Human and social capital.** Early, continuous, and quality efforts in education and training must be a core and principal priority to all stakeholders concerned. Educating and training, and attracting and retaining of technical, managerial and entrepreneurial talent is key. It is essential to tackle issues related to mismatch and weak quality in terms of output and demand in education, training and labour market mobility and overall weaknesses in ICT awareness and digital literacy. There is little room for complacency in responding to overall changes in human resource needs and labour markets.

**4. Financing.** Access to local and foreign capital and the existence of established financial institutions is essential. It is essential to tap into multiple effective avenues for financing, including angel investors and venture capital firms with capacity not only to provide finance but also advice and mentoring. While well-established entities typically have better access to funding it is acknowledged that long-term growth hinges on greater emphasis on R&D and financing smaller firms and startups.

**5. Technology and innovation.** Adoption of technology developed in advanced industrial economies has been a fundamental driver of ICT industry and diffusion development. This is reflected in the role of foreign and indigenous firms, the government, the academe, diaspora, consulting firms and various other networks and their interfacing. Also, there has been a notable potential to adapt technology to local market conditions, e.g., software and content. The increasingly short life cycle of technologies and skills competency constitutes a major concern especially in areas where there is major international competition.

**6. Infrastructure.** New and more efficient telecommunication technology and the growth in computer and broadband as well as other infrastructure is a basic need. The government and subsequently also major private and public private partnership investments in infrastructure have been central to the development of industry, especially due to the fact that many areas lack basic physical and soft infrastructure. The track record in terms of ICT and other infrastructure initiatives available has thus been mixed, pointing both to major successes as well as failures. Continuous upgrading of ICT and other local, regional and international infrastructure is vital, e.g., high-quality and reliable electricity, telecommunications, Internet, airports and local transport systems.

**7. Agglomeration, urban and rural development.** Agglomeration or “clustering” of industry in major cities and sustaining development in major cities or industry centres is key. Coherent and consistent efforts are needed to develop industrial parks, economic zones and corridors through partnerships. Also, the international experience points to the fact that development of rural areas not only offers major markets for ICT products and services in the long term but also leads to sources of attracting talent and in some cases locations for the BPM industry. Furthermore, the “death of distance” can empower not only on international and domestic trade but also, sourcing and telecommuting within cities also more broadly peri-urban and rural areas. Past experiences and prospects for further development point to the need for coherent and effective efforts to tackle weaknesses in city planning, infrastructure, the environment and other requirements for the development of competitive and liveable cities and to promote the development of smart villages and cities.

## **B. Institutions and role of key stakeholders**

**8. Government policy and investment.** National and sub-national governments should take on multiple roles in education, e-government, telecom and other infrastructure, urban planning and other public sector development initiatives. In

addition policymakers can play a special role as general facilitators of private sector development by providing a generally sound investment environment including appropriate legal and regulatory frameworks, and fiscal and other incentives. The government continues to have key roles not only in terms of procurement, research and leadership in promoting industry development and diffusion of technology, but also in minimising unwarranted implications of digital transformation. This applies to the fact that the digital revolution is associated with a wide range of disruptions in the overall socio-economic fabric; it creates new manifestations of cultural, economic, political and social development empowerment opportunities as well as risks such as marginalisation, and digital divides or gaps; it results in a complex set of issues that can be a consequence of poor design and ill-managed dependency on technology and weaknesses in the overall public administration and governance ecosystem. More generally, government policies need to be coherent in serving both short- and long-term national and sub-national development goals while being stable and predictable and yet bold and flexible.

**9. Legal and regulatory ecosystems.** The digital and other innovative developments imply multiple challenges in creating or augmenting the legal and regulatory ecosystem so that it can respond to general as well as sector- and issue-specific local as well as international developments. This imposes needs for swift, effective and resilient responses to legal and regulatory and other policy challenges in terms of labour and migration, industrial development and competition, finance services and ecommerce, intellectual property, harmonisation of technical standards, cyber security, data protection including privacy, consumer protection, data ethics, conflict resolution, environmental and technology risk disasters adaptation and other unwarranted implications of ICT development. The digital transformation thus requires that the judiciary system is efficient and effective in enforcing existing and new laws and regulations and warrants a need for trust among key stakeholders.

**10. Multi-faceted large firms, micro, small and medium-sized enterprises and startups; the technology, business services and industry association ecosystems.** Indigenous firms and other institutions as well as foreign firms, consulting firms and other entities typically have key roles in the development of IT-BPM industries. Attracting foreign investment and developing strategic alliances or other forms of international collaboration are vital as is dynamic and multi-faceted entrepreneurship of large firms, MSMEs and ICT industry as well as other startups. A swift response to existing business opportunities is central. In addition, it is central to develop research and other capabilities to move up the value chain and responding to new path-breaking technology and business model development issues, or else

businesses risk stagnating or failing to avail to opportunities to become major internationally competitive firms. Conventional forms of local and foreign investment, strategic alliances and partnerships coupled with the use of new technologies, business models, management skills and connections among local and international value chains, knowledge and other networks are all essential in the new networked economy development.

**11. Diaspora** can have an especially pivotal role as investors and in serving as mentors and inspiring role models.

**12. Leadership and collaboration.** Political, corporate and civil society leadership with a strong commitment to understanding and implementing what is doable in the short term as well as providing an early response to new technology and other societal transformational development challenges is central. Sound government, corporate, academic and civil society leadership and collaboration capabilities to respond to technological, market and other change requirements are key. It is imperative to fully acknowledge country and project track records in terms of quality of leadership and collaboration which has resulted in major successes as well as examples of poor performance.

All of the above illuminates the potential of collaboration and learning from different individual and collective experiences within countries and internationally.

Finally, it points to the need for continuous re-orientation of both corporate strategies and public policies coupled with a strong commitment to sound prioritisation of investments and effective implementation of programmes and projects.

**Raja Mikael Mitra** has served with the World Bank in Washington DC for twenty years. Recent assignments include, among others, work on high-tech industry, human talent and higher education, innovation and entrepreneurship, digital and knowledge economy transformation, infrastructure development, urbanisation and smart cities, in Asia and globally. He graduated from the University of Stockholm and Harvard University.

## References

- Arora, Ashishand and Alfonso Gambardella (eds). 2005. *From Underdogs to Tigers: The Rise and Growth of the Software Industry in Brazil, China, India, Ireland, and Israel*. New York. Oxford University Press.
- Asian Development Bank Institute (ADBI). 2014a. *ASEAN 2030: Towards a Borderless Economic Community*. Tokyo. ADBI.
- . *ASEAN, the PRC, and India: The Great Transformation?* Tokyo, ADBI.
- Asian Development Bank (ADB) and Asian Development Bank Institute (ADBI). 2012. Masahiro Kawai, Rajat Nag and Biswa N. Bhattacharyay (eds). *Infrastructure for Asian Connectivity*. Tokyo and Manila. ADB, ADBI and Edward Elgar.
- Association of Southeast Asian Nations (ASEAN). 2009. *ASEAN Economic Community Blueprint*. Jakarta. ASEAN Secretariat.
- . 2010 and 2017. “Master Plan on ASEAN Connectivity”. Jakarta: ASEAN Secretariat.
- . 2013. “ASEAN Integration Monitoring Report”. Jakarta and Washington DC. A Joint Report by the ASEAN Secretariat and the World Bank ASEAN Integration Monitoring Office. ASEAN and Office of the Chief Economist, East Asia and Pacific Region and the World Bank.
- AT Kearney. 2018. *Industrial Transformation Asia-Pacific Region*. AT Kearney.
- Bain & Company. 2017. *Advancing Towards ASEAN Digital Transformation: Empowering SMEs to Build ASEAN's Digital Future*.
- . 2018. *Digital Acceleration in Southeast Asia: Navigating Tectonic Shifts*.
- Baldwin, Richard. 2016. *The Great Convergence: Information Technology and the New Globalization*. London. Belknap Press of Harvard University Press.
- Beschorner Natasa and James Neumann. 2018. *Benefiting From The Digital Economy Cambodia Policy Note*. Washington DC. World Bank.
- Boon Tan Tech and Wu Shang-Su. 2017. *Public Policy Implications of the Fourth Industrial Revolution for Singapore*. Singapore. RIIS, Nanyang Technical University.
- Boston Consulting Group (BCG). 2018a. The report titled *The Internet's New Billion: Digital Consumers in Brazil, Russia, India, China, and Indonesia*.
- Breznitz, Dan. 2006. *Innovation and the State—Development Strategies for High Technology Industries in a World of Fragmented Production: Israel, Ireland, and Taiwan [Taipei, China]*. Published by Oxford University Press on behalf of the Business History Conference.
- Brynjolfsson, Erik and Andrew McAfee. 2017. “The Business of Artificial Intelligence: What it Can—and Cannot—Do for Your Organization.” *Harvard Business Review*, July 2017.

- Brynjolfsson, Erik and Tom Mitchell. 2017. "What Can Machine Learning Do? Workforce Implications." *Science* 358(6370): 1530-1534.
- Cameron A., Pham T., and Atherton J. 2018. *Vietnam Today—first report of the Vietnam's Future Digital Economy Project*. Brisbane. Australia. Commonwealth Scientific and Industrial Research Organization.
- Carmel, Erran. 2003. "Taxonomy of New Software Exporting Nations". *Electronic Journal on Information Systems in Developing Countries*. 13(2).
- Castells, Manuel. 2000. *The Rise of Network Society*. Oxford: Blackwell.
- E27. 2018. *Southeast Asia Startup Ecosystem Report 2018*. Singapore. file:///C:/Users/lenovo/Desktop/Documents/Act%20Jan%2029%2019/.Read%20all%20asia%20etc%20all/.Asia%20regional%20read/ASEAN%20ICT%20new%20read/e27-Southeast-Asia-Startup-Ecosystem-Report-2018.pdf.
- Felipe Jesus. 2019. *Policies to Support the Development of Indonesia's Manufacturing Sector During 2020-2024*. Manila. Asian Development Bank.
- Google and Temasek 2018. *e-Conomy SEA 2018: Southeast Asia's internet economy hits an inflection point*. Singapore. Google and Temasek.
- Government of Singapore. 2017a. Singapore. <https://www.gov.sg/microsites/future-economy/thecfe-report/7-strategies>.
- . 2018a. <https://www.smartnation.sg/about/Smart-Nation#sthash.LsvEf1oW.dpuf>.
- Hallward-Driemeier, Mary and Gaurav Nayyar. 2018. *Trouble in the Making? The Future of Manufacturing-Led Developments*. Washington DC. The World Bank.
- Hew, D. (ed). 2007. *Brick by Brick: The Building of an ASEAN Economic Community*. Singapore. Institute of Southeast Asian Studies.
- Infocom Media Development Authority (IMDA). 2019. Singapore. <https://www.imda.gov.sg/sgdigital/tech-roadmap> Accessed January 21, 2019.
- International Telecommunication Union (ITU). 2018. *Measuring the Information Society 2018* (and earlier issues). Geneva. ITU.
- Mazzucato, M. 2013. *The Entrepreneurial State: Debunking Public vs Private Sector Myths*. London. Anthem Press.
- McKinsey Global Institute. 2014. "Southeast Asia at the Crossroads: Three Paths to Prosperity". McKinsey Global Institute.
- McKinsey. 2016a. *Indonesia in the Digital Age – an Anthology of Digital Perspective*. McKinsey & Co.
- . 2016b. *Unlocking Indonesia's Digital Opportunity*. McKinsey & Co.



