AVI
ASIAN VISION INSTITUTE

Cambodia in Cyberspace: Anthology

Editors:
Siriwat Chhem
Phannarith Ou
Vatana Chea

Chhem, Siriwat, Phanarith Ou, and Vatana Chea
Cambodia in Cyberspace: Anthology

ISBN-13: 978-9924-9704-0-8

Published by Asian Vision Institute, 2nd Floor, Jaya Smart Building, Street 566, Boeung Kok 2, Toul Kork, Phnom Penh, Cambodia. Postal Code: 120408

AVI
ASIAN VISION INSTITUTE

For information on all Asian Vision Institute Publications
Visit our website: https://www.asianvision.org/publications-1

Acknowledgments

This anthology is the result of the hard work and dedication of the Centre for Inclusive Digital Economy (CIDE) at the Asian Vision Institute (AVI), over the last three years since its establishment. I would like to start by thanking our two co-editors Mr. Ou Phannarith and Dr. Chea Vatana, Research Fellows at AVI, for providing technical and publication expertise, respectively.

Moreover, I would like to thank H.E. Pr. Dr. Chhem Kieth Rethy, Member of the Board of Directors of AVI, for guiding our team throughout the publication process with his experience and wisdom. In addition, I would also like to express my gratitude to H.E. Dr. Sok Siphana and H.E. Dr. Chheang Vannarith, Chairman and President of AVI, respectively, for the opportunity to lead this initiative. Furthermore, I would like to thank H.E. Sous Yara, Director General of the Asian Cultural Council, for always inspiring and supporting our team.

With regards to the contents of the book, I would like to thank Dr. Nguon Kimly, Editor-in-Chief of AVI, for taking his valuable time and efforts in editing all the publications, as well as Mr. Fai Mesa and Mr. Kong Pitou for their important facilitation. I would also like to thank the core team members of CIDE that have been essential in coordinating all our publications over the last few years: Mr. Bong Chansambath, Ms. Hay Seangmey, Ms. Vong Chakriya, Ms. Sun Molika, and our amazing team of interns. A special thanks to Ms. Costa Monica for designing the book cover.

Last but not least, I would like to thank all authors that contributed towards the publications included in this anthology – without their commitment to producing high-quality policy research papers, this book would not have been possible.

Foreword

Nowadays, the expressions « digital technology » and « digital transformation » are becoming increasingly trendy buzzwords. Few truly understand the meanings of these socio-technological changes that have intensified, due to the increasing adoption of smartphones and other mobile devices. The COVID-19 pandemic significantly contributed to the acceleration of e-commerce and e-learning among other deep social transformations. The publication of this anthology on the innumerable applications of digital technology is timely. The three editors of this anthology of "Cambodia in Cyberspace", Mr. Chhem Siriwat, Mr. Ou Phannarith, and Dr. Chea Vatana, are true practitioners of cybertechnology and will share their immense experience working in the realm of cyberspace, with the readers. Mr. Chhem Siriwat brings his combined experience in the management of digital technology/AI and cyberdiplomacy. Mr. Ou Phannarith has unparalleled expertise and experience in addressing cybersecurity issues. Dr. Chea Vatana, who leads the research agenda at a technical university, has deep experience in managing scientific publications. This book contains various topics that deal with economics, finance, governance, geopolitics, and diplomacy in cyberspace. Some of the chapters address the role of digital technology in mitigating the COVID-19 pandemic. Finally, this collection of articles on cyberspace issues was completed with a section on science education (math and physics), without which there is no possible advancement of technology. Complementarily, digital technology also serves as a tool to further advance scientific development. Our three pioneers of cyberspace studies have succeeded in articulating together a vast and diverse body of knowledge that will certainly help the readers to capture the true and practical meaning of "digital technology" and "digital transformation". The rich content of this book helps in demystifying the buzzword "digital technology" and reveals the vast range of these intelligent technological applications. In sum, the "Cambodia in Cyberspace" book is an invitation to an immersive learning journey through the fascinating cyberspace, as a new realm of existence for all of us.

Chhem Kieth Rethy, MD, PhD (Edu), Phd (His)

Preface

"Cambodia in Cyberspace" is an anthology, based on a collection of publications by the Asian Vision Institute (AVI), from 2019-2022. The Centre for Inclusive Digital Economy (CIDE) spearheads AVI's policy research initiatives related to cyber and digital issues in Cambodia. CIDE was established in August 2019, by Founding Director Mr. Chhem Siriwat.

Over the last two to three years since its establishment, CIDE has grown to 40 members consisting of a Director, Deputy Director, Programme Coordinators, Advisors, Senior Research Fellows, Research Fellows, Research Associates, and Interns. Only four members are full-time operational staff, and the rest are appointed pro-bono or project-based, coming from diverse academic backgrounds (Science, Engineering, Arts, Business, etc.), as well as professional backgrounds (Public, Private, NGO, IO, etc.). With this wide range of expertise, CIDE emphasizes an interdisciplinary approach to provide sound and well-rounded policy research for Cambodia. One of CIDE's unique traits is its 100% remote or online working culture, meaning that the entire team communicates and works online, without any fixed working hours in a physical office. CIDE strives for flexible, but results-based efficiency, leveraging the use of digital applications and platforms. Ever since, CIDE has published over 50 commentaries, policy briefs, and perspectives, predominantly focusing on the digital economy and cyberspace, in the context of Cambodia. These policy papers have been disseminated and shared to a wide diversity of audiences, both locally and internationally, ranging from top policymakers, international donors, the private sector, and to the public as well. On their own, these publications provide interesting perspectives on various topics of science, technology, and innovation, in the context of the digital era. However, our team was inspired to bring all these papers together, to illustrate the big picture of Cambodia's digital economy and the role that these digital technologies play in cyberspace.

This anthology was categorized into five themes: 1) Science, Technology, and Education; 2) Governance of Cyberspace; 3) Economics in Cyberspace; 4) Geopolitics and Diplomacy in Cyberspace; and 5) COVID-19 Pandemic and Forced Digital Transformation.

Cambodia is a developing country with a young and tech-savvy population, where digital transformation is inevitably taking over all sectors - understanding cyberspace and its impact on Cambodia is of paramount importance. Above all, this book will aim to provide a local perspective on Cambodia's emerging role and integration into the fascinating, yet daunting realm of cyberspace.

Chhem Siriwat, MDTM, MA
Centre for Inclusive Digital Economy
Asian Vision Institute

Meet the Co-Editors

Mr. Chhem Siriwat is Director of the Centre for Inclusive Digital Economy at the Asian Vision Institute, Advisor to the Council for the Development of Cambodia, with the rank of Director General, and Advisor to CamTech University. He focuses on digital and cyberspace issues from policy, academic, and business perspectives. His professional experiences include leadership and advisory roles at think tanks, government agencies, science and technology universities, commercial banks, and tech startups. He has a combined academic background in science, arts, and business, specializing in Digital Technology Management, Artificial Intelligence, Diplomacy, Chemistry, Physics, and Environmental Science. He has published numerous papers and is regularly invited as a guest speaker at international conferences, on the topic of Digital Economy and Cyberdiplomacy.

Mr. Ou Phannarith is the Director of Information and Communications Technology (ICT) Security of the Ministry of Post and Telecommunications (MPTC) of Cambodia. He is the former Head of the National Cambodia Computer Emergency Response Team (CamCERT). He has been involved in the development of Cybersecurity, ICTs, and related regulations in Cambodia for the last 15 years. Mr. Phannarith has been the research fellow at the Center for Inclusive Digital Economy, Asian Vision Institute (AVI), the Professor at Royal University of Law and Economics (RULE) specializing in Cybersecurity and Senior advisor to Cambodia Digital Tech Association (CDTA). He is the founder of the first cybersecurity awareness website (www.secudemy.com), ISAC-Cambodia (Cybersecurity), Cyber Studies Network (CSN), founder of Cyber Youth Cambodia, and Chairman of Cloud Security Alliance (CSA) Cambodia Chapter.

Dr. Chea Vatana is Director of Research and Innovation and of the Center for Professional Education and Training, Cambodia University of Technology and Science (CamTech). Prior to joining CamTech, he worked as a researcher at a policy think-tank based in Phnom Penh. He was also a doctoral fellow at the Center for the Study of International Politics (CeSPI) and Roma Tre University, Rome, Italy. Dr. Vatana holds a master and a doctoral degree in Demography from Chulalongkorn University. Apart from serving as a Secretary General of the Comparative Education Society of Cambodia, he is also a member of the International Union for the Scientific Study of Population (IUSSP). His research interests include population projection, migration and development, human capital development, and economics of household. Dr. Vatana has authored and co-authored more than a dozen peer-reviewed scientific articles including book chapters and journals in ISI and SCOPUS databases.

Content

Section 1: Science, Technology, and Education

Section 2. Governance of Cyberspace

Section 3: Economics in Cyberspace

Section 4: Geopolitics and Diplomacy in Cyberspace

Section 5: COVID-19 Pandemic and Forced Digital Transformation

AVI COMMENTARY

ISSUE 2020, No. 08

Cambodia | 31st March 2020

The Birth of Modern Science in Cambodia

CHHEM Rethy[a], MD, PhD (Edu), PhD (His)

The rise of Angkor civilisation from 9th to the 13th century CE was the result of divine inspiration but the remarkable building of Angkor's temples, infrastructure, university and health systems was made possible only because of the strong scientific culture that prevailed at the royal court. Kings were advised by their teachers and surrounded themselves by a highly educated elite made of mathematicians, engineers, and astronomers.

The Angkor "scientific" enlightenment predated similar phenomenon observed in Renaissance Italy during the 16th century CE. Respect for "science" was observed before the term "scientist" was first coined in 1833 by the English polymath, philosopher and historian of science William Whewell.

Turning to modern times, a nascent science emerged briefly in the post-independence period when the first modern universities were founded with a view to educate and train young Cambodians to participate in the development of the nation. Math, physic, chemistry, engineering teaching flourished. Attempts to use nuclear technology to boost agriculture was taken with the technical assistance of the International Atomic Energy Agency in the mid 60's, that sadly was prematurely interrupted by war.

In more recent years, leading think tanks such as the Cambodia Development Resource Institute ensured that evidence was used to support the value of science and technology in decisions affecting the economic and social development of Cambodia. Policies on industrial

[a] **CHHEM Rethy** is an Honorary Senior Fellow at the Cambodia Development Resource Institute (CDRI).

development, STEM education, vocational training, and Science and Technology have been adopted.

Coordinating and implementing policies across these areas has finally been achieved. The Ministry of Industry, Science, Technology and Innovation, a national institution was established to design an inspiring national ecosystem for science and technology. The new ministry is expected to coordinate strategies and programmes that provide policy guidance, legal frameworks and proper resources for Science, Technology and Innovation (STI) to flourish. The era of "orphan" science is over.

Hundreds of Cambodian scientists, highly educated in reputable universities locally and abroad can finally operate in a cohesive ecosystem driven by national needs in view of economic and social development. The nascent clusters of scientific research are currently dispersed in a few reputable local universities without interaction with each other because of the lack of a clear national science agenda. A few government funding programmes had been recently launched in order to help young scientists and entrepreneurs to get seed money to explore their innovative ideas.