- . 2018a. *Industry 4.0: Reinvigorating ASEAN Manufacturing For the Future*. McKinsey & Co.
- . 2018b. *The Digital Archipelago: How Online Commerce is Driving Indonesia; Economic Development*. McKinsey & Co.
- Mitra, Raja M. 2009. "IT Industry in Transformation: Opportunities and Challenges for India". *Asia Research Centre Working Paper 29*. London: London School of Economics.
- . 2013a. *The Information Technology and Business Process Outsourcing Industry: Diversity and Challenges in Developing Asia*. Chapter 3 in "Developing the Service Sector as an Engine of Growth for Asia". Manila and Washington DC. Asian Development Bank and the Peterson Institute of International Economics.
- . 2018. *Digital Economy and Industry 4.0 Transformation: Opportunities and Challenges for Asia*. Research submitted to State University of Michigan, London School of Economics, Singapore Management University and others.
- . 2019a. *Digital and Knowledge Economy Transformation: Disruptive Opportunities and Challenges for Asia and its Partners* (Forthcoming).
- . 2019b. *Leveraging Digital and Knowledge Economy Transformation: Opportunities and Challenges for India and its Partners* (Forthcoming).
- Organisation for Economic Co-operation and Development (OECD). 2018. *Economic Outlook for Southeast Asia, China and India: Fostering Growth through Digitalisation*. Paris. OECD Development Centre.
- Oxford Business Group. 2017. *The Report: Vietnam 2017*.UK. Oxford Business Group.
- Preen, Mark. 2018. "China's Mega City Clusters: Jing-Jin-Ji, Yangzte River Delta, Pearl River Delta". Hong Kong. China Briefing. Dezan Shira & Associates, Hong Kong.
- Research Gate. 2018. [https://www.researchgate.net/publication/270762593\\_Thailand\\_New\\_ICT\\_Master\\_Plan\\_to\\_Promote\\_ICT\\_Innovations\\_and\\_Services\\_for\\_e-Ageing](https://www.researchgate.net/publication/270762593_Thailand_New_ICT_Master_Plan_to_Promote_ICT_Innovations_and_Services_for_e-Ageing).
- Santoso, S. 2017. *How can ASEAN nations unlock the benefits of the Fourth Industrial Revolution?* Davos. World Economic Forum.
- Saxenian, A. L. 2005. *From Brain Drain to Brain Circulation: Transnational Communities and Regional Upgrading in India and China*. *Studies in Comparative International Development*, June 2005, Volume 40, Issue 2, pp 35-61.
- Schumpeter, Joseph. 1942. *Capitalism, Socialism and Democracy*. New York. Taylor & Francis Group.
- Schwab, Klaus. 2016. *The Fourth Industrial Revolution: what it means, how to respond*. Davos: World Economic Forum.
- . 2018. *Shaping the Fourth Industrial Revolution*. Geneva. World Economic Forum.

- Severino, R. 2006. *Southeast Asia in Search of an ASEAN Community*. Singapore. Institute of Southeast Asian Studies.
- United Nations Conference for Trade and Development (UNCTAD). 2012 and onwards. *Information Economy Report*. <http://unctad.org/en/Pages/Publications>.
- Wongwuttawat Jittima and Adtha Lawana. 2018. *The Digital Thailand Strategy and the ASEAN Community*", *The Electronic Journal of Information Systems in Developing Countries*.
- World Bank. 2016. *Digital Dividends. World Development Report*. Washington DC.
- . 2018a. *World Development Report*. World Bank. Washington DC.
- . 2018b. *Ease of Doing Business Reports*. Washington DC.
- . 2018c. *Information and Communications for Development: Data-Driven Development*. Washington, DC.
- . 2018d. *Malaysia's Digital Economy: A New Driver of Development*. Kuala Lumpur.
- . 2018e. *Preparing ICT Skills for Digital Economy: Indonesia within the ASEAN context*. Jakarta.
- . 2019. *World Development Indicators Online Database*. Washington DC.
- World Economic Forum (WEF). Geneva. 2018a. *The Global Information Technology Report 2018* (and earlier issues).
- . 2018b. *The Global Competitiveness Report 2018* (and earlier issues).
- . 2018c. *Readiness for the Future of Production*.



# Energy Security in the Digital Age and Its Geopolitical Implications for Asia

*Frank Umbach*

The worldwide energy sector stands at the crossroads, coping with unprecedented changes and challenges: increasing deployment of renewable energy resources (RES), rising energy demand, greater energy efficiency, disinvestment in carbon-intensive industries and the US shale oil and gas revolution (together with the rapidly expanding worldwide liquefied natural gas (LNG) trade) have far-reaching impacts on the global oil and gas markets. Furthermore, digitalisation, new forms of mobility, and new consumption patterns, providers and platforms are changing established industries. The “energy transition” affects in particular the global electricity sector, which is being transformed by the reinforcing strategic trends of the “3 Ds”: decarbonisation, digitalisation and decentralisation. Furthermore, electrification and digitalisation of the transport and heating sectors as well as the forthcoming “industry 4.0”-revolution, based on robotics and Artificial Intelligence (AI) systems, might result in a much higher electricity demand than currently projected. This will increase the role of electricity in final energy consumption significantly. These megatrends will affect not only the industries but also the daily life of citizens and public order as it will become ever more dependent on the stable functioning of critical (energy) infrastructures.

Increasing internet interconnectivity and a vast amount of sensitive data, as well as asymmetric conflict patterns in international relations, have dramatically amplified the risks and vulnerability of national and global energy infrastructures in

---

\* This article is a short version of Frank Umbach’s study “Energy Security in a Digitalised World and its Geostrategic Implications”, published by KAS Regional Project Energy Security and Climate Change Asia-Pacific (RECAP)/Hong Kong. To access the study, please visit <https://www.kas.de/web/recap/single-title/-/content/energy-security-in-a-digitalised-world-and-its-geostrategic-implications>.

terms of sophisticated cyberattacks on services.<sup>1</sup> Those threats can even multiply with the next wave of digitalisation in the energy sector (especially electricity generation and distribution), the further global expansion of RES and the electrification of the transport (e.g., rapid expansion of electric vehicles) and heating sectors. It is not least due to this development of unprecedented changes, opportunities and risks that the International Energy Agency (IEA) stated in 2017,

Every unit of the IEA – from efficiency to investment, from electricity to transportation, from renewables to modelling, from sustainability to statistics – is examining the implications of digitalisation on the energy sector. [...] The interest in this topic is strong, but the world’s current understanding of the scale and scope of its potential remains limited, particularly when it comes to analytically-rigorous assessments.<sup>2</sup>

New (disruptive) technologies for digitalisation, AI, clouds, robotics, and industry 4.0 are even more welcomed in Asia as they promise to improve the daily lives of citizens and offer new economic perspectives for enhancing living standards and productivity.<sup>3</sup> Together with a growing population in ASEAN and South Asia, these technologies transform Asia into the most dynamic region in the world. Asian states and governments demonstrate in their supported programmes (e.g., Singapore’s “Smart Nation Initiative” or Japan’s “Society 5.0”) their political will to use and adopt those new technologies which will decisively shape the worldwide digital transformation. Up to now, those programmes are developed for their entire economy and society, but do not appear to be very detailed with regard to energy transformation and future energy security.

Against the background of these dramatic forthcoming changes, at least four geopolitical implications of the digitalisation of the energy sector – alongside the other already impacting strategic energy developments – can be identified on the global and regional levels:

<sup>1</sup> See F. Umbach, “Critical Energy Infrastructure and Risk of Cyber Attack”, in KAS-International Reports, September 2012, pp. 35-66; idem, “Cyber Security – Dossier”, Geopolitical Information Service (GIS - [www.geopolitical-info.com](http://www.geopolitical-info.com)), August 2013; idem, “The Fog of Cybersecurity”, Geopolitical Intelligence Service (GIS), 10 July 2017.

<sup>2</sup> See IEA, <https://www.iea.org/newsroom/news/2017/april/iea-examines-critical-interplay-between-digital-and-energy-systems.html>, accessed 18 January 2018.

<sup>3</sup> To AI see Richard Waters, “Why We Are in Dangers of Overestimating AI”, FT, 5 February 2018; “Limiting the Downsides of Artificial Intelligence”, FT, 22 February 2018; Rana Foroohar, “How We Can Protect Workers from AI? FT Readers Respond”, FT, 21 February 2018; “The Global Policy Response to AI”, FTI Consulting Inc., February 2018.

(1) A further rising electricity demand, which has already been forecasted to grow much faster than the overall primary energy demand on national, regional and global levels. While the digitalisation might also promise new energy efficiency gains and energy conservation, many newly introduced and identified new technologies have proved to be very energy intensive and might lead to even higher electricity demand.

(2) Electricity supply, alongside expanding volatile renewables and advancements of battery storage technologies, becomes ever more important for future energy supply security. Advancing technologies for battery storage may cause one of the most disruptive changes and is a major game changer in the power and renewable industries.

(3) With smart meters and smart grids, the electrification of the transport and heating sectors, the internet of things (and applications) and critical (energy) infrastructures (CEIs), the energy sector becomes more vulnerable towards sophisticated cyber-attacks and blackmail attempts to disrupt a stable supply of electricity and sensitive communication flows.

(4) Renewables are often considered as indigenous energy resources, which – in contrast to fossil fuels – do not need to be imported from other producing countries, often being politically unstable. The myth suggests that renewables do not cause any inherent risks and vulnerabilities, but rather decrease import dependencies on politically unstable producers and, thereby, increases supply security. However, renewables, batteries and other “green technologies”, including further digitalisation, AI systems and robotics, need many CRMs (i.e., rare earth, lithium, cobalt, platinum and others). Their production is often concentrated in few countries (e.g., China has a 90% production and export monopoly of rare earth) and huge mining companies. A stable supply and rise of global demand may have wide ranging geo-economic and geopolitical implications – particularly when future economic and military superpowers such as China will have the combined capability of being one of the future technology and R&D leaders of AI having available the much-needed CRMs as well as the production capabilities to dominate the worldwide demand and value chains of their supply.

Hence, non-energy resource security will become a major dimension in global energy security in the future. These challenges not only require a comprehensive discussion of national energy systems<sup>4</sup> but also more multilateral cooperation on re-

---

<sup>4</sup> See Francois Austin, “How to Solve the Energy ‘Trilemma’”, 27 November 2017, <https://www.greenbiz.com/article/how-solve-energy-trilemma>, accessed 30 January 2018.

gional and global levels to avoid new antagonistic conflict patterns and geopolitical rivalries.

Instead of analysing these four dimensions in more detail, I will explore and discuss digitalisation in the worldwide energy sector, which is offering both new economic and business opportunities, but also new risks and vulnerabilities on national, regional and global levels. In this context, I will also address some wider strategic implications for Asia.

## **UNDERSTANDING DIGITALISATION IN THE INTERNATIONAL ENERGY SECTOR**

The energy sector has always been at the forefront of adapting technological innovations. Oil and gas companies already operate some of the world's most powerful supercomputers. The new US shale revolution 2.0 includes cloud computing services, which store and analyse an unprecedented amount of data on seismic information, drilling and production much more precisely. Digitalisation and automation, as well as new alliances between oil and IT companies, will make future operations of oil and gas drilling even safer, cleaner, and more efficient. Moreover, the industry is already coupling AI with new advanced sensors, sophisticated seismic data processes and management as well as automated drilling rigs to maximize production of tight oil and shale gas with only a few engineers and technicians.

Power utilities have proved to be “digital pioneers” since the 1970s by using technologies to improve grid management and operations, while oil and gas companies used digital technologies for modelling exploration and production assets. Today, the increasingly fast pace of digitalisation with the widespread use of “Information and Communication Technology” is changing the established energy sector and the traditional energy business models by creating new consumption patterns, providers and platforms (also from outside of the energy sector).