Coincidentally, this development occurs alongside Cambodia's efforts to accelerate the digital transformation of its government and economy in an effort to reach a fully developed country status by the year 2050. This national drive calls for an overhaul of the mindset in terms of learning new knowledge whether it happens inside or outside the school system. AI algorithms, big data and industry 4.0 processes will bring revolutionary changes in the way we learn. Deep cultural changes that lead to the "scientification" of Cambodian citizens are necessary; the appearance of scarecrows in the Cambodian countryside will not tame the COVID-19 pandemic, but science will.

Schools and universities are now all closed to protect students and staff from the threat of the pandemic. Many businesses will follow. Students and staff will be forced to work from home. COVID-19 has become the most disruptive reformer of the education system and of the organisation of work. Online learning and telework are now the top priorities for government and the private sectors to address. Proper digital infrastructures and its legal and policy frameworks are yet to be determined. Finally, if science and technology are to provide the impetus for national development, all policies, related to science or not, have to be founded on strong scientific evidence, established by scientists in order to inform policymakers.

The launch of the Ministry of Industry, Science, Technology, and Innovation in the midst of a pandemic brings a light of hope to Cambodia, not because local science and technology can provide solutions to the current situation – but it will help build STI capacity for Cambodia to better prepare and respond to future disease outbreaks. Above all, this new STI capacity will allow Cambodia to rebuild its economy and social coherence in the post-COVID-19 era.

As Galileo observed long before our time: "If you could see the earth illuminated when you were in a place as dark as night, it would look to you more splendid than the moon".

The views expressed are the author's own and do not reflect the views of the Asian Vision Institute.

AVI COMMENTARY

ISSUE 2020, No. 32

Cambodia | 12th October 2021

Importance of Mathematics Education for Cambodia's Industries

HUL Seingheng[a], PhD
CHHEM Siriwat[b], Master in Digital Technology Management

Due to the conceptual complexity of mathematics, the universal agreement on its definition is highly-debated. Simply put, it is commonly understood that mathematics is about numbers. Going deeper, mathematics is a subject of deductive reasoning and logic, concerning a fundamental abstract object. In the context of Cambodia with its high development potential, mathematics education will be crucial for equipping its young population to drive its national industries.

Mathematics and Industrial Growth

Mathematics is the fundamental pillar of science and technology. The book entitled "Mathematik Motor der Wirtschaft" emphasises that "without mathematics nothing is possible. It is like walking in the dark." The ideal of mathematics through the development of science and time remains unchanged from its birth in 3000 BCE recorded in Egypt, to the history of modern society. The rise of many great civilisations was the result of richness in mathematical sciences. Dating back to 683 CE, engineers of the Khmer Empire used the Zero concept in building its majestic Angkor Complex.

Placing a high value on mathematics is the way of enlightening development and sustainability in an innovative technological strategy. In the modern society of industry-driven development, mathematics plays a crucial role as a logically coherent framework and language for analysis,

[a] **HUL Seingheng** is a Senior Research Fellow at the Centre for Inclusive Digital Economy (CIDE) of the Asian Vision Institute (AVI). Concurrently, he is the Director General of the General Department of Science, Technology, and Innovation (GDSTI) at the Ministry of Industry, Science, Technology, and Innovation (MISTI).
[b] **CHHEM Siriwat** is Director of CIDE, AVI.

simulation, optimisation, computation, and process control. There are endless emerging technology applications that require mathematics such as Artificial Intelligence, Cybersecurity, Blockchain, FinTech, etc.

Mathematics is ingrained in nature, taking shape of snail shells, spider webs, beehives, and other complex but beautiful natural architectures. Incontestably, industrial production and efficiency have increased significantly in these last few decades and mathematical tools will be the core of data science in this revolution. Mathematical concepts combined with Information Technology in statistics, scientific computing, system technology, automation and control, image analysis, data analysis, optimisation, simulation and modelling, and data visualisation are significantly applied in the development of industry and business enterprises. Thus, this industrial development driven by innovation will rely heavily on applied mathematics. The essence of mathematics has been consistently acknowledged in human history. The sustainability of our society, environment, and economy would not be secured without the incorporation of mathematics into our future development strategies. To promote relevant mathematical applications to end users, the basic research of mathematics must be institutionalised. Industrial mathematics plays an inevitable role in strengthening supply chains and boosting competition. Industry 4.0 is challenging the current status of productive processes and decision-making of many companies and industries. The augmented era of Industry 4.0 will strive based on significant contributions from mathematicians and corresponding policies for multifaceted training of mathematics, to achieve sustainable growth of production and consumption.

Increasingly, complex problems in businesses and industries will require mathematical expertise. Big data analysis would not be possible without proper integration of computational mathematics in analysis models. Industry 4.0 requires the knowledge of mathematical analysis of data to utilise data and information for decision-making to return the highest profit and efficiency. Consequently, the strong linkage between industrial manufacturers and mathematicians drives sustainable business growth.

The value of mathematicians and mathematical education must be leveraged within a supportive ecosystem. Encouraging and inspiring the young generation of Cambodians to become interested in mathematics through formal and informal education is key to Cambodia's future industries. Thus, strong communication channels between academia and industry are essential, so that academic learning outcomes cater to national industry needs. Mathematical thinking and reasoning must be fostered as a fundamental pillar of education. For instance, mathematics teachers in school should involve more engineering problems encountered in real-life industry settings such as signal processing, computer graphics, risk management, system reliability, software testing and verification, database systems, and production line optimisation, with emphasis on problem solving – not just pure theory.

Harnessing Mathematics to Develop Cambodia

Mathematics on a simpler level, still drives the most important sectors of Cambodia, including tourism, garment, agriculture, and construction. At the next level of economic growth, Cambodia needs to move into the industrial sector, where mathematics is already essential in supporting our existing industries but will be even more crucial as we move towards automation and data exchange in Industry 4.0 and beyond.

In Cambodia, there is a common local stigma that an academic path in mathematics will not generate much income and only lead to one profession: a mathematics teacher. This peculiar misconception has pushed countless potential students away from studying mathematics over the years. This mentality must change now – studying mathematics will indeed provide an individual with sound logic and mental sharpness that would be beneficial in whichever career they may choose, even outside the realm of mathematics. Scholarships should be provided for top mathematics students, more national mathematics competitions should be organised, and mathematics clubs should be established in all school – in order to promote interest in mathematics and its significance for Cambodia's development.

The era of mathematical capitalism has come. The importance of mathematics for the industry has not yet been fully realised in our current context. Yet, it has been observed as crucial for the development scheme of all societies in history. The digital era calls for mathematical skills and expertise, more than ever before. Cambodia will need mathematics to drive our industries, increase our global competitiveness, and even protect our nation. Although we may not be able to exactly pinpoint the fields of expertise we should focus on to further develop Cambodia; starting with a strong foundation in mathematics from a young age will provide the next generation with strong logical reasoning and problem-solving skills, to drive Cambodia's future industries.

The views expressed are the author's own and do not reflect the views of the Asian Vision Institute.

AVI COMMENTARY

ISSUE 2021, No. 24

Cambodia | 28th October 2021

The Power of Physics for Cambodia: Beyond the Classroom

KUOK Fidero[a], PhD
CHHEM Siriwat[b], Master in Digital Technology Management

There is a common misconception among students and parents in Cambodia that all university graduates in that major in physics eventually become teachers of that discipline. This paper aims to debunk this myth and show that physics graduates are in high demand in a fast-developing country like Cambodia. Various studies have shown that physicists are well equipped with critical skills for problem-solving using complex data sets. They are familiar with data collection, analysis, and processing. With their strong background in physics, they are well trained in modeling and computer programming that are valuable technical tools for all socioeconomic sectors, from engineering to finance and from medicine to architecture. As such, physicists can turn countless ideas into impactful commercial and social projects. Physicists are also well prepared to cope with the emergence of new digital technologies because of their logical minds and powerful reasoning skills.

In 1952, immediately after the death of Chaim Weizmann, Israel's first president, Albert Einstein, a Nobel Prize winner for discovering the photoelectric effect and famous for the special and general theory of relativity – one of the world's greatest physicists, was offered to be the President of Israel. It comes as no surprise that Einstein is globally well-known for his intellectual achievement in physics, and people believed that he would be a great leader. Why would physics be essential for policymakers? Many, if not all national leaders' momentous decisions are related to cutting-edge technologies, for instance: reliable, affordable, secure, and clean energy, cybersecurity, CubeSats – i.e. mini satellites, to name a few. Then, the knowledge

[a] **KUOK Fidero** is Director General of the National Institute of Science, Technology and Innovation at the Ministry of Industry, Science, Technology, and innovation.
[b] **CHHEM Siriwat** is Director of the Centre for Inclusive Digital Economy (CIDE) at the Asian Vision Institute (AVI).

of physics would inform crucial decision-making processes. In the current COVID-19 pandemic, physics plays ubiquitous roles from generation and aerosolisation of virus-laden respiratory droplets to airborne dispersion and deposition on solid surface. Physics has also reinforced sanitary measures in the form of face masks, hand washing, social distancing, and speeding up the design and production of vaccines.

Physics for Health

The two main applications of medical physics in healthcare include medical imaging/radiation treatment and healthcare informatics/computational physics. The most well-known applications of physics to medicine are the use of equipment to detect diseases, such as magnetic resonance imaging (MRI), computerised tomography (CT), nuclear medicine, and positron emission tomography (PET) scanning. Others are the different types of radiotherapy machines used in the treatment of cancer. Qualified medical physics experts are required to utilize radiation safely and effectively for healthcare purposes. Computational physics is used to manage medical data, bioinformatics, and telemedicine. During this ongoing pandemic, physics instruments such as cryo-EM (X-Rays crystallography) enabled Chinese scientists to accelerate the identification of the corresponding viral spike protein. The molecule was then quickly shared through an open-source platform to all scientists across the globe, paving the way for the design and production of the mRNA vaccine, the first of its kind in the history of vaccines.

Physics for Finance

The financial sector needs experts who understand math and quantitative skills, while physics graduates are comfortable working with large data sets. Furthermore, financial securities investment requires specialised expertise from physicists who understand complex mathematical models to generate profits and decrease risks. Another field where physics concepts are essential is econophysics, an emerging academic discipline that capitalises on the unique role of physicists in solving economic problems. Their research focuses on new conceptual approaches deriving from physical science. Finally, the advent of big data opens even more opportunities for physicists who can deal with complex systems. As such, physicists are highly desired for business intelligence, quantitative finance, and trading stocks.

In other words, physicists are equipped with scientific rigour and trained to deal with systems and their components, all valued skills for creating and analysing financial models. Although the job market and employers in Cambodia might not yet fully realise the potential for physics graduates to excel in the field of finance, companies that take the first step in investing and developing this scarce pool of experts to work in finance will benefit from their unique transferable skills. Moreover, providing new career paths and job opportunities for physics graduates outside the field of physics will highlight their true value in the job market, aside from the conventional options of becoming a physics teacher, researcher, or lab technician. From an optimistic view, this shift in mindset might rebrand physics as a more appealing academic path to follow in Cambodia.

Physics for Smart Factories in IR 4.0

Albert Einstein once said, "A theory should be as simple as possible, but no simpler". Indeed, the word *theory*, e.g., physics, has sounded impractical for practitioners despite its usefulness for predicting natural events or phenomena yet to be observed. The question of how a manager of a manufacturing company could undoubtedly increase productivity at low costs and generate higher revenue with attractive customer service remains difficult. Understanding physics, which objectively explains the solution for a particular problem, could be lifesaving for such managers. How does physics help us to understand factory management? Just about 20 years ago, Moog Inc., a specialised designer and supplier of aircraft and missile components, faced a significant problem of meeting customer deadlines, while losing market competitiveness. George Cameron, the materials manager who had attended the Factory Physics Seminar, utilized scientific tools to understand the underlying manufacturing issue and implemented improvements accordingly. Inspired by physics, the team decided to rearrange buffers and reduce waste in the fabrication areas, which solved their inefficiency problems. Today, physics plays a fundamental role for the smart industry, including agile value networks, advanced manufacturing processes and services, the synergy of man and machine, and interoperable digital manufacturing platforms.

In conclusion, physics is not just about obscure theories – there are endless applications outside the classroom. The aim of this paper was to raise awareness on the importance of physics to inspire more students in Cambodia to pursue this major as part of STEM education. Without physics, industrial development is not possible. The famous expression goes: "No physics, no life", as we all live in a physical world and must understand how it works.

The views expressed are the author's own and do not reflect the views of the Asian Vision Institute.

AVI POLICY BRIEF

ISSUE 2020, No. 19

Cambodia | 26th November 2020

Pedagogy of Online Learning in Cambodia: Revisiting Ideas of Connection, Engagement, Attendance, and Assessment

CHEA Sin[a], PhD
KHIENG Sothy[b], PhD
LENG Phirom[c], PhD
WATER Tineke[d], PhD

Executive Summary

- The closure of physical classrooms across higher education institutions (HEIs) due to the COVID-19 pandemic, the rapid digital transformation across the world, and the resultant rise of e-learning have brought critical questions regarding the pedagogy of learning and teaching, particularly on issues of attendance, engagement and assessment.
- One of the positive changes favoured by COVID-19 is how education will be delivered in the future. In this respect, blended learning seems to be a viable methodology. Thus, HEIs and policymakers need to consider carefully how they will implement this to improve the learning experience of students. Meanwhile, more policies and strategies should be formulated to support these changes, including educators and students.
- Policy options for stakeholders in the higher education subsector:
  - HEIs should address barriers to e-learning by developing appropriate digital infrastructure and resources, including e-learning studios, smart classrooms and high-speed internet connectivity. Educators need to be trained and re-trained on

[a] **CHEA Sin** is Dean of the Faculty of Pharmacy at the University of Puthisastra.
[b] **KHIENG Sothy** is Vice President in charge of Research and Administration of the Kirirom Institute of Technology (KIT) and an Advisor to the Centre for Inclusive Digital Economy (CIDE) at the Asian Vision Institute (AVI).
[c] **LENG Phirom** is President of KIT and an Advisor to CIDE, AVI.
[d] **WATER Tineke** is Associate Professor of Research at the University of Puthisastra.

digital literacy and blended learning approaches while developing and making accessible resources for lecturers on how to develop e-learning materials.

- HEIs should consider redefining ways of measuring attendance and undertaking assessments to reflect the changing nature of educational delivery, including in-person, online and blended approaches.
- The Ministry of Education, Youth and Sport (MoEYS), the private sector and civil society organisations need to build partnerships to invest more concretely in digital infrastructure (4G and 5G networks, smart-classroom, e-learning applications, e-library), training programmes, and other resources to support HEIs, HEI leaders, educators and students in their efforts to adapt and adopt digital education.
- Higher education regulators and policymakers should also revisit the policy and guidelines for attendance and assessment to ensure they are linked with the digital transformation of higher education.

សេចក្តីសង្ខេបអត្ថបទ

- ការបិទថ្នាក់រៀននៅតាមបណ្តាគ្រឹះស្ថានឧត្តមសិក្សាដោយសារជម្ងឺរាតត្បាតសកលកូវីដ-១៩ និងការផ្លាស់ប្តូរឌីជីថលយ៉ាងឆាប់រហ័សនៅទូទាំងពិភពលោក ក៏ដូចជាការកើនឡើងនៃការសិក្សាតាមប្រព័ន្ធអនឡាញ បានចោទជាបញ្ហាចំពោះគុកោសល្យនៃការរៀន និងការបង្រៀន ជាពិសេសទៅលើបញ្ហាវត្តមាន ការចូលរួម និងការវាយតម្លៃការសិក្សារបស់សិស្ស។
- ជម្ងឺកូវីដ-១៩បាននាំមកនូវការផ្លាស់ប្តូរជាវិជ្ជមានមួយទៅលើរបៀបនៃការបង្រៀននាពេលអនាគត។ ក្នុងន័យនេះ វិធីសាស្ត្របង្រៀនរួមបញ្ចូលគ្នាហាក់ក្លាយជាជម្រើសថ្មីមួយ។ អាស្រ័យហេតុនេះ គ្រឹះស្ថានឧត្តមសិក្សាគ្រប់កំរិត និងអ្នកតាក់តែងគោលនយោបាយត្រូវពិចារណាឲ្យបានល្អិតល្អន់អំពីរបៀបនៃការអនុវត្តវីធីសាស្ត្របង្រៀនថ្មីនេះ ដើម្បីធ្វើឲ្យបទពិសោធន៍នៃការសិក្សារបស់សិស្សកាន់តែមានភាពប្រសើរឡើង។ ទន្ទឹមគ្នានេះដែរ គោលនយោបាយនិងយុទ្ធសាស្ត្រសម្រាប់គ្រូនិងសិស្សគួរត្រូវបានបង្កើតបន្ថែមទៀត ដើម្បីគាំទ្រការផ្លាស់ប្តូរទាំងនេះ។
- ជម្រើសគោលនយោបាយសម្រាប់បុគ្គលពាក់ព័ន្ធនានានៅក្នុងអនុវិស័យឧត្តមសិក្សា៖
  - គ្រឹះស្ថានឧត្តមសិក្សាគួរដោះស្រាយឧបសគ្គនៃការសិក្សាតាមប្រព័ន្ធអនឡាញដោយការអភិវឌ្ឍហេដ្ឋារចនាសម្ព័ន្ធនិងធនធានឌីជីថល ដូចជាបន្ទប់រៀនបំពាក់ប្រព័ន្ធអេឡិចត្រូនិច ថ្នាក់រៀនឆ្លាតវៃ និងមានភ្ជាប់អ៊ីនធឺណែតល្បឿនលឿន ។ គ្រូបង្រៀនត្រូវទទួលបានការបណ្តុះបណ្តាលអក្ខរកម្មឌីជីថល និងវិធីសាស្ត្របង្រៀនរួមបញ្ចូលគ្នា ស្របពេលជាមួយនឹងការ

អភិវឌ្ឍនិងការបង្កើតធនធាន ដែលគ្រូអាចយកទៅប្រើដើម្បីរៀបចំឯកសារមេរៀនតាមប្រព័ន្ធអនឡាញ។

- គ្រឹះស្ថានឧត្តមសិក្សាគួរបង្កើតវិធីសាស្ត្រថ្មីក្នុងការធ្វើសម្រង់វត្តមាន និងការវាយតម្លៃការសិក្សារបស់សិស្ស ដើម្បីអាចឆ្លុះបញ្ចាំងការអប់រំតាមរបៀបថ្មីនេះ ដែលរួមមាន វិធីសាស្ត្របង្រៀនដោយផ្ទាល់ តាមអនឡាញ និងវិធីសាស្ត្ររួមបញ្ចូលគ្នា។
- ក្រសួងអប់រំ យុវជន និងកីឡា វិស័យឯកជន និងអង្គការសង្គមស៊ីវិលត្រូវកសាងភាពជាដៃគូដើម្បីវិនិយោគហេដ្ឋារចនាសម្ព័ន្ធឌីជីថលឲ្យបានរឹងមាំ (បណ្តាញ 4G និង 5G ថ្នាក់រៀនឆ្លាតវៃ កម្មវិធីរៀនអនឡាញ បណ្ណាល័យអេឡិចត្រូនិច) កម្មវិធីបណ្តុះបណ្តាល និងធនធានផ្សេងទៀត ដើម្បីគាំទ្រគ្រឹះស្ថានឧត្តមសិក្សា ថ្នាក់ដឹកនាំគ្រឹះស្ថានឧត្តមសិក្សា គ្រូបង្រៀន និងសិស្ស ដើម្បីឲ្យពួកគេសម្របខ្លួនទៅនឹងការអប់រំតាមបែបឌីជីថល។
- អ្នកតាក់តែងបទប្បញ្ញត្តិនិងគោលនយោបាយការអប់រំថ្នាក់ឧត្តមសិក្សា គួរពិនិត្យមើលឡើងវិញនូវវិធីសាស្ត្រសម្រង់វត្តមាន និងការវាយតម្លៃការសិក្សា ដើម្បីធានាថា វិធីសាស្ត្រទាំងនេះផ្សារភ្ជាប់ទៅនឹងការផ្លាស់ប្តូរឌីជីថលនៃការអប់រំថ្នាក់ឧត្តមសិក្សា។

Introduction

In early March 2020, the initial outbreak of the COVID-19 pandemic in Cambodia led the Ministry of Education, Youth and Sport (MoEYS) to order for physical closure of schools and higher education institutions (HEIs) throughout the country, which had to rapidly respond to delivering education online or risk a permanent shutdown. Although restrictions began to ease in late October, the "3rd November Incident," which refers to the event when officials of the Royal Government of Cambodia were forced to self-quarantine due to their direct or indirect contacts with Hungarian Foreign Minister Peter Szijjarto who visited Cambodia and later tested positive for COVID-19 shortly after his arrival in Thailand, forced schools nationwide into another two-week shutdown. This series of closure and reopening of schools across Cambodia have presented huge challenges for HEIs in preparing staff and students, many of whom had little prior digital exposure or experience, on how to use online platforms. Five months later, most HEIs have adapted to online platforms such as Google Classroom, Google Meets, Zoom or Moodle and the rhythm of delivering online learning has been established. However, with the closure of HEIs stretching into the future, and e-learning is now seen as an important complement to learning even when HEIs return to face-to-face classrooms, it is timely and necessary to think about the pedagogy of e-learning.

Pedagogies of online learning are the same as and yet also different from those of in-person teaching. Online learning is not just a matter of transposing classroom lectures onto an online platform, many of which have been based on didactic models of learning. Rather they involve new ways of thinking around the challenges of engaging students, assessing learning, and ensuring attendance in online environments, and providing a connection to learning that considers the social environment of learning. Although most HEIs are set to start reopening in Cambodia, the shift to blended learning with a mix of face-to-face and online is here to stay. It is the online component of learning that we examine in this article.

As the focus has shifted towards mastering online platforms, lecturers have turned their attention to the 'how' dimensions of online learning and pedagogy, such as how to 'engage' students in online learning and how this fits with new ideas of what 'attendance' is in online environments (though this needs to fit with Ministry of Health/MoEYS COVID-19 safety requirements); and how assessment is linked to student engagement and learning outcomes which could influence how assessments could be undertaken in the future.

Based on our analysis of data drawn from primary and secondary sources, we argue that engaging students, promoting attendance as active participation, and providing assessments to promote critical thinking and application of learning rather than knowledge recall will shape highly skilled graduates of the future. Our research also indicates that in an online environment, connection, engagement, attendance, and assessment cannot be discussed in silos; rather each plays a part in complementing the other and provides a way forward to thinking about new pedagogies of learning in Cambodia.