Digitalisation and other technology developments allow better decentralisation and distribution of renewable energies, and enable their linkages with smart grids (i.e., “microgrids”) and smart metering technologies (“smart meter data hubs”) as well as new battery storage solutions. Therefore, German utilities, for example, are striving to become consumer-centred and service-based organisations, but their actual market share in the digitalised retail market is still very small. New business models need to be developed to address the “3 Ds”. For those energy utilities, the major challenge is not just the digitalisation itself, but the interlinkages with the other two “Ds” and its impacts on the markets, including the smart home market, and implications for their future business models and business development strategies.


Furthermore, expanded robotics and AI promise that half of the activities (not jobs) traditionally carried out by workers can be automated.<sup>5</sup> “Deep learning systems” are using artificial neural networks and real-time data to predict demand trends on a hyper-regional basis.<sup>6</sup>

**Figure 1: Recent and Forthcoming Changes in the Global Energy Sector.**

**Energy market changes and impacts**

<i>Recent changes in global energy markets</i>	<i>Forthcoming changes due to:</i>	<i>Impacts</i>
<ul style="list-style-type: none"> <li>● Expansion of renewables</li> <li>● Energy efficiency technologies and strategies</li> <li>● Decarbonization/disinvestment in fossil fuels</li> <li>● U.S. shale oil and gas revolution</li> <li>● LNG revolution</li> <li>● Rising cyberattacks on critical energy infrastructures</li> <li>● Decreasing public acceptance of energy infrastructure investments (i.e. in fossil fuels)</li> </ul>	<ul style="list-style-type: none"> <li>● Electrification of the transport and heating sectors</li> <li>● Digitalization               <ul style="list-style-type: none"> <li>- Energy utilities and electricity/power sectors (smart grids, smart metering, internet of things/smart home etc.)</li> <li>- Fossil fuel production</li> </ul> </li> <li>● Blockchain technology</li> <li>● Decentralization</li> <li>● Battery storage solutions</li> <li>● Quickening decarbonization</li> </ul>	<ul style="list-style-type: none"> <li>● Energy prices and competition between fossil fuels and renewables</li> <li>● Additional rise of worldwide and European electricity demand (already growing much faster than global primary energy consumption)</li> <li>● Increasing need for battery or other storage solutions</li> <li>● Rising cyber risks and vulnerabilities of critical energy infrastructures due to internet linkages and digitalization</li> <li>● Socioeconomic and political stability of oil and gas producers</li> <li>● Risks and vulnerabilities of the rising critical raw material demand for supply security</li> </ul>

*Source: Dr. Frank Umbach*


www.GISreportsonline.com

Source: Dr. F. Umbach/GIS, 2018.

Digitalisation and electrification have also led to rising competition among energy companies which face at the same time new competitors from outside (e.g., IT companies). This is even true for the oil and gas companies, which have created strategic alliances and partnerships with IT companies. Renewables, as well as energy storage solutions, have become much cheaper and competitive. This also offers oil and gas companies new options to diversify their energy sources and businesses and has led to a new class of hybrid energy enterprises, reconciling fossil fuels with renewables. In Europe, Royal Dutch Shell and Total have also begun to invest in further expansion into the electricity supply chain and building a retail energy business in Europe for an integrated power supply chain from generation to retail supply, challenging traditional power companies. But the barriers and challenges to implementing the full spectrum of new digital technologies – ranging

<sup>5</sup> See also Patrick McGee, “Auto Bosses Accused of Failing to Train Workers for AI Revolution”, FT, 17 June 2018.

<sup>6</sup> See also Richard Waters, “‘Deep Learning’ - the Hot Topic in AI”, FT, 14 May 2018.



from adequate timing of capital-intensive large projects, the existing infrastructures, risk-averse management perspectives toward introduction of new disruptive technologies, high fragmentation along the supply chains, and long-term demand trends, to dependence on a up-to-date information technology support infrastructure – might slow their fast implementation and full exploitation of the new disruptive technologies.

The electricity sector is expected to undergo the greatest digital transformation as it will break down the traditional boundaries between various energy sectors, increase flexibility, blur the distinction between generation and consumption as well as increase the rate of integration across entire systems. Since 2014, global investments in digital (electricity) infrastructure and software have jumped by 20% per year up to US\$47bn in 2016. Around 90% of the world's data have been created in just over the past two years! While the digitalisation is at first glance primarily a technology revolution, its impacts for companies and governments will change markets, business models, organisational structures and companies' cultures substantially in the forthcoming years. The potential savings in costs and investments in the worldwide power sector due to digitalisation by reducing operation and maintenance costs, improving the efficiency of the power plants and networks, decreasing unplanned outages and downtime, and extending operational lifetimes of assets has been estimated at around US\$80bn between 2016 and 2040. The current electricity model is increasingly being disrupted and undergoing major change. Even fundamentals are increasingly questioned: (1) electricity prices are always based on usage-based prices (i.e., negative electricity prices); (2) only energy companies will generate and sell electricity; (3) all private and industrial customers need an electricity and wider grid connection as well as a regional system operator; and (4) local distribution companies will necessarily function as a stable and profitable source of funds to local governments owning them. All these traditional assumptions will change in the forthcoming years.

In consequence, the whole electricity industry needs to adopt radical changes in its business models. Many won't survive and/or be able to compete in fundamentally different future markets. The greatest potential for the digitalisation in the energy sector might be the elimination of traditional segmentation and boundaries between various energy sectors as well as with other sectors and industries. They will enforce the integration of entire systems and the creation of new ones. In this context, connectivity becomes the most important driver factor for the digitalisation of the industrial and electricity sectors.

## GEOPOLITICAL DIMENSIONS

In contrast to the years before 2010, the world is no longer confronted with any scarcity of fossil fuels, which had sparked debates of a near “peak oil”-era with ever increasing fossil fuel prices. Instead, the present world has now to cope with fossil fuel oversupplies and rapidly decreasing fossil fuel prices, which have changed the overall geo-economic and geopolitical balance of power between consumer and producer countries, leading to new “buyers’ markets”.

Traditionally, geopolitical risks and vulnerabilities due to supply disruptions have been considered as exclusively linked with fossil fuels as renewables are immaterial and available almost everywhere (“no one can ever embargo the sun”). Their expansion has also promoted the overall decentralisation of energy supplies – widely perceived as enhancing energy security. They may not just reduce the dependence on politically unstable fossil fuel suppliers (both state and corporate), but also their political and geo-economic power in international relations. The loss of their previous geo-economic and geopolitical influence translates into the emergence of global “buyers’ markets” instead of the traditional “sellers’ markets”. The creation of “prosumers” (energy consumers becoming simultaneously energy/electricity producers) and the redistribution of economic as well as political power offers new participation, investment and strategic influence to new centralised powers (e.g., internet giants such as Facebook, Amazon, Netflix, Google and others, which become either energy producers themselves or are digital technology partners of energy companies) as well as to new players on the local level as a result of the decentralised energy supplies. According to this logic, expanding RES and “energy abundance” will “depoliticise markets” by decreasing the traditional geopolitical risks of supply disruptions and, therewith, enhancing national, regional and global energy supply security in our traditional understanding and defined concepts.

While traditional supply risks such as supply disruptions due to political instabilities in producer countries or attempts at political blackmail (i.e., Russia) indeed will decrease and be marginalised in the mid- and long-term future, new geopolitical risks and vulnerabilities will arise with the expansion of renewables and the rapid introduction of new disruptive technologies (including smart meters, smart and super- as well as micro-grids etc.) in the context of digitalisation, electrification of the transport and heating sectors, robotics and Artificial Intelligence systems. Up to now, supporters of RES have hoped that power generation will become more dispersed and decentralised, while regions may become more self-sufficient in energy supply, triggering a process of “energy democratisation”, in contrast to the traditional centralised energy systems. Enhanced energy access via mini-grids and

rooftop solar panels in Africa, South and Southeast Asia as well as other regions has offered new energy options for reducing “energy poverty” alongside the further growth of the global population. But the changing energy systems, from the traditional one, coping with scarcity challenges, to abundant RES, will inevitably produce losers such as the currently leading oil and gas producer superpowers in the mid- and long-term future.

It is indeed true that a more diversified energy mix increases energy supply security and renewables decrease those traditional geopolitical risks of supply disruptions. But it has largely been overlooked that the expansion of renewables also creates new geopolitical dependencies, risks and vulnerabilities.<sup>7</sup> The worldwide electrification of the transport and other industry sectors, the development of a new generation of batteries for electricity storage as well as the digitalisation of the industries, including the spread of robotics and Artificial Intelligence systems in the industry (“industry 4.0”) will further boost the worldwide demand for CRMs such as lithium, cobalt, rare earths and others.<sup>8</sup> As a result, this might create new, unprecedented challenges, including bottlenecks and supply shortages, for the global supply chains of the CRMs at each stage, ranging from mining to processing, refining and manufacturing. The challenge again is not so much physical scarcity of those materials, but rather timely sufficient investments and their concentration in production in even fewer producer countries as well as companies. Compared with the conventional oil and gas resources, the production of CRMs is geopolitically even more challenging and problematic – particularly when the future rise of the global demand is taken into consideration.

The production of CRMs is geopolitically – compared with the concentration of conventional oil and gas resources – more challenging and problematic as currently 50% of CRMs are located in fragile states or politically unstable regions. Moreover, security of supply risks are not just confined to primary natural resources and CRMs but also include the import of semi-manufactured and refined goods as well as finished products. Manipulated prices, restricted supplies and attempts at

---

<sup>7</sup> See also Megan O’Sullivan, Indra Overland, and David Sandalow, “The Geopolitics of Renewable Energy”, Columbia/SIPA, Belfer Center/Harvard and Norwegian Institute of International Affairs (NPI) 2017; Daniel Scholten, “Renewable Energy Security”, EUCERS-Newsletter, Issue 64, April 2017, pp. 2-4; Daniel Scholten and Rick Bosman, “The Geopolitics of Renewables: Exploring the Political Implications of Renewable Energy Systems”, Technological Forecasting & Social change, 103/2016, pp. 273-283; Meghan L. O’Sullivan, “Renewables Won’t End Geopolitics of Energy”, Japan Times, 24 August 2017, and Ian Morris, “Imagining a World after Fossil Fuels”, Stratfor, 22 March 2017.

<sup>8</sup> See also Walt Patterson, “How Renewables Will Change the Geopolitical Map of the World”, [www.energypost.eu](http://www.energypost.eu), 9 February 2018.

cartelisation of CRM markets with wide-ranging negative economic consequences are not just restricted to producing and exporting countries. Powerful state and private companies have also been responsible for non-transparent pricing mechanisms for many precious CRMs. Global supply chains have become ever more complex with blurred boundaries between physical and financial markets and weakly governed market platforms. These market imperfections lead to the manipulation of prices, thus threatening the stability of the future security of supply of CRMs.

Given China's strategic interest to become the world's largest battery producer and market for electric mobility as well as the worldwide interest (i.e. South Korea, Japan, the EU's and U.S.) in new industrial battery storage options, the dependence on CRMs such as lithium, cobalt, graphite, rare earth and others will equally rise. Those geopolitical impacts have already been highlighted during 2010–2011 when China, in the midst of an escalating diplomatic conflict with Japan, stopped all exports of Rare Earth Elements (REEs) to the world's biggest importer and blackmailed Tokyo diplomatically by instrumentalising its status as the world's largest producer and exporter of REEs. It sent a troubling message to the world that the new rising Asian economic and military power might not respect international law or the existing global rules of the WTO and cast doubt on the political willingness of Beijing to accept the regional and global responsibilities that go with its emerging superpower status. During the last months, China has further strengthened its efforts to control the entire global supply chain of lithium, from owning international mines to production, up to manufacturing of batteries and electric vehicles (EVs).