Revisiting "Attendance," "Learning," and "Assessment"

The Merriam-Webster Dictionary (n.d.) defines attendance as "the act of being present at a place" or "a record of how often a person goes to classes, meetings, etc." This definition, often associated with 'marking' attendance, is described as waiting to act upon the directions or decisions of a superior (such as the lecturer) which does not foster the independence or critical thinking that HEIs expect of graduates. More recently, attendance, however, has been reframed as not just being physically present but as active 'participation' in the activities of learning or 'attention-based attendance,' which is seen as applying your mind to something and investing effort in it (Belshaw 2011).

Attention-based attendance means that students do not have to be physically present to learn. In contrast, it is their engagement and efforts that count towards having attended to something. This means that traditional methods of 'taking attendance' to meet the required number of hours for a course is more a reflection of procedural expectations than measuring or understanding how students are learning in a course. Definitions of attendance also include ideas of a community such as a class or community of learners, where attendance is based on community 'interaction,' including webinars or podcasts, or within the community itself, where members moderate and participate in online discussions (Belshaw 2011). This shifts away from viewing attendance as a single individual who is present in a physical location to emphasis on knowledge-sharing interactions between a community of learners.

Belshaw (2011) posits that learning institutions need to move towards definitions of attendance as 'attention' and 'engagement' rather than students just being physically present at a virtual or in-person class. For many organisations, including the University of Puthisastra (UP) and Kirirom Institute of Technology (KIT), active student 'engagement' in learning is a highly essential goal in supporting high-quality graduates who will be the future leaders in their respective fields, locally and internationally. Graduates of the future are those who engage with their profession and workplace rather than just showing up for work.

Meanwhile, Stauffer (2020) argues that graduates in the 21st century need both hard and soft skills. In particular, learning skills (critical thinking, creativity, collaboration, and communication), literacy skills (information literacy, media literacy, and technology literacy), and life skills (flexibility, leadership, initiative, productivity, and social skills) are seen as vital in developing high-quality graduates who will contribute productively to society and the economy. Teaching hard and soft skills should be included regardless of whether learning is in the classroom or online. Therefore, promoting ways of learning that foster these skills are essential for preparing the current and future workforce.

One of the challenges of any learning is how HEIs connect students with learning. This spans from the physical resources students and staff need to connect to learning such as physical space, learning materials, and technology, to how students are connected to learning and whether this is measured as physical attendance or active engagement in learning. Belshaw (2011) suggests that organisations trying to re-examine how they think of attendance should ask, "what type of attention and engagement is being generated and how are students (and society) benefitting?" Although these questions require a methodological shift by HEIs, there are also practical considerations that must be addressed for students or organisations to successfully connect students with online learning.

In Cambodia, the first barrier to engaging students in e-learning is the lack of digital infrastructure or resources such as laptops or computers. Students instead are using their smartphones to access classes, information, write, submit assignments, and undertake exams. This problem is compounded by unstable internet connections or lack of 3G/4G data. KIT has addressed this issue early on by providing students with laptops and prepaid Internet access. However, not all Cambodian HEIs can afford to do this. Online classrooms are no different from physical classrooms in that they require resourcing and accessibility for students. These resources also include technological support such as training on the utilisation of online platforms and learning sites. Removing the barriers to e-learning requires an institutional shift in thinking and for many (students, lecturers, and support staff) to become adept at using technology.

Once students and lecturers are comfortable with the e-learning platforms, the next step is to think about how online learning happens and whether it is based on attendance in a synchronous classroom space as evidence of learning or attendance as students and staff actively engaged in the process of learning. HEIs-implemented online learning currently faces decisions around whether to offer synchronous, asynchronous or a mixture of the two for learning. Traditional synchronous environments do offer the advantage of providing a learning environment, where students engage in active discussion, get immediate feedback, and have a chance to build positive social interactions that prepare them for real-life environments later on in their career. Lecturers can also assess if students understand the topic, their strengths, and where student learning may need extra support.

Although in Cambodia teaching has traditionally relied on synchronous models of classroom teaching, there has been an increasing call for asynchronous forms of learning and teaching. In a recent survey of students at UP, students described the benefits of asynchronous modes of learning and teaching as addressing their issues around internet connectivity and challenges of having to attend classes in 'real-time' and subsequently being penalised if they were not able to attend. KIT deals with similar issues, as on average, students' attendance in online learning has been not as high as in-person learning. In addition to classroom learning, KIT students had to devote another half-day (five days/week) to attend their internship. In this regard, one may argue that asynchronous learning and teaching would allow students the flexibility to learn when and where work best for them, which is crucial as many students have difficulty finding a quiet location to join their classes or have to deal with personal responsibilities such as child care or family business. Asynchronous teaching also allows students to review materials more than once, which they perceive as encouraging them to become independent learners. However, a move to asynchronous teaching has challenged HEIs to find other ways to measure students' connection with learning other than physical attendance.

Reframing attendance as 'attention' or 'engagement' can provide an alternative to measuring attendance as a physical presence in a class. Students' attention or engagement also shifts the focus from didactic forms of teaching that view the lecturer as the repository of knowledge and the student as an empty vessel to be filled with knowledge to progressive educational models in which students engage and drive much of their learning. In Cambodia, students have felt comfortable with didactic teaching, being taught content, and then assessed by their ability to recall and recite "the knowledge" (primarily through MCQ assessment) and direct this back to the lecturer. This method privileges rote learning rather than critical thinking, problem-solving, and independent learning. Therefore, changing from didactic models of teaching is challenging regardless of whether this is online or in a physical classroom. However, one of the positive experiences to come out of the rapid move to online learning is that UP students reported they felt more confident in using the internet to find knowledge from multiple sources (as an adjunct to classes) and in turn felt more responsible for their learning. Similarly, KIT students gradually improved their time management skills and became more responsible for their learning and internship.

There have been strategies to promote effective e-learning that have worked. Firstly, focusing on students as a community of learners and part of a learning team has not only been successful in engaging students but also creating opportunities for social connection and cross-learning. Even before COVID-19, one of the major determinants of learning is the quality of connection and communication between lecturers and students. If students feel acknowledged, valued, and included they are much more likely to be successful in their academic achievements and in developing soft skills essential for future employment.

Creating online discussion forums, reinforcing the value of the contribution, and creating a sense of a class community are some of the strategies that can foster a sense of community. Students also describe the importance of regular contact with lecturers, whether this is synchronous or asynchronous, and that lecturers respond promptly to any questions or issues raised by the student. In addition to in-class interaction, KIT's adoption of the residential college model has promoted student-faculty engagements in other extracurricular activities and outside the classroom schedules. This underlines the significance of student-lecturer relationship and value of human connection – part of the core foundation which has sustained and maintained their active engagement in online learning, especially during the COVID-19 pandemic.

Problem/case/narrative-based learning is a form of progressive pedagogies that move the classroom away from didactic methods of teaching to modes of teaching that will foster critical thinking, lifelong learning, and engagement. Focusing on real-life examples connects students to their future profession and fosters ways of navigating knowledge in a way that provides building blocks of knowledge for the profession as well as skills that will help them become lifelong learners. At UP, learning is underpinned by evidence-based practice approaches and frameworks where students are encouraged to learn how to ask questions (and how and where to look for questions in everything), how to find evidence to answer these practice questions, and how to synthesise this knowledge before making any conclusion.

Likewise, KIT has adopted a problem-based learning approach, in which students spend their morning learning the concepts and their afternoon applying their in-class theoretical understanding to address real-world problems through the internship programmes. These internship programmes are designed in the forms of “virtual companies,” and over a span of four years at KIT students have been engaged in different capacities and different projects related to the latest trends in the technological and tourism industry. Not only does this support learning skills but also provides students with the vital skills needed to keep up with the rapid knowledge generation and changes in their profession. By engaging in real-life case/problem-based learning activities, students will develop initiative, long-life learning, and skills in research, critical thinking, communication, creativity, information, and media literacy.

Assessing students' learning then also needs a shift from knowledge recall to understanding and application of knowledge. Assessments that help develop building blocks of learning that are progressive and incremental and that assess different types of learning styles and understanding are important in supporting student learning. Project-based learning helps students develop group work skills (essential in future work environments) and foster creative and problem-based learning. For students to gain lifelong learning and develop attributes that add value in the workplace, assessments should be authentic and involve meta-approaches. Other activities that help shape graduates’ attributes beyond the classroom include extra-curricular activities, such as university clubs, involvement in sport and volunteering in the community – all of which are highly valued and promoted by both UP and KIT.

Policy options

As blended learning that promotes flexibility and independent learning will be the future methodology for learning and teaching in the post-COVID-19 era, HEIs and policymakers need careful consideration in how they will implement this to improve the learning experience of their students. Below are some policy options for stakeholders in the higher education subsector:

- HEIs should address the barrier to e-learning by developing appropriate digital infrastructure or resources including e-learning studio, smart classrooms and high-speed internet connectivity. Educators must be trained and re-trained on digital literacy and blended learning pedagogy while developing and making accessible manuals for lecturers on how to develop e-learning materials.

- HEIs need to critically examine whether current forms of teaching and learning, and whether current practices of keeping attendance and assessing learning will support the hard and soft skills needed for 21st-century graduates. Therefore, HEIs need to help connect students with more satisfying learning environments, a solid grounding for their future contributions to their profession and Cambodia. HEIs should consider redefining and measuring attendance and assessment to reflect the changing nature of delivery which may shift completely to an online or blended mode of online and in-person.
    - Attendance should be reframed as active engagement;
    - Learning should be considered as exploration and thinking; and
    - Assessment should be more about measuring understanding and critical thinking rather than knowledge recall.
- MoEYS, the private sector and civil society organisations need to build partnerships as a form of public-private partnership to invest more concretely in digital infrastructure (4G and 5G network, smart-classroom, e-learning applications, e-library), training programmes, and other resources to support HEIs, HEIs leaders, educators and students to adapt and adopt digital education.[a]
- Higher education regulators and policymakers should also revisit the policy and guideline of attendance and assessment to be on par with the digital transformation of higher education.

The opinions expressed are the author's own and do not reflect the views of the Asian Vision Institute.

[a] Two major recent initiatives are examples of partnership for supporting educational digital infrastructure. One is the collaboration among the MOEYS, the Open Institute and Smart Axiata in the project "Smart 1,000 Grade 12 Video Collection" through Smart Axiata's 1 Million USD COVID-19 Relief Fund. The second example is the 2020-2023 multi-stakeholder partnership between MOEYS, the Ministry of Posts and Telecommunications, development partners and the private sector to provide internet access to 3,000 public schools to support digital education.

References

Belshaw, Douglas A. J. 2012. “What Is ‘Digital Literacy’? A Pragmatic Investigation.” PhD Diss., Durham University. Durham e-Theses.

Merriam-Webster Dictionary. n.d. “Attendance.” *Merriam-Webster Dictionary*. Accessed on November 18, 2020. https://www.merriam-webster.com/dictionary/attendance.

Stauffer, Bri. 2020. “What Are 21st Century Skills?” *Applied Educational Systems*. Accessed on November 18, 2020. https://www.aeseducation.com/blog/topic/21st-century-skills.

AVI POLICY BRIEF

ISSUE 2021, No. 06

Cambodia | 19th May 2021

Massive Open Online Courses (MOOCSs) for Supporting 'Free of Charge' Professional Development and Digital Literacy of Cambodian Civil Servants

CORRADO Riccardo[a]*, PhD*
TUNGJAN Patchanee[b]*, MSc Candidate*

Executive Summary

- ❖ The vision of the Royal Government of Cambodia (RGC) is to become an upper-middle-income country by 2030, but to achieve this, it is fundamental to rely on technologies, which are the pivotal element for the RGC's transition to its e-version. The e-government vision aims to support and accelerate Cambodia's recovery after the COVID-19 pandemic, with Prime Minister Hun Sen confirming this, saying that it is fundamental to "accelerate the development of digital connectivity in the region and the digital transformation of society". A digital government may offer three C's benefits: Contextual, Coordinated, and Cognitive (The World Bank 2020).
- ❖ For supporting e-government and implementation of technologies in every aspect of the RGC, the first problem to tackle is the inadequate preparation of skilled labour, and more specifically of trained civil servants, mostly for what concerns digital literacy (Corrado and Tungjan 2019). Training can be expensive, but thanks to the affordability offered by Information Communication Technologies (ICTs), this problem can be

[a] **CORRADO Riccardo** is an Assistant Professor and Chair of the ICT program at the American University of Phnom Penh, and Advisor to the Cambodian Ministry of Post and Telecommunications.

[b] **TUNGJAN Patchanee** is a certified Occupational Therapist holding a bachelor's degree in Occupational Therapy (OT), and currently a graduate student in OT at Chiang Mai University, Thailand.

partially solved with the usage of free sources available online: Massive Open Online Courses (MOOCs).

- Policy options for stakeholders in the public sector:
    - Each Minister and public office should implement a professional development programme focused on digital literacy and the implementation of MOOCs, allowing the civil servants to update themselves following a KPIs model.
    - Each professional development programme should address a micro-credential system of credits for rewards and promotions, or even useful for human resources transfer between ministries or within the same ministry.
    - Each professional development programme should be structured in a way that civil servants can both improve themselves based on their interests (leveraging intrinsic motivation) and at the same time select courses from a pool of options created ad-hoc aiming to prepare them for serving the needs of each ministry.
    - Ministries and public offices should initiate cooperation programmes with local colleges and universities to offer professional development to the civil servants leading them to professional or academic degrees, capable of both professionally developing them and rewarding them with official credentials that could support their careers in the public and private sectors.

សេចក្ដីសង្ខេបអត្ថបទ

- ចក្ខុវិស័យរបស់រាជរដ្ឋាភិបាលកម្ពុជាគឺ ការក្លាយទៅជាប្រទេសមានប្រាក់ចំណូលមធ្យមកម្រិតខ្ពស់នៅឆ្នាំ២០៣០។ ដើម្បីសម្រេចឱ្យបាននូវចក្ខុវិស័យនេះ រដ្ឋាភិបាលត្រូវពង្រឹងវិស័យបច្ចេកវិទ្យាដែលជាធាតុស្នូលសំខាន់សម្រាប់ការឈានទៅរករដ្ឋាភិបាលអេឡិចត្រូនិច។ រដ្ឋាភិបាលអេឡិចត្រូនិចមានទិសដៅគាំទ្រ និងពន្លឿនការស្តារសេដ្ឋកិច្ចឡើងវិញក្រោយវិបត្តិជំងឺកូវីដ-១៩ ស្របតាមប្រសាសន៍របស់លោកនាយករដ្ឋមន្ត្រី ហ៊ុន សែន ថា វាគឺជាការចាំបាច់ណាស់ក្នុង «ការពន្លឿនការតភ្ជាប់ប្រព័ន្ធឌីជីថលនៅក្នុងតំបន់ និងការឈានទៅរកសង្គមឌីជីថល»។ រដ្ឋាភិបាលឌីជីថលនឹងផ្តល់នូវផលអត្ថប្រយោជន៍បីគឺ Contextual, Coordinated និង Cognitive។
- ដើម្បីគាំទ្ររដ្ឋាភិបាលអេឡិចត្រូនិច និងការប្រើប្រាស់បច្ចេកវិទ្យានៅគ្រប់ទិដ្ឋភាពរបស់រដ្ឋាភិបាល បញ្ហាដែលត្រូវដោះស្រាយដំបូងគេគឺ ការបណ្តុះបណ្តាលកម្លាំងពលកម្មជំនាញ ជាពិសេសមន្ត្រីរាជការស៊ីវិល អំពីអក្ខរកម្មឌីជីថល។ ការបណ្តុះបណ្តាលអាចមានតម្លៃថ្លៃ ប៉ុន្តែដោយសារបច្ចេកវិទ្យា

គមនាគមន៍ និងព័ត៌មាន (ICTs) បញ្ហានេះអាចត្រូវបានដោះស្រាយមួយផ្នែកតាមរយៈការប្រើប្រាស់ Massive Open Online Courses (MOOCs)។

- ❖ ជម្រើសគោលនយោបាយសម្រាប់ភាគីពាក់ព័ន្ធនានានៅក្នុងវិស័យសាធារណៈ៖
  - ○ ក្រសួង និងការិយាល័យសាធារណៈនីមួយៗ គួរអនុវត្តកម្មវិធីអភិវឌ្ឍន៍វិជ្ជាជីវៈ ដោយផ្តោតទៅលើអក្ខរកម្មឌីជីថល និងការអនុវត្ត MOOCs ដែលអនុញ្ញាតឱ្យមន្ត្រីរាជការស៊ីវិលអភិវឌ្ឍសមត្ថភាពរបស់ខ្លួនតាមគំរូ KPIs។
  - ○ កម្មវិធីអភិវឌ្ឍន៍វិជ្ជាជីវៈនីមួយៗ គួរប្រើប្រាស់ប្រព័ន្ធ Micro-credential System of Credits ដើម្បីផ្តល់រង្វាន់ និងការដំឡើងឋានៈ។ វាក៏មានប្រយោជន៍ផងដែរ សម្រាប់ការផ្ទេរធនធានអន្តរក្រសួង ឬនៅក្នុងក្រសួងតែមួយ។
  - ○ កម្មវិធីអភិវឌ្ឍន៍វិជ្ជាជីវៈនីមួយៗ គួរត្រូវបានរៀបចំឡើងតាមរបៀបមួយដែលមន្ត្រីអាចពង្រឹងសមត្ថភាពរបស់ខ្លួនដោយផ្អែកលើចំណាប់អារម្មណ៍របស់ពួកគេ និងអាចជ្រើសរើសមុខវិជ្ជាណាដែលមានប្រយោជន៍ទៅថ្ងៃក្រោយសម្រាប់បម្រើសេចក្តីត្រូវការរបស់ក្រសួង។
  - ○ ក្រសួង និងការិយាល័យសាធារណៈនីមួយៗ គួរផ្តួចផ្តើមកិច្ចសហការជាមួយសាលារៀន និងសាកលវិទ្យាល័យក្នុងស្រុក ដើម្បីផ្តល់ឱកាសឱ្យមន្ត្រីអាចទទួលបានសញ្ញាបត្រជំនាញ ដែលមានប្រយោជន៍ដល់អាជីពរបស់ពួកគេក្នុងវិស័យសាធារណៈ និងឯកជន។

Introduction

It is common knowledge that education represents one of the fundamental pillars of economic growth and social progress. Information and Communication Technology (ICT) has fostered both in the last decade (Doong and Ho 2012). Organisations such as the United Nations (UN) and the G8 countries are focusing on exploring the impacts ICT has on developing a country. It is a fact that, currently, technology adoption does not take place uniformly across the world (Ibid). Doong and Ho (2012) showed that countries with different Gross National Income (GNI) levels have different ICT development paths. ICT infrastructure and investment have a positive association with the level of a country's wealth. For what concerning ICT for education, ICT can enhance education in multiple ways, enabling, for example, the effective storing of data and reducing the quantity of information. It can create new types of interactive learning media (Khan et al. 2012), triggering and leveraging on a different form of learning preferences.

Regarding ICT for education, UNESCO defined Open Educational Resources (OER) as "teaching, learning and research materials in any medium – digital or otherwise – that reside in the public domain or have been released under an open license that permits no-cost access, use, adaptation and redistribution by others with no or limited restrictions". One of the most well-known forms of OER is represented by Massive Open Online Courses (MOOCs) (Hulsmann 2016). MOOCs are open online courses usually developed by educational institutions, governmental bodies, or private companies, offering free education to interested learners and targeting specific learning outcomes.

Thus, the use of ICT supports the delivery and access of information and the creation of knowledge, both of which represent ways for Cambodia to achieve the goals set by the Ministry of Education, Youth and Sport (MoEYS) and if used properly can be beneficial for the country (Corrado et al. 2019). MOOCs can represent not only a great way to provide open access to online education at the press of a button, but they also allow international students to participate in the activity due to the asynchronous nature of the courses and thus support the idea of connectivism. Culturally, social competencies and capacity or experience in extending beyond one's cultural context are very important, more so than in traditional courses (McAuley et al. 2010), and represent an asset for Cambodian MOOCs' learners.

MOOCs: Concepts and Significance

Initially, MOOCs captured the public imagination because they seemed not only capable of offering ivy-league education for free, but they also could solve the problem of access to higher education and quality professional development (Hulsmann 2016). Dillahunt et al. (2014) stated that MOOCs provide free access to universities for anyone with internet access, which is considered capable of democratising education. Mazoue (2013) wrote, “MOOCs address two of the three challenges facing postsecondary education, such as access and cost.” Furthermore, “MOOCs are an effective remedy to the ‘cost disease’ plaguing higher education,” Mazoue (2013) argued.

Even with MOOCs representing a very appealing solution, distance teaching universities in developed countries have reacted cautiously to the new affordances of digital technologies (Hulsmann 2016). There are two existing business models of MOOCs platforms with very different pricing strategies: the business-to-business (B2B) model and the business-to-customer (B2C) model (Jia et al. 2017). In the B2B model, MOOCs offering platforms target businesses interested in providing professional development to their employees or using educational resources to enhance their educational offer, for example, at universities. In the B2C model, instead, MOOCs platform targets individuals interested in learning and professionally develop themselves for their personal needs. While, by definition, the MOOCs are free and open-to-all, the MOOC platforms sell value-added MOOC services for profit, and it is a common model in internet services - called the freemium strategy. This strategy is underpinned by the idea that “the basic materials of MOOCs are open and free to all users, and the MOOC platforms also offer fee-based online value-added services to the users” trying to “cultivate the users’ payment habits with online marketing strategies” (Jia et al. 2017). Nevertheless, even without the possibility to pay, most MOOCs platforms offer basic materials free of charge.

MOOCs rely on the theoretical framework of connectivism. This framework defines, “Learning takes place when learners make connections between ideas located throughout their learning networks, which are composed of numerous information resources and technologies” (Dunaway 2012, 676). The recognition of connections between concepts, opinions, and perspectives becomes a fundamental element for the learning process (Ibid). In summary, connectivism emphasises, “The importance of the ability to recognise connections, patterns, and similarities” (Ibid), highlighting the idea that “choosing what to learn is a core component of the learning process in these contexts" (Wang and Baker 2015, 18). It is in this framework that each learner is responsible for their learning, something that can be experienced in the xMOOCs, where "the instructor provides video presentation to teach the course while each student follows their coursework at their learning speed" (Kesim and Altınpulluk 2015, 17).