The future CRM supply security depends largely on timely investments, and alternative strategies such as (1) the re-use of CRMs; (2) reduced use; (3) substitution; and (4) recycling. Using these strategies would allow reducing the imports of CRMs from a long-term perspective. These options need also to be an integral part of the development of "circular economies" as a response strategy, by using CRMs more economically, efficiently and environmentally, thereby reducing their mining demand in order to strengthen their security of supply.

The present energy transition<sup>9</sup> and the digitalisation have fuelled a global race for the best and most disruptive technologies and competition in access to as well as strategic control of critical raw materials, such as rare earth, lithium, cobalt and others. These strategic developments have wider geo-economic and geopolitical impacts and may transform international energy relations between countries and

---

<sup>9</sup> Quoted following Quinn Connelly, "Energy Transitions? Not so Fast", RealClear Energy, 18 April 2018.

regions. The heightened competition for global technology-industrial leadership has already led to a growing technology race between the US and China, which is shaping the present and will determine future geopolitical competition between the two superpowers of the 21st century.<sup>10</sup> Those technology transformations could also lead to a new “securitisation” of raw materials alongside the monopolisation of political *and* economic power, strengthening the autocratisation of political systems inside countries as well as internationally.<sup>11</sup> In this context, China’s worldviews and geopolitical strategies – such as the “Belt and Road-Initiative” (BRI), formerly known as “One Belt One Road” Strategy (OBOR) – and its nationalist tendencies in its domestic policies under President Xi Jinping are of utmost strategic importance for the West and global stability.

## CYBER SECURITY REQUIREMENTS

The expansion of renewables is linked with other disruptive technologies (such as smart meters, smart grids, batteries and other new storage options), the further digitalisation of the energy sector, the electrification of the transport and heating sectors as well as robotics and Artificial Intelligence. As the future energy sector in general and the electricity generation, supply and distribution networks in particular will be linked to the internet, cyber security challenges in the energy sector will dramatically increase the risks of national or transnational electricity blackouts, threatening the overall functioning of all critical infrastructures, as they are dependent on a stable electricity supply and a functioning access to a reliable Internet.

Given this internet interconnectivity of the energy and other industrial sectors, the existence of a vast amount of sensitive data and asymmetric conflict patterns have dramatically increased the risks and vulnerability of “Critical Energy Infrastructures (CEIs)” to sophisticated cyberattacks by national hacker groups, transnational crime organisations and state-supported secret services.

In recent years critical infrastructures have increasingly been the target of cyberattacks. In 2009, viruses were discovered in the US electricity grid that

---

<sup>10</sup> See also Richard B. Freeman and Wei Huang, “China’s ‘Great Leap Forward’ in Science and Engineering”, NBER Working Paper, No. 21081, 2015; “The Tech Giants Growing Behind China’s Great Firewall”, Stratfor.com, 6 February 2018, and Kai-Fu Lee; Paul Trioto, “China’s Artificial Intelligence Revolution. Understanding Beijing’s Structural Advantages”, Eurasia Group, Sinovation Ventures, 2017 and “The Coming War Tech War with China”, Stratfor.com, 6 February 2018.

<sup>11</sup> See also Peter Hefele, “Of Streams of Data, Thought, and other Things”, KAS-International Report 1/2018, pp. 56-63 (58).

supposedly originated from China and Russia. It could have made the US a victim of blackmail if relations between the two countries had soured. While the knowledge of creating computer viruses is expanding exponentially, many industrial computer systems that control power plants (via Supervisory Control and Data Acquisition/SCADA-systems) as well as other CEIs are often old and outdated even in Western countries, making them very vulnerable to cyberattacks.

As all critical infrastructures (CIs) are dependent and directly or indirectly connected to the regular internet, and dependent on a stable supply of electricity, the energy and in particular electricity sectors of highly industrialised countries may be considered as the Achilles heel of their political, social and economic stability.

Digitalisation of the electricity sector is also linked with the digitalisation of the building sector and “smart home” technologies such as smart thermostats, smart lighting and various IoT-devices. By 2020, more than 20 billion connected IoT-devices, and nearly 6 billion smartphones are expected to be online. By 2040, 1 billion households and 11 billion smart appliances could be an active part of a highly interconnected electricity system. Their “smart demand response” has been estimated to provide 185 GW of inherent flexibility to the system (the presently installed electricity supply capacity of Italy and Australia combined). It could save up to US\$270 bn of investment in new electricity supply infrastructure needed to ensure energy supply security. The roll-out of “smart charging” of electric vehicles, shifting the charging to off-peak times, could save another US\$100-280 bn by avoiding the need to build new electricity infrastructure by 2040.

But the widespread introduction and use of digital technologies and devices, as well as their benefits, are dependent on overcoming the manifold challenges in regard to technical and economic considerations (cost-benefit calculations of private consumers and industry), safety and security risks (against cyberattacks) and concerns regarding private data security and timely as well as adequate political guidelines (introducing new regulations and defining new standards). Critical questions about how much information people are willing to share with electricity and internet service providers, how private and commercial confidentiality can be best protected, and who owns, collects and uses consumer-specific data (including for prosumers), including for third parties, need to be answered. A new regime of close and trust-infused collaboration in the form of public-private partnerships (PPP), involving the energy and internet industry as well as governments in institutionalised PPP discussions, has yet to be created.

## STRATEGIC PERSPECTIVES

The geo-economic and geopolitical megatrends outlined above are impacted by the global ascendancy of a rising number of autocratic states with a (combined) unprecedented economic power and the political will to use their economic-financial soft power to divide and weaken Western democracies. The share of “not free” and “partially free” countries in global income has grown from 12% to 33% nowadays – a level not seen since the early 1930s and the rise of fascism in Europe.<sup>12</sup>

China, for instance, has proclaimed a “digital silk road” and announced investments in overseas fibre-optic cables, telecommunication and internet infrastructures, data and cloud computing services, global positioning, wireless communications, and smart city sensors, all of which have attracted Asia’s and worldwide attention, but also increasing concerns. The potential insertion of backdoor viruses and mechanisms could increase China’s industrial and political espionage, intelligence and propaganda missions in BRI partner countries. Beijing is suspected of being willing to export its worldwide unrivalled internet censorship and its comprehensive political control of data collection and traffic with its “Belt and Road Initiative”. It raises basic questions in regard to human rights by undermining personal freedom, privacy as well as anonymity as granted by liberalised Western democracies and their constitutions.<sup>13</sup>

For Asia’s energy sector and other industrial sectors, digitalisation offers new perspectives for enhancing energy efficiency, expanding renewables with new storage options, boosting productivity and decreasing the costs of production as well as business operations. New risks are primarily perceived with cyber security, but – with the exception of Japan and South Korea – not so much in regard to the supply security of CRMs. In Southeast Asia, Singapore has been at the forefront as a “smart city state” in addressing various cyber security challenges nationally and enhancing cyber security cooperation as well as coordination within ASEAN. The initiated project of a Japan-ASEAN Cyber Centre not only serves the enhancement of resilience of cyber security on both sides, but also growing interregional cooperation and new global governance initiatives for international standards and norms. But perceived state-supported “offensive cyber operations” have, not only in the US but also in Asian countries, caused increasing cyber security concerns. The “Five Eyes”

---

<sup>12</sup> See also Yascha Mounk and Roberto Stefan Foa, “The End of the Democratic Century”, *Foreign Affairs*, 16 April 2018, here p. 2.

<sup>13</sup> See also Stewart M. Patrick, “Belt and Router: China Arms for Tighter Internet Control with Digital Silk Road”, *Council of Foreign Relations*, 2 July 2018 and Kenny Liew, “Belt & Road Bolsters China’s Technological Clout”, *CSIS-Reconnecting Asia Project*, 24 September 2018.

intelligence alliance between Australia, Canada, New Zealand, the UK and the US has not only deepened security consultation and coordination to combat perceived Chinese and Russian cyber threats and investments, but the member countries are also willing to share their intelligence with European partners such as France and Germany as well as Japan and other countries in the future. The real challenge in regard to the future global governance of the internet and digitalisation between Western countries and China (and Russia) is clearly linked with their respective different political systems as China's understanding of "cyber sovereignty", for instance, makes the global internet a battlefield for domestic political stability (i.e., control of the world's largest online population) and wider-defined national security interests inside and outside the country.

Although not all implications for and impacts on the worldwide, regional and national energy sectors can already be identified and analysed in regard to digitalisation challenges in detail or are even fully understood, it has already become clear that those unprecedented technological changes in the worldwide energy sectors will also have wide-ranging geo-economic and geopolitical implications. Many geopolitical implications are still being overlooked as current discussions concerning digitalisation alongside the other developments still centre on the economic changes, the management of the perceived short-term challenges of the energy transition to a non-fossil fuel age and the risks for traditional business models and strategies as well as company cultures rather than on the long-term implications for the worldwide energy and raw material supply security as well as on an adequate global governance system for it.



**Dr. phil. Frank Umbach** is Research Director at the European Centre for Energy and Resource Security (EUCERS), King's College, London ([www.eucers.eu](http://www.eucers.eu)); Executive Advisor, ProventisPartners, Munich (M&A; [proventis.com](http://proventis.com)); Adjunct Senior Fellow at the S. Rajaratnam School of International Studies (RSIS), Nanyan Technological University (NTU), Singapore ([www.rsis.edu.sg](http://www.rsis.edu.sg)), and Visiting Profssor at the EU-College at Natolin (Warsaw) on EU energy (foreign) policies (<https://www.coleurope.eu/about-college/welcome-natolin>). He has also done various consultancy projects on behalf of European and Asian governments/ministries, international organisations (i.e. NATO and EU), the international energy industry and consultancy companies on international energy security, geopolitical risks, cyber security and critical (energy) infrastructure protection/CEIP, as well as (maritime) security policies in Asia-Pacific. He was also Co-Chair of the European Committee at CSCAP (2002-2007); Dr. Umbach is the author of more than 500 publications in more than 30 countries worldwide; contract author of the *Geopolitical Intelligence Service (GIS)*, Liechtenstein since 2011, and Co-Editor of the (monthly intelligence reports on) *Energy and Geopolitics (E&G)*, Berlin.

# Defying Gravity: Europe in the Digital Transformation

*Mario Voigt*

“Because there is a law such as gravity, the universe can and will create itself from nothing.”

- Stephen Hawking

## Introduction: State of Play

The world is witnessing a New Moon Race. Looking at the digital economy, today's world is organised around two centres of gravity: the United States (US) and China. They are home to nine of the top 10, and 18 of the top 20 internet companies as measured by market capitalisation. All the leading companies in online search, social media, and e-commerce are based in these two countries.<sup>1</sup> But as the digital transformation continues, it is now shifting toward other economic sectors like transportation (Lyft and Uber) and hospitality (Airbnb). Other industries like automotive, manufacturing, financial services or healthcare will be swift to follow, and new technological developments in Artificial Intelligence (AI), the Internet of Things (IoT) and Big Data will spark even faster and more widespread disruption.

In the age of a growing digital economy, Europe's prosperity is being created, not inherited. The future of Europe depends on a competitive mindset and a willingness to gain an edge over the world's best competitors in the US and China. Hence, Europe's competitiveness depends on the capacity of its society, politics and economy to innovate and upgrade. As European companies and governments consider their own stakes in the game, a critical question remains: Are Europeans defying the two centres of gravity and if yes, how?

---

<sup>1</sup> Candelon, François, Reeves, Martin, and Daniel Wu. 2018. “18 of the Top 20 Tech Companies Are in the Western US and Eastern China. Can Anywhere Else Catch Up?”. Harvard Business Review, 3 May 2018.

This article discusses the role of Europe in a digitally transforming world. Therefore, in the first part, it examines the landscape of the digital world, where advanced technologies like AI, digital start-up ecosystems, e-commerce and platforms are dominated by the US and China. Most of the tech giants by market capitalisation are based in these two countries and Europe is being left behind. Hence, in the second section, the article seeks for necessary steps Europeans must take to become competitive. It explores the need for a better digital infrastructure, a strengthened Digital Single Market and a European digital mindset. Finally, it proposes a more competitive and particular European approach.