MOOCs offer the possibility for each learner to freely choose the course they are interested in, with the freedom to access an openly shared curriculum that targets specific learning outcomes. Learners thus are empowered with the opportunity to access a virtually unlimited body of reliable learning resources, with the only requirement of having an internet connection and a computer. It is the freedom of accessing this virtually unlimited pool of knowledge that offers the possibility to anyone interested to develop their skills for their personal growth and career (Corrado and Tungjan 2019), or even for serving the needs of a country when these learners are civil servants.

MOOCs for Professional Development and Digital Literacy of Civil Servants in Cambodia

MOOCs can represent a wonderful and appealing solution to many of Cambodia's problems in the education and professional development sectors. However, MOOCs rely on the availability and reliability of internet connections. In terms of internet connectivity, Cambodia ranks good among developing countries. According to the Telecommunication Regulator of Cambodia (TRC), there are currently six mobile internet service companies and eleven fixed internet service companies in Cambodia. The number of registered SIM cards reaching 20.8 million and internet users reaching 98.5 per cent of the population (*Bangkok Post* 2019). This is conducive for assuring the successful implementation of online courses in every curriculum, since one of the major obstacles for using online courses passes by the quality of connection, bandwidth, power cuts, and cost of the service. Additionally, it is essential to pass through an effective learning design process for effective implementation of online courses, capable of selecting the right MOOCs and aligning them with the learning outcomes. "Nothing worth having comes easy," said Theodore Roosevelt.

In the case of Cambodia, MOOCs can support the vision of the RGC, which is to transition to e-government. Many projects are being discussed or have already started regarding different aspects of the transitioning process to e-government. One of the major undermining issues of this transition resides in the very limited tech-savviness of the civil servants, something that represents an issue for effective implementation and usage of all those digital tools on which e-government relies. Currently, many civil servants in Cambodia lack the necessary tech-savviness for supporting the government's vision, risking undermining the success of the whole e-government transition.

To tackle this obstacle, the Ministry of Post and Telecommunications, in cooperation with the other ministries, is initiating a pilot project to prepare its civil servants first before it will be rolled out to all public servants. However, it is a massive professional development process that can be difficult and expensive, if considered the need for skilled trainers. MOOCs can perfectly come in handy to support this process, offering free resources capable of supporting the professional development of the civil servants, with only the need for a well-developed curriculum designed ad-hoc to meet the needs of each role, duty, and ministry.

In aligning with the B2B model offered by MOOCs, platforms like Coursera or edX are already offering plans for corporations and businesses to offer access to their employees for learning and improving knowledge, thus building the capacity of their companies. This is a model not new to Cambodia. It has already been implemented by a few companies, such as the telecommunications company Smart Axiata and the insurance company Prudential Cambodia.

Even without paying MOOCs platforms, Cambodia's civil servants can still have access to the MOOCs completely for free. Professional development, mostly in digital literacy, is an essential element for updating and growing professions within an ecosystem, whether it is in the private or public domain. Thus, professional growth represents a pivotal element capable of constantly updating members of a group and capable of triggering in-house innovations, supporting the professional development of Cambodia and Cambodian civil servants.

Conclusion: Policy Options

Most MOOCs are offered on a free basis, with certification upon completion. Even in Cambodia, some companies have used this opportunity to develop their employees professionally at the personal level. However, at the public level, this opportunity has not been seized or implemented. Below are some policy options for stakeholders in the public sectors to seize the opportunity of MOOCs for professional development of Cambodia's civil servants:

- Each Minister and public office should implement a professional development programme focusing on digital literacy and implementing MOOCs, allowing the civil servants to update themselves by following a KPIs model of achievements.

- Each programme should address a micro-credential system of credits to be used for rewards and promotions.

- Each programme should be structured so that civil servants can improve themselves, based on their interests, but at the same time select courses from a pool of options created to prepare them for serving the scopes of each Ministry.

- Ministries and public offices should initiate cooperation programmes with local universities to offer professional development to the civil servants leading them to professional or academic degrees, capable of both professionally developing them and rewarding them with personal development that can support their careers in the public and private sectors.

The opinions expressed are the author's own and do not reflect the views of the Asian Vision Institute.

References

Bangkok Post. 2019. “Internet Users in Cambodia near 16m.” *Bangkok Post*. https://www.bangkokpost.com/business/1719527/internet-users-in-cambodia-near-16m.

Corrado, Riccardo, Robert E. Flinn, and Patchanee Tungjan. 2019. “Can ICT Help Cambodian Students Become the Solution for Improving Education in the Country?” *Journal of Management, Economics, and Industrial Organization* 3 (2): 1–15. https://doi.org/10.31039/jomeino.2019.3.2.1.

Corrado, Riccardo, and Patchanee Tungjan. 2019. “How Digital Tech Can Help Fix Cambodia’s Broken Education and Healthcare Systems.” In *E-Governance in Cambodia*, edited by Christopher Perera and Robert Hör, 20–39. Digital Insights. Phnom Penh, Cambodia: Konrad-Adenauer-Stiftung, Cambodia.

Dillahunt, Tawanna, Zengguang Wang, and Stephanie D. Teasley. 2014. “Democratising Higher Education: Exploring MOOC Use among Those Who Cannot Afford a Formal Education.” *International Review of Research in Open and Distance Learning* 15 (5): 177–96.

Doong, Shing H., and Shu-Chun Ho. 2012. “The Impact of ICT Development on the Global Digital Divide.” *Electronic Commerce Research and Applications* 11 (5): 518–33. https://doi.org/10.1016/j.elerap.2012.02.002.

Dunaway, Kathleen. 2011. “Connectivism”. *Reference Services Review,* 39(4), 675–685. doi:10.1108/00907321111186686

Hulsmann, Thomas. 2016. *The Impact of ICT on the Costs and Economics of Distance Education: A Review of the Literature*. Commonwealth of Learning (COL). http://oasis.col.org/handle/11599/2047.

Kesim, Mehmet, and Altınpulluk, Hakan (2015). A Theoretical Analysis of MOOCs Types from a Perspective of Learning Theories. *Procedia - Social and Behavioral Sciences*, *186*, 15-19. https://doi.org/10.1016/j.sbspro.2015.04.056

Jia, Yongzheng, Zhengyang Song, Xiaolan Bai, and Wei Xu. 2017. “Towards Economic Models for MOOC Pricing Strategy Design.” In *Database Systems for Advanced Applications*, edited by Zhifeng Bao, Goce Trajcevski, Lijun Chang, and Wen Hua, 387–98. Lecture Notes in Computer Science. Springer International Publishing.

Khan, Md Shahadat Hossain, Mahbub Hasan, and Che Kum Clement. 2012. “Barriers to the Introduction of ICT into Education in Developing Countries: The Example of Bangladesh.” *International Journal of Instruction* 5 (2): 61–80.

Mazoue, Jim. 2013. “The MOOC Model: Challenging Traditional Education.” *Educause Review* 1 (2): 161–74.

McAuley, Alexander, Bonnie Stewart, George Siemens, and Dave Cormier. 2010. *The MOOC Model for Digital Practice*. University of Prince Edward Island. https://www.islandscholar.ca/islandora/object/ir:15366.

The World Bank. 2020. “Digital Government for Development.” The World Bank. https://www.worldbank.org/en/topic/digitaldevelopment/brief/digital-government-for-development.

AVI PERSPECTIVE

ISSUE 2021, No. 10

Cambodia | 15th September 2021

Cambodia Digital Economy and Society Policy Framework 2021-2035: An Outlook

CORRADO Riccardo[a], PhD
MOK Rady[b], MA
UNG Sokoudom[c], MSc

Executive Summary

- In June 2021, by intending to accelerate an inclusive and sustainable post-pandemic growth, the Royal Government of Cambodia (RGC) has introduced the Cambodia Digital Economy and Society Policy Framework 2021–2035, representing the long-term vision in orienting the development and process of a digital transformation with an approach based on clearly defined steps, revolving around the private and public sector's needs, resources, and capabilities.
- The RGC identified three specific responsibilities to address: (1) supporting and promoting the ecosystems conducive to innovation and investment, (2) enhancing trust in the digital system, and (3) promoting the infrastructure development for connectivity, technology, network/data, and physical connectivity.

[a] **CORRADO Riccardo** holds a PhD in Information Engineering from the University of Trieste, Italy, and a M.Ed. from the University of Johannesburg, South Africa. Riccardo is an assistant professor and chair of the ICT program at the American University of Phnom Penh (AUPP), and an advisor to the Ministry of Post and Telecommunications (MPTC). He is also a collaborator and advisor to the STEAM programme of the AUPP High School-Foxcroft Academy.

[b] **MOK Rady** holds a master's degree in Global Political Economy from the University of London, UK. Currently, he is Director General of Administration at the Ministry of Post and Telecommunications (MPTC).

[c] **UNG Sokoudom** holds a master's degree in Information Technology from Monash University, Australia. Currently he is an advisor to the Ministry of Post and Telecommunications (MPTC).

- The RGC identified two foundation elements for a digital economy and society: (1) infrastructures and (2) digital reliability and confidence.
- The RGC identified three pillars of a digital economy: (1) digital citizens, including digital leadership, a pool of digital talent human resources; (2) digital government, including public services, improving digital performance, and data-based governance; and (3) a digital business, including elements such as enterprise digital transformation, entrepreneurship, startup ecosystems, and digital value chains.

សេចក្តីសង្ខេបអត្ថបទ

- ខែមិថុនាឆ្នាំ ២០២១ ក្នុងគោលបំណងពន្លឿនកំណើនសេដ្ឋកិច្ច ប្រកបដោយចីរភាព ក្រោយការរីករាលដាលនៃជំងឺរាតត្បាតកូវីដ១៩ រាជរដ្ឋាភិបាលកម្ពុជាបានដាក់ចេញនូវក្របខ័ណ្ឌគោលនយោបាយសេដ្ឋកិច្ច និងសង្គមឌីជីថលកម្ពុជា ឆ្នាំ២០២១-២០៣៥ ដែលឆ្លុះបញ្ចាំងពីចក្ខុវិស័យរយៈពេលវែងក្នុងការតំរង់ទិសដៅអភិវឌ្ឍន៍ និងដំណើរការនៃបរិវត្តកម្មឌីជីថលដោយផ្អែកលើវិធីសាស្ត្រដែលមានជំហានកំណត់យ៉ាងច្បាស់លាស់ ផ្តោតលើតម្រូវការធនធាន និងសមត្ថភាពរបស់វិស័យឯកជន និងសាធារណៈ។
- រាជរដ្ឋាភិបាលកម្ពុជា បានកំណត់នូវការទទួលខុសត្រូវដាក់លាក់ចំនួនបីចំនុច៖ (១) គាំទ្រនិងលើកកម្ពស់ប្រព័ន្ធអេកូឡូស៊ីដែលផ្តល់អំណោយផលដល់នវានុវត្តន៍និងការវិនិយោគ (២) បង្កើនការជឿទុកចិត្តលើប្រព័ន្ធឌីជីថលនិង (៣) លើកកម្ពស់ការអភិវឌ្ឍន៍ហេដ្ឋារចនាសម្ព័ន្ធសម្រាប់ការតភ្ជាប់ឌីជីថល បច្ចេកវិទ្យា បណ្តាញ/ទិន្នន័យ និងការតភ្ជាប់រូបវ័ន្ត។
- រាជរដ្ឋាភិបាលកម្ពុជា បានកំណត់នូវមូលដ្ឋានគ្រឹះពីរសំខាន់ៗសម្រាប់សេដ្ឋកិច្ចនិងសង្គមឌីជីថល៖ (១) ហេដ្ឋារចនាសម្ព័ន្ធនិង (២) ទំនុកចិត្តនិងភាពជឿជាក់លើប្រព័ន្ធឌីជីថល។
- រាជរដ្ឋាភិបាលកម្ពុជាបានកំណត់សសរស្តម្ភចំនួនបីនៃសេដ្ឋកិច្ចឌីជីថល៖ (១) ពលរដ្ឋឌីជីថល រួមមានភាពជាអ្នកដឹកនាំឌីជីថល និងប្រភពធនធានមនុស្សដែលមានទេពកោសល្យឌីជីថល។ (២) រដ្ឋាភិបាលឌីជីថល រួមមាន សេវាកម្មសាធារណៈឌីជីថល គន្លឹះជំរុញការអនុវត្តឌីជីថល និងអភិបាលកិច្ចផ្អែកលើទិន្នន័យ និង (៣) ធុរកិច្ចឌីជីថលដែលមានជាតុផ្សំដូចជា បរិវត្តកម្មឌីជីថលសហគ្រាស ប្រព័ន្ធអេកូឡូស៊ីសហគ្រិនភាពនិងធុរកិច្ចថ្មី និងប្រវាក់តម្លៃឌីជីថល៕

Introduction

To accelerate an inclusive and sustainable post-pandemic growth, the Royal Government of Cambodia (RGC) introduced in 2021 the Cambodia Digital Economy and Society Policy Framework 2021–2035. The framework has been developed as a long-term vision of the RGC in "orienting the development and process of a digital transformation" with an approach based on clearly defined steps revolving around the private and public sector's needs, resources, and capabilities (RGC 2021, 2). The Cambodia Digital Economy and Society Policy Framework 2021–2035 lays down the vision to "build a vibrant digital economy and society by laying the foundations for promoting digital adoption and transformation in all sectors of society – the state, citizens, and businesses – to promote new economic growth and improve social welfare in the new normal" (RGC 2021, 2). This article provides an analysis of the outlook of this newly introduced framework.

Every Challenge Is an Opportunity

The COVID-19 pandemic has been a major setback for sustainable development everywhere (Sachs et al. 2020). Different accesses to financial support and vaccines are fundamental factors in enlarging the development gap between developing and developed countries across the world (Sachs et al. 2021). East and South Asian regions have progressed towards achieving the Sustainable Development Goals (SDGs) introduced by the UN more than any other region since the adoption of the goals in 2015 (ESCAP 2021). This progression, however, has been characterised by a mismatch between realities based on different major indicators of the impact imposed by the pandemic. Considering the size and level of economic development as indicators, the pandemic has affected different countries and their path towards achieving the SDGs (Sachs et al. 2021, 19).

In the specific, the pandemic has negatively impacted many dimensions of societies since 2020. With a focus on sustainable development, Sachs et al. (2021) suggested that the whole region has been affected in all three dimensions of sustainable development, economic, social, and environmental. Consequently, a serious threat has been presented to the regional ability to sustain the race towards its post-pandemic growth characterised by sustainability elements. The impact has been even more manifested for developing countries, including Cambodia. While those developing countries are already suffering from the disadvantage compared to more developed nations, they are still directly and negatively impacted by them (RGC 2021). In this aspect, the 2021 International Spillover Index underlined “how rich countries can generate negative socioeconomic and environmental spillovers, including through unsustainable trade and supply chains” (Sachs et al. 2021, 8). For the specific case of Cambodia, essential sectors for the economic growth, such as garment, tourism, construction, and agriculture, have recorded a steady decline despite many years of high growth.

However, as the second US president, John Adams, wrote: “Every problem is an opportunity in disguise”. The Cambodian commitment to develop and move forward was already clearly pointed out before the pandemic. Specifically, during the opening ceremony of the 2018 Cambodia Outlook Conference, Cambodian Prime Minister Hun Sen said: “In our vision, Cambodia will become an upper-middle-income country by 2030 and a high-income country by 2050”. Prime Minister Hun Sen continued his speech, saying that to achieve this goal, Cambodia would continue focusing on human resources development, institutional capacity building, modernisation of technical equipment and materials, and on the information communication technology infrastructure, development, and expansion. Cambodia is working on many aspects of this vision, trying to improve the education sector, strengthening the Information and Communication Technology (ICT) and telecommunications infrastructures to support the digitalisation process and develop the overall physical and technological infrastructures throughout the country (Corrado, Flinn, and Tungjan 2019; Corrado and Tungjan 2019; Corrado and Hill 2021).

Nevertheless, even if economic growth is the target for the RGC, it is fundamental to aim for an economic growth that addresses specific elements of sustainability embodied in the 17 SDGs of the UN. In fact, an obsession with economic growth can lead to what Banerjee et al. (2021) called reductionist thinking across the board. In the specific, Banerjee et al. (2021) highlighted elements like “naïve quantitative formulations of a healthy economy, one-dimensional notions of the good life, instrumental views of the purpose of the natural world” as consequences of reductionist thinking driven by an obsession with economic growth, without a structured plan for the sustainability of it.

The Outlook

In June 2021, the RGC officially announced the implementation of the Cambodia Digital Economy and Society Policy Framework 2021–2035. This framework was aligned with the awareness of the importance of good governance for sustainably driving a digital economy, an essential element that emerged as a priority in this digital era (Jiang 2020). Additionally, along with digital governance, it is also important to account for the need to rely on data and our general increasing dependency on new economic indicators and new statistical approaches for driving good government decision-making (Jiang 2020).

Good governance for Cambodia represents the fundamental prerequisite for fostering a digital transformation that maximises the benefits that the ICT affordances can offer to increase productivity and economic efficiency (RGC 2021). A digital economy may affect the economy in several aspects, such as workforce and employment restructuring, changes in tax revenue collection, and changes in public investment expenditures (RGC 2021). Thus, it is essential to anticipate these changes and drive ICT usage to support the evolution of these areas of interest.

Foundation Elements

Moreover, in the Cambodia Digital Economy and Society Policy Framework 2021–2035, areas such as national economic growth, digital inclusiveness, reliability, and trustworthiness, without compromising national identity and culture, were identified as paramount areas that could benefit from the technological advances, if driven in a proper manner (RGC 2021). Furthermore, in the same framework, the RGC also identified three specific responsibilities to address: (1) supporting and promoting the ecosystems conducive to innovation and investment, (2) enhancing trust in the digital system, and (3) promoting the infrastructure development for connectivity, technology, network/data, and physical connectivity (RGC 2021). Considering these premises, to define specific elements to address within the identified responsibilities, the RGC has classified two main foundation elements and three pillars for a sustainable and inclusive digital transition of the economy. Within the foundation elements for a digital economy and society, the RGC listed (1) infrastructures and (2) digital reliability and confidence.

Focusing on the identified foundation elements, the first one is represented by digital connectivity. Regarding this, an e-government implementation is a complicated and costly process that involves risks and demands skills, technical resources, and a stable technical infrastructure (Fathey, Othman, and Norafida 2016). To support an effective and successful implementation, three main aspects need to be guaranteed: digital connectivity, the development of digital infrastructure, and the development of physical infrastructure (RGC 2021). Physical and digital infrastructures are essentials for supporting digital public services.

In addition to the individual ability to use devices, the internet, and digital services, connectivity, bandwidth, coverage, and even electronic devices ownerships are all elements relying on an effective and efficient ICT infrastructure, real enabler, even if not only essential factor, for supporting a digital government. Currently, Cambodia has several limitations, including a lack of backbone networks to provide ICT services for public organisations and the low coverage and bandwidth of the national network operated by the state-owned organisation and administration network (KOICA 2020). As noticed by Corrado and Hill (2021), an improvement of the ICT infrastructure passes by the better accessibility of telecom services, expansion of ICT infrastructure through government assistance and private investment, and an enhanced convergence of digital dimensions. Those dimensions include voice and data, wired and wireless, and telecom and broadcasting services (KOICA 2020). To reach this goal, the Ministry of Post and Telecommunications (MPTC) has already embarked on a long-term project for enabling digital connectivity throughout Cambodia by improving and extending telecommunication infrastructure in the country. It is a long and not-easy project, nonetheless, it is an essential starting point for achieving sustainable digital connectivity in Cambodia.

In terms of digital reliability and confidence, the second foundation element for enabling a Cambodian digital economy, one fundamental enabler factor is represented by the effective e-government. Specifically, e-government is a pivotal element for improving relationships between government and the public (Ravishankar 2013; Shareef et al. 2016). The RGC also describes it as one of the pillars of the digital economy. In a digital economy, without a doubt, it is crucial to create a strong relationship between the government and the public. Noticeably, establishing such a strong relationship is a common issue throughout the world, and several research works in the body of literature have investigated this area of interest. Several researchers have shown that citizens' trust in the government has declined dramatically in the past decades (Hosking 2019). The necessity to ensure trustworthiness is thus fundamental. Based on a comprehensive literature review, nineteen factors associated with the trustworthiness in e-government were identified (Janssen et al. 2018). Within the list of factors, Janssen et al. (2018) identified benevolence, integrity, trust in government, trust in technology, transparency, responsiveness, competence, accountability, privacy concerns, perceived security, perceived risk, system quality, service quality, satisfaction, political attitude, perceived ability to use, perceived prior knowledge, disposition to trust, and use. The complicated and multifaceted reality depicted by Janssen et al. (2018) highlighted the degree of difficulty in achieving trustworthiness.

Three Pillars

In addition to the two foundational elements, namely infrastructures and digital reliability and confidence, the RGC identified three pillars of digital economy: (1) digital citizens, including digital leadership, a pool of digital talent human resources; (2) digital government, including public services, improving digital performance, and data-based governance; and (3) a digital business, including elements such as enterprise digital transformation, entrepreneurship, startup ecosystems, and digital value chains.

With a specific focus on the first pillar, namely digital citizens, Cambodia is currently lagging in digital readiness (Corrado, Khat, and Nhean 2021; Corrado and Tungjan 2019). Cambodia is ranked seventh out of nine ASEAN member countries, and at the global level, it ranks 102nd out of 141 positions (RGC 2021). The digital readiness incorporates the idea of digital citizens, which includes elements like Digital Ethics, Media and Information Literacy, Participation/ Engagement, and Critical Resistance (Choi, Cristol, and Gimbert 2018). The Council of Europe defines digital citizenship as "the capacity to participate actively, continuously and responsibly in communities (local, national, global, online and offline) at all levels (political, economic, social, cultural and intercultural)" (Council of Europe 2021). Additionally, Choi et al. (2018, 1) defined digital citizenship "in terms of individuals' thinking, skills, and behaviours with regard to Internet use". Nonetheless, digital readiness cannot be limited to an elite of tech experts but should be an integral part of a society since it is a fundamental prerequisite for fostering effective and inclusive digital growth.