## **Europe between Two Centres of Gravity: Uncle Sam versus The Dragon**

We are in the midst of a technological revolution: digitalisation. For some, the revolution looks full of promises. Self-driving cars will bring us safely to our destination, communication networks connect continents and 3-D printers meet all customer-specific requirements. However, others suggest a different scenario in which the US, Europe and China are engaged in a race for digital supremacy. The one who loses it, they say, loses the future. With half of the world's population online, demonstrating competitiveness and market potential for further digital economic growth is key for success.

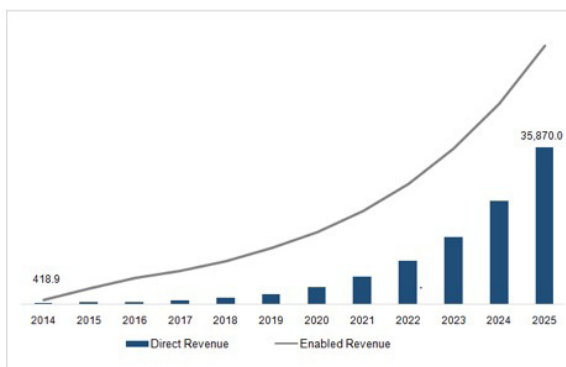
Technology advances quickly and the digital landscape is mainly driven by an imbalance in the platform economy. In order to measure future potential, one has to look at innovation and start-up ecosystems, investment in new technologies and market capitalisation in the digital economies of the US, China and Europe.

## **Advanced Technology: Putting a Stamp on Artificial Intelligence**

Developments in Artificial Intelligence and robotics are generally recognised as the main driver of future growth, competitiveness and job creation by increasing productivity and efficiency, and lowering costs. But AI also triggers far-reaching societal and economic changes, which will transform all aspects of life from employment, the social contract to warfare. The impact of AI leadership has been summed up by

Russia's President Vladimir Putin: "whoever becomes the leader in this sphere will become the ruler of the world".<sup>2</sup>

In Artificial Intelligence, the US and China are in an arms race for global leadership. Rapid improvements in information storage capacity, high computing power, and considerable advancements in Artificial Intelligence technology in end-use industries are driving economic growth. The global Artificial Intelligence market size was valued at 641.9 million USD in 2017 on the basis of its direct revenue sources and at 5,970 million USD in 2017 on the basis of AI-based gross value addition (GVA) prognoses. The market is projected to reach 35,870 million USD by 2025 in direct revenue sources, growing at a compound annual growth rate (CAGR) of 57.2% from 2018 to 2025.<sup>3</sup>



Source: Artificial Intelligence Market Analysis. 2017.

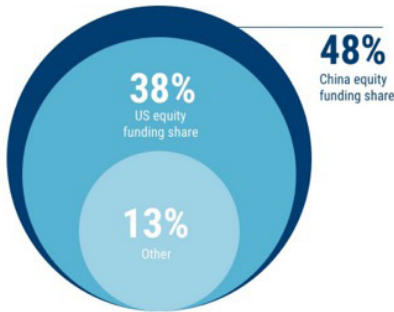
While taking an either more state-driven (China) or a more private-sector-driven (US) approach, in their entrepreneurial frenzy, China and the US are outshining other countries. In 2017, China's Artificial Intelligence start-ups took 48% of all dollars going to AI start-ups globally, more than that by US start-ups (38%). Both combined made up almost 90 percent.<sup>4</sup>

<sup>2</sup> Gigova, Radina. 2017. "Who Vladimir Putin thinks will rule the world". <https://edition.cnn.com/2017/09/01/world/putin-artificial-intelligence-will-rule-world/index.html>. Accessed 18 December 2018.

<sup>3</sup> Grand View Research. 2017. "Artificial Intelligence Market Analysis By Solution (Hardware, Software, Services), by Technology (Deep Learning, Machine Learning, Natural Language Processing, Machine Vision), by End-use, By Region, and Segment Forecasts, 2018 - 2025". <https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-ai-market/methodology>. Accessed 18 December 2018.

<sup>4</sup> CB Insights. 2018. "Artificial Intelligence Trends To Watch In 2018". <https://www.cbinsights.com/research/report/artificial-intelligence-trends-2018/>. Accessed 18 December 2018.

**China dominates global AI funding**  
US vs. China total equity funding to startups in 2017



Source: CB Insights. 2018.

In July 2017, China outlined a bold multi-billion national strategic plan to catch up in global AI research by 2020 and to deliver major breakthroughs and become the world leader by 2030. On the other side, however, the US still leads in both the total number of AI start-ups and total funding overall. Both countries can draw from a wealth of data and opportunities for companies to scale quickly.

For some, Europe's role in this arms race is defined as that of a colony in the American tech empire.<sup>5</sup> Indeed, Europe still lacks a comparable AI ecosystem. Even the European Commission admits that Europe is lagging behind in private investments in AI: "2.4-3.2 billion EUR in 2016, compared to 6.5-9.7 billion EUR in Asia and 12.1-18.6 billion EUR in North America".<sup>6</sup> A lack of a strategic plan at the European Union (EU) level, a low level of public and external investment, a cautious approach to adoption from companies and the general public and no EU-wide liability rules on AI and robotics are credited for the underperformance.<sup>7</sup> This has led European countries to lay down AI-specific and comprehensive AI strategies (e.g., the UK, France), integrate AI technologies within national technology or digital roadmaps (e.g., Denmark) or develop a national AI Research and Development (R&D) or Work strategy (e.g., Finland). In April 2018, 25 EU countries signed a declaration to join forces and to engage in a collective "European approach" to AI. This push includes

<sup>5</sup> Lee, Kai-Fu. 2018. *AI Superpowers: China, Silicon Valley and the New World Order*.

<sup>6</sup> European Commission. 2018. "Factsheet: Artificial intelligence for Europe". <https://ec.europa.eu/digital-single-market/en/news/factsheet-artificial-intelligence-europe>. Accessed 18 December 2018.

<sup>7</sup> European Commission. 2018. "Digital Transformation Monitor. USA-China-EU plans for AI: where do we stand?". [https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM\\_AI%20USA-China-EU%20plans%20for%20AI%20v5.pdf](https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_AI%20USA-China-EU%20plans%20for%20AI%20v5.pdf). Accessed 18 December 2018.

funding for research to harvest the potential of Artificial Intelligence.<sup>8</sup> Under the research programme “Horizon 2020” public funding will be 1.5 billion EUR for the period 2018-2020 and adds up to a combined public and private investment in the same period of 20 billion EUR.<sup>9</sup> Germany’s Minister for Economy, Peter Altmaier, has called for a “European Airbus for AI” as an “Important Project of Common Interest” (IPCI), which fits Germany’s AI Strategy to create a joint French-German AI research centre.<sup>10</sup> In such an endeavour, European institutions will play a key role in coordinating, “filling in policy gaps that cannot be addressed solely at the national level and support the widespread development of competitive AI ecosystems throughout Europe” as well as aim for “a common, internationally recognised ethical and legal framework for the design, production and use of AI, robotics, and their increasingly autonomous systems”.<sup>11</sup> Prioritising the protection of the user’s privacy would be a distinctly different approach compared with the commercial quest for data and analytics of the American and Chinese companies. It seems that Europe will seize the opportunity by fostering a continent-wide collaboration to put its distinct stamp on AI by taking a different path from that of the US and China. Or in the words of Emmanuel Macron: “to be an acting part of this AI revolution”.<sup>12</sup>

## Innovation: Flourishing a Digital Start-Up Ecosystem

Such an aggressive competition for innovation and new technologies spills over to the venture capital market and start-up ecosystem. The US and China have the most active digital-investment ecosystems in the world. In fact, the members of the so-called “Global Unicorn Club”, private companies in the tech sector whose value exceeds 1 billion USD each, speak predominantly American-English or Chinese-Mandarin. For the 274 companies founded in 2003 or later that have

---

<sup>8</sup> European Commission, 2018. “EU Member States sign up to cooperate on Artificial Intelligence”. <https://ec.europa.eu/digital-single-market/en/news/eu-member-states-sign-cooperate-artificial-intelligence>. Accessed 18 December 2018.

<sup>9</sup> European Commission, 2018. “Factsheet: Artificial intelligence for Europe”. <https://ec.europa.eu/digital-single-market/en/news/factsheet-artificial-intelligence-europe>. Accessed 18 December 2018.

<sup>10</sup> Peter Altmaier at the Digitalgipfel, 4 December 2018.

<sup>11</sup> Delponte, Laura. 2018. “European Artificial Intelligence (AI) leadership, the path for an integrated vision”. [http://www.europarl.europa.eu/RegData/etudes/STUD/2018/626074/IPOL\\_STU\(2018\)626074\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2018/626074/IPOL_STU(2018)626074_EN.pdf). Accessed 18 December 2018.

<sup>12</sup> Thompson, Nicholas. 2018. “Emmanuel Macron talks to wired about france’s ai strategy”, 31 March 2018. <https://www.wired.com/story/emmanuel-macron-talks-to-wired-about-frances-ai-strategy/>. Accessed 18 December 2018.

reached unicorn status, half are in the US and China, which with its 69 has more than twice as many unicorns as Europe with 33.<sup>13</sup> More strikingly, American companies in Silicon Valley tend to scoop up the promising digital start-ups from Europe. From 2011 to 2017, the GAFAM companies<sup>14</sup> acquired more than 65 leading-edge European technology companies like Skype and AI pioneer DeepMind. And it is no wonder that in most cases the size of the respective European operations shrank after their acquisition.<sup>15</sup>

In China, the “Great Firewall” of legislative actions and technologies hinders competition and helps the three Internet giants to nurture a homegrown digital ecosystem that is now spreading beyond China. Baidu, Alibaba, and Tencent<sup>16</sup> have been developing a multi-industry digital ecosystem that touches almost every aspect of consumers’ lives. How important Chinese digital companies are for the venture capital market becomes obvious by looking at the numbers. In 2016, Baidu, Alibaba, and Tencent (BAT) provided 42 percent of all venture-capital investment in China. They have a far more prominent role than Amazon, Facebook, Google, and Netflix, which together contributed only 5 percent to the US venture-capital investment in that same year.<sup>17</sup>

In contrast, European companies make up about 11% of the total number in the “Global Unicorn Club”, that is, only 30 companies. These European start-ups have an aggregate valuation of about 64 billion USD, and operate across a range of industries, including fintech, e-commerce, or healthcare.<sup>18</sup> Europe’s tech community seems to be still “Balkanised” along national borders, while connections between local venture capitalists and start-up founders across the continent are needed if Europe ever wants to play in the big leagues.<sup>19</sup> The lack of a competitive venture capital market is described by the most recent numbers of 2017. From the 57 start-

---

<sup>13</sup> CB Insights. 2018. “The Global Unicorn Club”. <https://www.cbinsights.com/research-unicorn-companies>. Accessed 18 December 2018.

<sup>14</sup> GAFAM stands for Google/Alphabet, Apple, Facebook, Amazon, Microsoft.

<sup>15</sup> Candelon. 2018.

<sup>16</sup> Collectively known as BAT.

<sup>17</sup> Woetzel, Jonathan et al. 2017. “China’s digital economy. A leading global force”. <https://www.mckinsey.com/featured-insights/china/chinas-digital-economy-a-leading-global-force>. Accessed August 2018.

<sup>18</sup> CB Insights. 2018b.

<sup>19</sup> Scott, Mark. 2018. “Goodbye internet: How regional divides upended the world wide web”. 28 January 2018, Politico. <https://www.politico.eu/article/internet-governance-facebook-google-splinternet-europe-net-neutrality-data-protection-privacy-united-states-u-s/>. Accessed 18 December 2018.

ups which became unicorns in 2017, 32 are from the US, 18 from China and just four from Europe; interestingly all four were from the UK.<sup>20</sup> The lack of appropriate and swift funding of new ideas to make them products or a company is a major weakness of Europe.

## **Market Share: Competing in the Platform Economy and E-Commerce**

Even in a digital world, size matters. In a digital economy, Napoleon Bonaparte's old saying becomes reality: "China is a sleeping lion. Let her sleep, for when she wakes she will shake the world." In e-commerce, China is the world's largest market and accounts already for more than 40 percent of the value of worldwide transactions compared to less than 1 percent only about a decade ago. The current value of China's e-commerce transactions is estimated to be larger than that of France, Germany, Japan, the United Kingdom, and the United States combined. One explanation for China's dominance is the explosion in use of mobile payments, which grew from just 25 percent in 2013 to 68 percent in 2016. In 2016, the value of mobile payments related to individuals' consumption was 790 billion USD, 11 times that of the United States.<sup>21</sup>

Two factors drive this quick digital transformation of the Chinese Dragon. Firstly, China is benefiting from its large domestic market to achieve scale and to surround itself with rich ecosystems of start-ups, suppliers and customers. In 2016, 731 million of China's 1.4 billion citizens used the internet, more users than in the European Union and the United States combined. Beyond scale, it is the enthusiasm for digital tools among China's much younger consumer base which accelerates growth and quick adoption.

Such an imbalance can also be found in the platform economy. According to the Center for Global Enterprise, the Asia-Pacific has seen the creation of 82 digital platforms with close to 350,000 employees and a combined market capitalisation of 930 billion USD. Europe is trailing behind both the United States and the Asia-Pacific region in encouraging successful platform enterprises. Only 27 digital platforms were created in Europe, with 109,000 employees and a combined market capitalisation of 181 billion USD. However, Europe and China do not come close to

---

<sup>20</sup> Desjardins, Jeff. 2017. "The 57 Startups That Became Unicorns in 2017". <https://www.visualcapitalist.com/57-startups-unicorns-in-2017/>. Accessed 18 December 2018.

<sup>21</sup> McKinsey. 2018.



the combined market capitalisation of US-based digital platforms – about 3 trillion USD.<sup>22</sup>

## Market Capitalisation: Financial Strength in Tech

From 2010 to 2017, the market capitalisation of the GAFAM companies (Google/Alphabet, Amazon, Facebook, Apple, and Microsoft) increased by 2.6 trillion USD. In contrast, the value of the 28 non-GAFAM companies that make up the Dow Jones Industrial Average rose by 2.1 trillion USD. In China, Alibaba and Tencent are among the 10 most valuable companies in the world and, along with Baidu, are collectively worth more than 1 trillion USD.<sup>23</sup> In today's digital economy the US and China are the two centres of gravity, where their tech giants dominate the markets. Out of the top 10 companies by market capitalisation nine are based in these two countries.

There is another aspect aside from the duality between the US and China driven by the winner-takes-all mentality of digital companies in the US and China. Looking at the world's 20 largest tech giants, there is a divide between the top-tier companies and those further down the ladder. The top companies on the list like Apple, Alibaba, Alphabet, Amazon, Microsoft and Tencent are all above the 450 billion USD mark and account for over 80% of the total value of the Top 20 tech companies. Not a single company hovers between 200 and 450 billion USD. This underpins the divide. First of all, digitalisation is driven by American or Chinese companies, and secondly, for tech newcomers it is pretty hard to vault into the upper echelon of the market. The only European company in the Top 20 ranks is German based SAP.

In conclusion, Europe is facing two major risks. First, European companies are struggling to keep pace with their US and Chinese competitors in core areas of technological change. In particular, platform economies and digital ecosystems are heavily imbalanced from the European point of view. Second, the digital arms race between the US and China in the area of Artificial Intelligence draws tech-talents away from the European market. It has a strong base of homegrown engineering talent and a good start-up creation rate, but the availability of venture capital in Europe is sparse compared to the financial El Dorado in the US or the Chinese-style government approach to sheltering and nurturing its tech industry.

---

<sup>22</sup> Evans, Peter, and Gawer, Annabelle. 2016. "The Rise of the Platform Enterprise: A Global Survey", Center for Global Enterprise.

<sup>23</sup> Candelon. 2018.

## A Third Way? Europe's Role in a Digital Age

The EU is prosperous, technologically advanced and has a well-educated but aging workforce. Europe is the second largest economy after China, coming in ahead of the US, and its domestic market is providing a powerful launching pad for world-changing technologies and companies. However, the digital world seems to gravitate towards either the Chinese or the American pole, whereas Europe is stuck in the middle. On the one hand, big US companies like Google, Apple, Facebook, Amazon, or Microsoft dominate in Europe. On the other hand, China is challenging Europe's industrial strength and innovative industries. Europe could potentially be the biggest loser of a successful "China 2025" strategy, when its leadership in research and development of high technology is challenged.<sup>24</sup> Accordingly, a competitive Europe has to address how prosperity for both citizens and companies can be produced to an extent that companies operating in the EU are able to compete successfully in the global digital economy while supporting high living standards for the average European: a global digital player and a better place to work and live in.

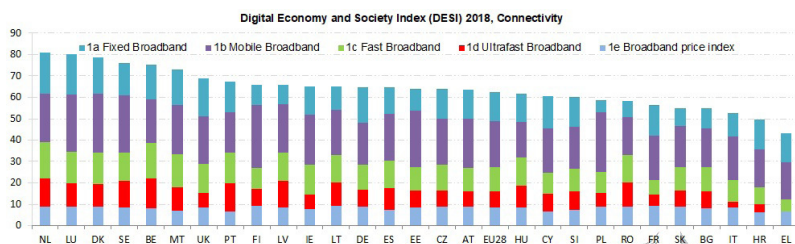
What are necessary steps to becoming competitive? Three major issues which hinder European excellence have to be addressed: digital infrastructure, a Digital Single Market and a digitally educated mindset.

### Improving the Backbone: Investing in Digital Infrastructure

A big bottleneck towards achieving a more competitive Europe is the slow expansion of digital infrastructure in the EU. There was a political target to achieve fast broadband coverage (more than 30 mega-bits per second) for all Europeans by 2020. But this seems to be out of reach, because in 2017, only 79% of all households had access to such connections (up from 55.8% in 2013).

---

<sup>24</sup> For different scenarios, see Bertelsmann Stiftung. 2016. China 2030. Szenarien und Strategien für Deutschland. However, in a Bruegel study, Alicia Garcia Herrero sees a paradigm shift in terms of US-China economic relations which could potentially benefit the European Union. <http://bruegel.org/2018/08/us-china-trade-war-whats-in-it-for-europe/>. See also: Alicia Garcia Herrero and Jianwei Xu, "How Big Is China's Digital Economy?". Working Paper, 2018.



Source: European Commission, DESI. 2018.

In the EU, 4G mobile coverage is almost universal at 98%. However, rural areas remain challenging, as 8% of homes are not covered by any fixed network, and 53% are not covered by any NGA technology (VDSL, Cable Docsis 3.0 and FTTP).<sup>25</sup> Upgrading the digital infrastructure is an expensive endeavour and depending on the time horizon and the planned investments, their costs often reach several billion. The European Commission estimated that 515 billion EUR would need to be invested over ten years to achieve a European Gigabit Society by 2025.<sup>26</sup>

Increasing data volumes, more cloud storage capacities and a demand for real-time communication between physical and virtual “things” as a precondition for Industry 4.0 amplify the need for an improved digital infrastructure. Today’s European capacities are insufficient to meet increasing demand by European industries, innovators and scientists who process their data outside the EU because their needs are not matched by the computation time or computer performance available in the EU. Tim Hoettges, CEO of Telekom, recently stated that only five percent of German data are hosted by SAP or Telekom. The other 95 percent are with the hyperscaler Amazon, Microsoft or Google.<sup>27</sup> If data is a prerequisite for machine learning and AI, the EU must find better ways to reduce this disproportion. However, the EU has none of the 10 most powerful supercomputers worldwide and only 4 of the top 20 supercomputers. This situation has constantly deteriorated since 2012, when the EU possessed 4 of the top 10 supercomputers. Moreover, the best supercomputers in Europe are supplied by non-EU vendors and are based on

<sup>25</sup> European Commission. 2018. “Broadband Coverage in Europe 2017”. <https://ec.europa.eu/digital-single-market/en/connectivity>. Accessed 18 December 2018.

<sup>26</sup> European Commission. Commission Staff Working Document SWD (2016) 300 final. For yearly improvements the EU’s Digital Economy and Society Index (DESI) indexes relevant indicators on Europe’s digital performance and tracks the evolution of EU member states in digital competitiveness, see: <https://ec.europa.eu/digital-single-market/en/desi>. Accessed 18 December 2018.

<sup>27</sup> Tim Höttges at the Digital Summit of the German Federal Government 2018, Nuremberg on 4 December 2018.

non-EU technology. At the moment, EU industry provides about 5% of supercomputing resources worldwide, but consumes one third of them.<sup>28</sup>

Digital infrastructure is critical to achieving the goal of a Gigabit Society in 2025.<sup>29</sup> Europe has to improve significantly in order to keep up with China and the US.

## **A Union: Smart Regulation for a Digital Single Market**

Market fragmentation and regulatory barriers in Europe are major hurdles to building a vibrant digital economy. Hence, Europe has set out an ambitious agenda and the European Commission wants to make the EU's single market fit for the digital age – moving from 28 national digital markets to a single one. The EU's Digital Single Market (DSM) strategy was launched in May 2015 and is one of the European Commission's ten political priorities. It aims to create an area where businesses and consumers have unrestricted access to digital goods and services all over Europe, with free flow of data and an environment that allows for both competition and innovation.<sup>30</sup> Expectations for the DSM are high, and the European Commission suggests that creating a fully functioning DSM could add about 515 billion EUR per year to the EU GDP and help to create several hundred thousand new jobs. As Alphabet chairman Eric Schmidt rightly observed: "A digital single market will give European entrepreneurs, who have all the right building blocks, the incentive to invest and the ability to achieve global scale at greater speed".<sup>31</sup>

The DSM strategy rests on three main policy pillars:

---

<sup>28</sup> European Parliamentary Research Service. 2017. Developing supercomputers in Europe. Brussels.

<sup>29</sup> In 2016, the European Commission updated and extended its digital infrastructure goals:

- By 2025, all major socio-economic drivers (such as schools, transport hubs, the main providers of public services or highly digitalised companies) should have access to connectivity of at least 1 gigabit/second.
- all urban areas and all major terrestrial transport paths should have uninterrupted 5G coverage by 2025.
- all European households should have access to internet connectivity of at least 100 Mbit/s, which is upgradeable to gigabit speed, see: European Commission (2016). Connectivity for a Competitive Digital Single Market – Towards a European Gigabit Society. Brussels.

<sup>30</sup> For a complete overview: Erixon, Fredrik and Lamprecht, Philipp. 2018. "The Next Steps for the Digital Single Market. From Where do We Start?". <http://ecipe.org/publications/the-next-steps-for-the-digital-single-market-from-where-do-we-start/>. Accessed October 2018.

<sup>31</sup> Schmidt, Eric. 2014. "Why Europe needs a digital single market". <https://www.weforum.org/agenda/2014/09/new-digital-era-europe/>. Accessed 18 December 2018.

- Access: better access for consumers and businesses to digital goods and services across Europe by removing barriers to cross-border e-commerce and access to online content while increasing consumer protection.
- Environment: creating the right conditions by providing high-speed, secure and trustworthy infrastructures and services supported by the right regulatory conditions. Economy and Society: maximising the growth potential of the digital economy and enhancing digital skills, which are essential for an inclusive digital society.<sup>32</sup>

Overall, this has impacted different policy areas. They stretch from data and data security, copyright issues, mobile and broadband infrastructure, online cross-border trade, to e-government. Furthermore, with the strategy the EU has established a set of support mechanisms such as the “Building a European Data Economy” Communication. Different policy groups and workshops, e.g. the EU Blockchain Observatory and Forum, or working groups on 5G networks, have been created.

Financially, the Digital Single Market strategy has pushed, along with Horizon 2020, for more funding of R&D, e.g., for Digital Innovation Hubs, or the Future and Emerging Technologies Fund. The EU Commission proposes an overall budget of 9.2 billion EUR to shape and support the digital transformation of Europe’s society and economy. Through this targeted financial support, the future long-term budget of the EU should help bridge the digital investment gap.

Initial successes of the DSM strategy can be witnessed. Achievements on roaming and cross-border portability of digital content, or the infrastructure push to pave the way for the roll-out of 5G in 2020, were well received by consumers and businesses alike and enabled them to make the transition to Industry 4.0 models. For the public sectors, the DSM’s objective is to promote the digitalisation of public administrations of member states, and the E-government Action Plan sets standards and will improve their level of digital cooperation. On the other hand, the Directive on Security of Network and Information Systems (NIS Directive) has been criticised for not sufficiently promoting cybersecurity in the EU. And the geo-blocking regulation falls short of ending the legislative fragmentation that prevents the emergence of a single market for businesses and consumers using e-commerce. Furthermore, international initiatives already address tax base erosion:

---

<sup>32</sup> The complete Digital Single Market strategy can be found at: <https://ec.europa.eu/digital-single-market/en/news/digital-single-market-strategy-europe-com2015-192-final>.

profit shifting and countries like France introducing legislation regarding taxation in a borderless digital world.<sup>33</sup>

One initiative has gained particular prominence. The General Data Protection Regulation (GDPR) aims for a more harmonised data protection regime across the EU. It has been received with mixed reactions. Some praise it as a new global standard for data protection and privacy in a digital world. Others criticise its demanding administrative costs from businesses and the difficulties it causes to develop and provide market-driven services for data on an individual level.

The GDPR is symptomatic of the overall approach of the current commission. It puts more emphasis on regulation than liberalisation.<sup>34</sup> The “Balkanisation” of the European digital market is still strong as they remain all too segmented along national lines. Hence, a new competitive digital market is not advancing fast enough to address the disruptive change occurring and some European regulations even harden the digital barriers to non-EU countries.<sup>35</sup>

---

<sup>33</sup> European Commission. 2018. “Fair Taxation of the Digital Economy”. [https://ec.europa.eu/taxation\\_customs/business/company-tax/fair-taxation-digital-economy\\_en](https://ec.europa.eu/taxation_customs/business/company-tax/fair-taxation-digital-economy_en). Accessed 18 December 2018. And European Commission. 2018. “Shaping the Digital Single Market”. <https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market>. Accessed 18 December 2018. See also: See OECD, Tax Challenges Arising from Digitalisation.

<sup>34</sup> Erixon. 2018.

<sup>35</sup> Clearly, the EU as an institution and their member states often follow different paths and strategies. For a differentiated look at the European member states, see: Erixon, Fredrik, and Lamprecht, Philipp. 2017. “New Coalitions for Europe’s Digital Future – Building Capacity, Improving Performance”, Brussels, which divides the member states based on their openness towards a digital transformation in digital managerialists, digital frontrunners, and digital convergers.

Remaining initiatives	Impact	Status
<b>Data and Cybersecurity</b>		
European cybersecurity agency <sup>4</sup>	Establishes an EU agency to undertake EU responses to cyber-threats.	Proposed in September 2017, awaiting co-legislature.
EU cybersecurity certification framework <sup>6</sup>	Establishes a framework to promote cybersecurity via appropriate certification of digital goods and services.	Proposed in September 2017, awaiting co-legislature.
<b>E-commerce</b>		
Modernize e-commerce contract rules <sup>7</sup>	Switches majority of rules from minimum to maximum harmonization; recasts Consumer Sales Directive for online contracts, creating regime separate from offline sales; introduces notion of conformity of goods; hierarchy of remedies for online sales; codifies case law on consumer's rights to withhold, refunds, time limits;	Proposed in December 2015, awaiting co-legislature.
Value added tax (VAT) for e-commerce <sup>8</sup>	Introduces threshold (€100,000 cross-border sales) for application of rules on suppliers of electronic services; one-stop shop for VAT registration for electronic services.	Adopted in December 2017, coming into force in 2019 for e-services and 2021 for goods.
VAT rate on e-publications <sup>9</sup>	Allows e-publications to have same VAT as print publications.	Proposed in December 2016, awaiting co-legislature.
<b>Telecommunications</b>		
Modernization of EU telecom rules (European Electronic Communications Code) <sup>10</sup>	Amends 4 existing directives to establish common rules and regulatory objectives; improves coordination and use of radio-frequencies across the EU; facilitates process of switching suppliers; promotes rights to affordable contracts.	Proposed in September 2016, awaiting co-legislature.

Source: Erixon. 2018.

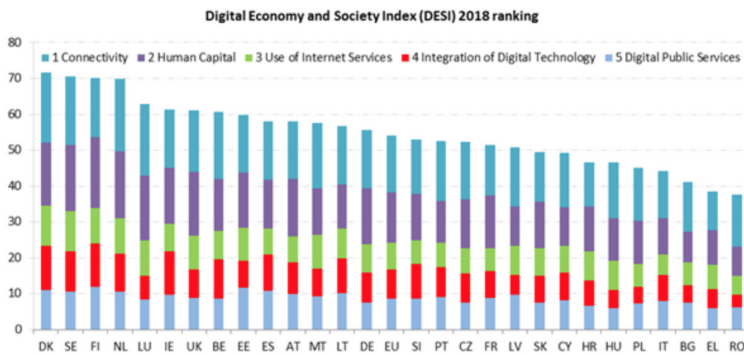
Currently, the pipeline for the DSM strategy, and its corresponding policies and initiatives, does not go far enough in promoting regulatory homogeneity and the next Commission has to push harder to allow EU member states to take full advantage of the Digital Single Market, by reducing the cost of cross-border exchange of digital goods and services, expanding the free flow of data and reducing regulatory red tape.

## A Distinct European Digital Mindset

A building block for a more competitive Europe is a sophisticated management of talent, a digital mindset and skills development. According to the Digital Economy and Society Index (DESI) of the EU,<sup>36</sup> 169 million Europeans between 16 and 74 years old – 44% – do not have basic digital skills. Of these, 77 million people have no digital skills at all. Furthermore, 37% or 80 million in the labour force do not have basic digital skills. The DESI report of 2017 projects a risk that Europe will lack 500,000 information and communication technology (ICT) specialists in 2020.<sup>37</sup>

<sup>36</sup> Digital Economy and Society Index (DESI) is a composite index that summarises relevant indicators on Europe's digital performance and tracks the evolution of EU member states in digital competitiveness, see: <https://ec.europa.eu/digital-single-market/en/desi>.

<sup>37</sup> European Commission. 2018. "Europe's Digital Progress Report 2017". <https://ec.europa.eu/digital-single-market/en/european-digital-progress-report>. Accessed 18 December 2018.

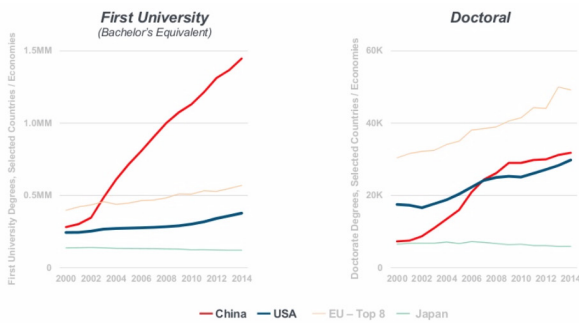


Source: European Commission, DESI. 2018.

While the Nordic countries of Denmark, Sweden, Finland, and the Netherlands have the most advanced digital economies in the EU, Romania, Greece and Italy have the lowest scores on the DESI. If Europe is ever going to meet its as-yet-unfulfilled promise as a global digital player, a continent-wide concerted effort to shape mindsets and skills is needed. The EU Commission launched the Digital Skills and Jobs Coalition, which brings together Member States and stakeholders from the private and public sectors to tackle Europe's existing digital skills gap and ensure the workforce is ready for the jobs of tomorrow. They defined four target areas: ICT professionals, labour force, citizens and education. The Coalition has a goal to train 1 million unemployed young people for digital jobs by 2020, to support the upskilling and retraining of the workforce and, in particular, to support small and medium enterprises (SMEs) and to modernise education and training for digital skills. Its activities have benefited several million citizens, with over 3.7 million trainings in digital skills provided, more than a million digital skills certifications issued, and 4,500 events conducted, from Riga TechGirls to Outreach with Educational Robotics.<sup>38</sup> Part of such an effort are also the Digital Innovation Hubs, which act as one-stop-shops where especially SMEs, start-ups and mid-size companies can get access to technology-testing, financing advice, market intelligence and networking opportunities. The EU Commission is investing 100 million EUR per year from 2016 to 2020.

<sup>38</sup> DESI Report 2018. Human capital. Riga Tech Girls, e.g., was the first community in Latvia dedicated to educating and inspiring girls and women about technology.





Source: Annual Natural Science or Engineering Degrees in Kleiner Perkins. 2018.

Beyond closing the digital skills gap, targeting students and technology experts becomes essential to offering opportunities to pursue trainings in advanced digital technologies, such as data analytics, robotics, Artificial Intelligence, blockchain technology, cybersecurity and high-performance computing. In this regard, Europe has potential: more Doctoral degrees in Natural Sciences and Engineering are pursued than in the US or China. In stark contrast, however, is the rapidly growing number of Chinese students with a first degree in Natural Sciences or Engineering.<sup>39</sup>

It seems that technological advances will demand unprecedented flexibility when it comes to learning. To predict what kind of knowledge and skills will still be relevant 20 years from now could be a rather difficult task, especially as some of the industries of tomorrow might not even exist yet. While education and basic science are potential equalisers, Europe’s strength could also arise from a different digital mindset and legal-philosophical tradition. Based on its culture, Europe should strive to set global standards and become a global norm leader, using its leverage and relevance due to its solid legal traditions, enduring focus on values and a European market of 500 million relatively rich consumers.<sup>40</sup> Setting standards on AI, Big Data, the IoT, critical thinking and a 360 degree ethical perspective become equally important to maintaining a competitive edge.<sup>41</sup> Germany’s digital modernisation strategy, “Industry 4.0”, is as much a way of upgrading its manufacturing base through machine-learning tools as a concept for a digital society.

<sup>39</sup> Kleiner Perkins. 2018. “Internet Trends Report 2018”. [https://www.kleinerperkins.com/files/INTERNET\\_TRENDS\\_REPORT\\_2018.pdf](https://www.kleinerperkins.com/files/INTERNET_TRENDS_REPORT_2018.pdf). Accessed 18 December 2018. S. 227.

<sup>40</sup> European Parliamentary Research Service. 2018. “Global Trends to 2035: Economy and Society”. Brussels.

<sup>41</sup> Trajtenberg, Manuel. 2017. “AI as the next GPT: a Political-Economy Perspective”. <https://www.nber.org/papers/w24245>. Accessed 18 December 2018.

Interestingly, the diverse European culture and their soft power mechanisms, which some perceive as a weakness, could become an asset.<sup>42</sup> As the basis of competition in a globalised world has shifted more and more to the creation and assimilation of knowledge and digitalisation, surprisingly the role of diversity has grown. Differences in cultures, values, economic structures, political institutions and regulations all contribute to competitive success. Here, Europe provides a unique perspective, which could mediate positions and bridge the gap between the two fairly extreme poles of the US and China in digital transformation. Or, as German chancellor Angela Merkel has pointed out with regard to data or AI: "In the US, control over personal data is privatised to a large extent. In China the opposite is true: the state has mounted a takeover". Europe has to find its place.<sup>43</sup>

## Europe: Show some Gravitas!

The world is in the midst of an exceptional revolution: Digitalisation has been a rather silent process moving horizontally through our economy and society, but with disrupting impact. It challenges not only businesses or societies but political entities as well. The current global digital power map knows two centres of gravity: the US and China.

The competition between the US and China seems like a New Moon Race and a test of two different systems. In this regard, Europe should defy gravity and show some gravitas in the digital transformation. Gravitas was one of the Roman virtues and valued as promoting collective and individual greatness. Hence, Europe must find its own way in the digital transformation if it wishes to remain relevant. It has to be done on the basis of strength, of competitiveness. Looking at the start-up ecosystem, the advanced technological developments, market share in the digital economy and the market capitalisation of the tech companies, Europe is clearly behind the US and China. To become a digital powerhouse, Europe will have to overcome its divisions, digital and otherwise, fight for its digital sovereignty and restore its digital ability to act autonomously.

The biggest threats are lack of time, dedication and vision. The digital innovation is accelerating, and competition is increasing. The EU must proceed with greater urgency and pool its combined resources. Most of Europe has the skills and

---

<sup>42</sup> Puddephatt, Andrew, Torreblanca, José Ignacio, and Prislán, Nika. "The New Great Game". [https://www.ecfr.eu/page/-/The\\_New\\_Great\\_Game\\_ECFR.pdf](https://www.ecfr.eu/page/-/The_New_Great_Game_ECFR.pdf). Accessed 18 December 2018.

<sup>43</sup> The Economist. "Can the EU become another AI superpower?". <https://www.economist.com/business/2018/09/20/can-the-eu-become-another-ai-superpower>. Accessed 18 December 2018.

experience necessary to improve productivity, to enhance innovation capability, and to customise products and services. Europe should use their good or leading position continent-wide, in areas such as robotics, Industry 4.0, networked mobility, or smart energy networks.<sup>44</sup> Europe's current position is built on a heritage of world-class science, business, education, entrepreneurship and innovation. Today, the EU has to play an active role in building world-class infrastructure, a digital education system based on innovation and values, and a strong Digital Single Market to move confidently in an open, global and competitive world.

**Mario Voigt** is Professor of Digital Transformation and Politics at the Quadriga University Berlin. He has been keynote speaker in more than 40 countries and published five books, numerous studies and articles on digital communication, digital transformation, and big data. Prof. Voigt is a consultant to companies, NGOs and public affairs campaigns and in the 2017 Bundestag election campaign, he was strategy consultant for mobilisation for Angela Merkel's re-election bid. Since 2009, Voigt has been elected twice as a Member of the State Parliament Thuringia and is a speaker on business, science and digital society.

## References

- Bertelsmann Stiftung. 2016. China 2030. Szenarien und Strategien für Deutschland.
- Candelon, François, Reeves, Martin, and Daniel Wu. 2018. "18 of the Top 20 Tech Companies Are in the Western US and Eastern China. Can Anywhere Else Catch Up?". Harvard Business Review. 3 May 2018.
- CB Insights. 2018. "Artificial Intelligence Trends To Watch In 2018". <https://www.cbinsights.com/research/report/artificial-intelligence-trends-2018/>. Accessed 18 December 2018.
- CB Insights. 2018. "The Global Unicorn Club". <https://www.cbinsights.com/research-unicorn-companies>. Accessed 18 December 2018.

---

<sup>44</sup> Körner, Kevin, Schattenberg, Marc, and Heymann, Eric. 2018. "Digital economics. How AI and robotics are changing our work and our lives". [https://www.dbresearch.com/PROD/RPS\\_EN-PROD/PROD000000000468705/Digital\\_economics%3A\\_How\\_AI\\_and\\_robotics\\_are\\_changin.pdf](https://www.dbresearch.com/PROD/RPS_EN-PROD/PROD000000000468705/Digital_economics%3A_How_AI_and_robotics_are_changin.pdf). Accessed 18 December 2018.

- Delponte, Laura. 2018. "European Artificial Intelligence (AI) leadership, the path for an integrated vision". [http://www.europarl.europa.eu/RegData/etudes/STUD/2018/626074/IPOL\\_STU\(2018\)626074\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2018/626074/IPOL_STU(2018)626074_EN.pdf). Accessed 18 December 2018.
- Desjardins, Jeff. 2017. "The 57 Startups That Became Unicorns in 2017". <https://www.visualcapitalist.com/57-startups-unicorns-in-2017/>. Accessed 18 December 2018.
- Erixon, Fredrik, and Lamprecht, Philipp. 2018. "Cooperation in Europe's Digital Economy. How do Countries Position Themselves?". <http://ecipe.org/publications/cooperation-in-europes-digital-economy/>. Accessed October 2018.
- European Commission. 2018. "Broadband Coverage in Europe 2017". <https://ec.europa.eu/digital-single-market/en/connectivity/>. Accessed 18 December 2018.
- European Commission. 2018. "Factsheet: Artificial intelligence for Europe". <https://ec.europa.eu/digital-single-market/en/news/factsheet-artificial-intelligence-europe>. Accessed 18 December 2018.
- European Commission. 2018. "Digital Transformation Monitor. USA-China-EU plans for AI: where do we stand?". [https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM\\_AI%20USA-China-EU%20plans%20for%20AI%20v5.pdf](https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_AI%20USA-China-EU%20plans%20for%20AI%20v5.pdf). Accessed 18 December 2018.
- European Commission. 2018. "Europe's Digital Progress Report 2017". <https://ec.europa.eu/digital-single-market/en/european-digital-progress-report>. Accessed 18 December 2018.
- European Commission. 2018. "EU Member States sign up to cooperate on Artificial Intelligence". <https://ec.europa.eu/digital-single-market/en/news/eu-member-states-sign-cooperate-artificial-intelligence>. Accessed 18 December 2018.
- European Commission. 2018. "Fair Taxation of the Digital Economy". [https://ec.europa.eu/taxation\\_customs/business/company-tax/fair-taxation-digital-economy\\_en](https://ec.europa.eu/taxation_customs/business/company-tax/fair-taxation-digital-economy_en). Accessed 18 December 2018.
- European Commission. 2018. "Shaping the Digital Single Market". <https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market>. Accessed 18 December 2018.
- European Commission. 2018. "The Digital Economy and Society Index (DESI)". <https://ec.europa.eu/digital-single-market/en/desi>. Accessed 18 December 2018.
- European Parliamentary Research Service. 2017. "Developing supercomputers in Europe. Brussels".
- European Parliamentary Research Service. 2017. "Global Trends to 2035: Economy and Society". Brussels.
- Evans, Peter, and Gawer, Annabelle. 2016. "The Rise of the Platform Enterprise: A Global Survey". Center for Global Enterprise, 2016.

- Garcia Herrero, Alicia. 2018. "US-China trade war: What's in it for Europe?". <http://bruegel.org/2018/08/us-china-trade-war-whats-in-it-for-europe/>. Accessed 18 December 2018.
- Gigova, Radina. 2017. "Who Vladimir Putin thinks will rule the world". <https://edition.cnn.com/2017/09/01/world/putin-artificial-intelligence-will-rule-world/index.html>. Accessed 18 December 2018.
- Grand View Research. 2017. "Artificial Intelligence Market Analysis By Solution (Hardware, Software, Services), by Technology (Deep Learning, Machine Learning, Natural Language Processing, Machine Vision), by End-use, By Region, and Segment Forecasts, 2018 - 2025". <https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-ai-market/methodology>. Accessed 18 December 2018.
- Kleiner Perkins. 2018. "Internet Trends Report 2018". [https://www.kleinerperkins.com/files/INTERNET\\_TRENDS\\_REPORT\\_2018.pdf](https://www.kleinerperkins.com/files/INTERNET_TRENDS_REPORT_2018.pdf). Accessed 18 December 2018. S. 227.
- Körner, Kevin, Schattenberg, Marc, and Heymann, Eric. 2018. "Digital economics. How AI and robotics are changing our work and our lives". [https://www.dbresearch.com/PROD/RPS\\_EN-PROD/PROD000000000468705/Digital\\_economics%3A\\_How\\_AI\\_and\\_robotics\\_are\\_changin.pdf](https://www.dbresearch.com/PROD/RPS_EN-PROD/PROD000000000468705/Digital_economics%3A_How_AI_and_robotics_are_changin.pdf). Accessed 18 December 2018.
- Lee, Kai-Fu. 2018. *AI Superpowers: China, Silicon Valley and the New World Order*.
- Puddephatt, Andrew, Torreblanca, José Ignacio, and Prislán, Nika. "The New Great Game". [https://www.ecfr.eu/page/-/The\\_New\\_Great\\_Game\\_ECFR.pdf](https://www.ecfr.eu/page/-/The_New_Great_Game_ECFR.pdf). Accessed 18 December 2018.
- Schmidt, Eric. 2014. "Why Europe needs a digital single market". <https://www.weforum.org/agenda/2014/09/new-digital-era-europe/>. Accessed 18 December 2018.
- Scott, Mark. 2018. "Goodbye internet: How regional divides upended the world wide web". 28 January 2018, Politico. <https://www.politico.eu/article/internet-governance-facebook-google-splinternet-europe-net-neutrality-data-protection-privacy-united-states-u-s/>. Accessed 18 December 2018.
- The Economist. "Can the EU become another AI superpower?". <https://www.economist.com/business/2018/09/20/can-the-eu-become-another-ai-superpower>. Accessed 18 December 2018.
- Thompson, Nicholas. 2018. "Emmanuel Macron talks to wired about france's ai strategy", 31 March 2018. <https://www.wired.com/story/emmanuel-macron-talks-to-wired-about-frances-ai-strategy/>. Accessed 18 December 2018.7
- Trajtenberg, Manuel. 2017. "AI as the next GPT: a Political-Economy Perspective". <https://www.nber.org/papers/w24245>. Accessed 18 December 2018.
- Woetzel, Jonathan et al. 2017. "China's digital economy. A leading global force". <https://www.mckinsey.com/featured-insights/china/chinas-digital-economy-a-leading-global-force>. Accessed August 2018.

**"China's Techno-Utilitarian Experiments with Artificial Intelligence"**  
- *Dev Lewis*

**"Social Credit System in China"** - *Chris Fei Shen*

**"China's Tech Giants: Baidu, Alibaba, Tencent"** - *Hong Shen*

**"Japan's Innovation Systems at the Crossroads: Society 5.0"**  
- *René Carraz and Yuko Harayama*

**"Taking Stock of Smart Nation Development in Singapore"** - *Teck-Boon Tan*

**"Redefining Parity at Work in India"** - *Terri Chapman*

**"Dissecting the Rise and Plateau of Digital Payments in India"**  
- *Bedavyasa Mohanty*

**"Promoting Prosperity and Providing Protection: Australia's International Cyber Engagement Strategy"** - *Damien Spry*

**"Asia Pacific Contributions to International Cyber Stability"** - *Caitríona Heint*

**"Digital Transformation and Industry 4.0 in Southeast Asia"**  
- *Raja Mikael Mitra*

**"Energy Security in the Digital Age and Its Geopolitical Implications for Asia"** - *Frank Umbach*

**"Defying Gravity: Europe in the Digital Transformation"** - *Mario Voigt*