For what concerns digital government, although there is not a universally accepted conception of the e-government (Halchin 2004), e-government is commonly conceptualised as the use of ICT by governments in combination with organisational change to improve their structures and operations (Twizeyimana and Andersson 2019). E-government would rely on digital technologies because of their abilities to foster essential values in the public sectors, such as transparency, accountability, efficiency, and democratic values such as equality, openness, and fairness (Panagiotopoulos, Klievink, and Cordella 2019). In general, in accordance with the body of literature, it can be said that the e-government paradigm can offer many benefits to a government, especially in the area of public value (Dahl and Soss 2014). After an extensive literature review, Twizeyimana and Andersson (2019) identified six overlapping dimensions of the public value of e-government, namely improved public services, improved administrative efficiency, open government capabilities, improved ethical behaviour and professionalism, improved trust and confidence in government, and improved social value and well-being. However, even though the e-government approach seems to be an obvious solution to be adopted, its effective implementation in any ecosystem is not a straightforward process. Furthermore, without a sound plan, it may seriously risk failing. In this sense, according to Ndou (2017), “one of the reasons why many e-government initiatives fail is related to the narrow definition and poor understanding of the e-government concept, processes, and functions”.

Following Alshehri and Drew (2010), the implementation of e-government may face several barriers that can be classified into four major categories: technical, organisational, social, and financial barriers. Regarding the technical barriers, Cambodian ICT infrastructure still needs improvement, even if the MPTC is already working on this from several prospective, ranging from enhancing the 4G coverage throughout the country to digitalising itself first and leading the other governmental bodies in the process. In general, for what concerns the Cambodian case, for improving the ICT infrastructure in the country, KOICA set 3 main goals: improve service accessibility of telecom and broadcasting for all the people; expand ICT infrastructure through government assistance and activating private investment; and set the base environment for diverse ICT (KOICA 2020). Regarding the second category of barriers, namely organisational, for any technological acceptance from an organisation’s perspective, it is important to have supportive top management. For instance, Corrado and Hill (2021) suggested a top-down approach for the Cambodian government to ensure the smooth and effective adoption of cloud computing solutions in the country.

Furthermore, for what concerns the social barriers, Cambodia is still suffering from a lack of qualified personnel and the digital divide issue. The MPTC has started several projects to enhance awareness and digital savviness, mostly through its educational arm, the Cambodia Academy of Digital Technology (CADT). A few more projects have been started in the country to merge an entrepreneurial mindset with digital skills, but Cambodia still needs to wait for these projects to bear their fruits. Currently, the figures depict a disproportion between Science Technology Engineering and Mathematics (STEM) and non-STEM majors, which shows how Cambodia needs to groom its young talents and boost the motivation and interest of students in STEM fields, something still lacking in Cambodia. Finally, in terms of financial barriers, one of the main issues to consider for a government transition to its e-version is represented by the initial investment, which represents a barrier mostly for developing countries like Cambodia (Corrado and Hill 2021).

Nevertheless, regarding digital businesses, digital development has deeply changed the business ecosystem and affected many traditional firms across a wide spectrum of sectors, where digital has become the new norm on how to serve customers (Verhoef and Bijmolt 2019). Internet of Things (IoT), cloud technology, big data, mobile technologies, Artificial Intelligence (AI), and Robotics are all considered disruptive technologies (Sousa and Rocha 2019). These technologies, in fact, are driving the ongoing shift in the business ecosystem and triggering new business typologies to emerge, such as process monitoring, analytics, digital learning and e-learning, 3D printing, batteries, e-tourism, home-care, e-healthcare, traffic monitoring, and intelligent parking (Sousa and Rocha 2019). This digital transformation has fostered the growth of new platform-based solutions that aim to deliver customers more value at a lower cost without major technological changes in the actual product (Verhoef and Bijmolt 2019). The Cambodia Digital Economy and Society Policy Framework 2021–2035 addresses many aspects of the digital transition in the Cambodian economy and represents a fundamental step towards a digital Cambodian economy in the years to come.

Conclusion

In summary, with the Cambodia Digital Economy and Society Policy Framework 2021–2035, the RGC sets the vision to build a vibrant digital economy and society by laying the foundations for promoting digital adoption and transformation in all sectors of society. This vision relies on two foundation elements, namely infrastructures and digital reliability and confidence. Additionally, within the newly introduced framework, the Cambodian digital economy has been envisioned as a reality leveraging on three pillars: digital citizens, digital government, and digital businesses. With a strong digital and physical infrastructure in an ecosystem characterised by trustworthiness, the three pillars can be solidified and rise sustainably to support a growing digital economy in the Kingdom.

The opinions expressed are the author's own and do not reflect the views of the Asian Vision Institute.

References

Alshehri, Mohammed, and Steve Drew. 2010. “Implementation of e-Government: Advantages and Challenges. In *Proceedings of the IASK International Conference E-Activity and Leading Technologies & InterTIC 2010*, 79–86. Oviedo, Spain: IASK. https://research-repository.griffith.edu.au/bitstream/handle/10072/40620/72631_1.pdf?sequence=1

Banerjee, Subhabrata Bobby, John M. Jermier, Ana Maria Peredo, Robert Perey, and André Reichel. 2021. “Theoretical Perspectives on Organisations and Organising in a Post-Growth Era.” *Organisation* 28 (3): 337–57. https://doi.org/10.1177/1350508420973629.

Choi, Moonsun, Dean Cristol, and Belinda Gimbert. 2018. “Teachers as Digital Citizens: The Influence of Individual Backgrounds, Internet Use and Psychological Characteristics on Teachers’ Levels of Digital Citizenship.” *Computers & Education* 121 (June): 143–61. https://doi.org/10.1016/j.compedu.2018.03.005.

Corrado, Riccardo, Robert E. Flinn, and Patchanee Tungjan. 2019. “Can ICT Help Cambodian Students Become the Solution for Improving Education in the Country?” *Journal of Management, Economics, and Industrial Organization* 3 (2): 1–15. https://doi.org/10.31039/jomeino.2019.3.2.1.

Corrado, Riccardo, and Randolph D. Hill. 2021. “Strategy and Barriers to Overcome for Cambodian E-Government: A Discussion Paper.” In *Proceeding of the 7th KKU International Engineering Conference 2021 (KKU-IENC 2021)*, 149–55. Kon Kaen, Thailand: Faculty of Engineering, Khon Kaen University.

Corrado, Riccardo, Sereyvuth Khat, and Panha Vattey Nhean. 2021. “The Role of Cambodian Universities in Preparing Cambodia for a Digital Economy.” In *Digitalization and Sustainable Development*, edited by Raimund Weiß and Robert Hör, 76–84. Digital Insights 3. Phnom Penh: Konrad Adenauer Stiftung, Cambodia. https://www.kas.de/en/web/kambodscha/single-title/-/content/digital-insights-2.

Corrado, Riccardo, and Patchanee Tungjan. 2019. “How Digital Tech Can Help Fix Cambodia’s Broken Education and Healthcare Systems.” In *E-Governance in Cambodia*, edited by Christopher Perera and Robert Hör, 20–39. Digital Insights 2. Phnom Penh: Konrad-Adenauer-Stiftung, Cambodia.

Council of Europe. 2021. “Result Details.” *Council of Europe*. 2021. https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=090000168098de08.

Dahl, Adam, and Joe Soss. 2014. “Neoliberalism for the Common Good? Public Value Governance and the Downsizing of Democracy.” *Public Administration Review* 74 (4): 496–504. https://doi.org/10.1111/puar.12191.

ESCAP. 2019. “Asia-Pacific Disaster Report 2019.” *UN Economic and Social Commission for Asia and the Pacific*. https://www.unescap.org/sites/default/d8files/knowledge-products/Asia-Pacific%20Disaster%20Report%202019_full%20version.pdf

Fathey, Mohammed, Ibrahim Othman, and Ithnin Norafida. 2016. “Factors Influencing Cloud Computing Adoption for E-Government Implementation in Developing Countries:

Instrument Development." *Journal of Systems and Information Technology* 18 (3): 297–327. https://doi.org/10.1108/JSIT-01-2016-0001.

Halchin, L. Elaine. 2004. "Electronic Government: Government Capability and Terrorist Resource." *Government Information Quarterly* 21 (4): 406–19. https://doi.org/10.1016/j.giq.2004.08.002.

Hosking, Geoffrey. 2019. *The Decline of Trust in Government*. Brill. https://doi.org/10.1163/9789004390430_007.

Janssen, Marijn, Nripendra P. Rana, Emma L. Slade, and Yogesh K. Dwivedi. 2018. "Trustworthiness of Digital Government Services: Deriving a Comprehensive Theory through Interpretive Structural Modelling." *Public Management Review* 20 (5): 647–71. https://doi.org/10.1080/14719037.2017.1305689.

Jiang, Xiaojuan. 2020. "Digital Economy in the Post-Pandemic Era." *Journal of Chinese Economic and Business Studies* 18 (4): 333–39. https://doi.org/10.1080/14765284.2020.1855066.

KOICA. 2020. "Cambodian ICT Masterplan 2020." Masterplan. Cambodian ICT Masterplan. Korea: Koica and KISDI. https://tinyurl.com/sdedxs.

Ndou, Valentina (Dardha). 2017. "E – Government for Developing Countries: Opportunities and Challenges." *The Electronic Journal of Information Systems in Developing Countries* 18 (1): 1–24. https://doi.org/10.1002/j.1681-4835.2004.tb00117.x.

Panagiotopoulos, Panos, Bram Klievink, and Antonio Cordella. 2019. "Public Value Creation in Digital Government." *Government Information Quarterly* 36 (4): 101421. https://doi.org/10.1016/j.giq.2019.101421.

Ravishankar, M N. 2013. "Public ICT Innovations: A Strategic Ambiguity Perspective." *Journal of Information Technology* 28 (4): 316–32. https://doi.org/10.1057/jit.2013.18.

Royal Government of Cambodia (RGC). 2021. "Cambodia Digital Economy and Society Policy Framework 2021–2035." *Royal Government of Cambodia*. https://mef.gov.kh/news/cambodia-digital-economy-and-societypolicy/.

Sachs, Jeffrey D., Christian Kroll, Guillaume Lafortune, Grayson Fuller, and Finn Woelm. 2021. *The Decade of Action for the Sustainable Development Goals: Sustainable Development Report 2021*. Cambridge: Cambridge University Press. https://s3.amazonaws.com/sustainabledevelopment.report/2021/2021-sustainable-development-report.pdf.

Sachs, Jeffrey D., Guido Schmidt-Traub, Christian Kroll, Guillaume Lafortune, and Finn Woelm. 2020. *Sustainable Development Report 2020*. Cambridge: Cambridge University Press. https://apo.org.au/node/306675

Shareef, Mahmud Akhter, Yogesh K. Dwivedi, Vinod Kumar, and Uma Kumar. 2016. "Reformation of Public Service to Meet Citizens' Needs as Customers: Evaluating SMS as an Alternative Service Delivery Channel." *Computers in Human Behavior* 61 (August): 255–70. https://doi.org/10.1016/j.chb.2016.03.002.

Sousa, Maria José, and Álvaro Rocha. 2019. "Skills for Disruptive Digital Business." *Journal of Business Research* 94 (January): 257–63. https://doi.org/10.1016/j.jbusres.2017.12.051.

Twizeyimana, Jean Damascene, and Annika Andersson. 2019. "The Public Value of E-Government – A Literature Review." *Government Information Quarterly* 36 (2): 167–78. https://doi.org/10.1016/j.giq.2019.01.001.

Verhoef, Peter C., and Tammo H. A. Bijmolt. 2019. "Marketing Perspectives on Digital Business Models: A Framework and Overview of the Special Issue." *International Journal of Research in Marketing*, Marketing Perspectives on Digital Business Models, 36 (3): 341–49. https://doi.org/10.1016/j.ijresmar.2019.08.001.

AVI PERSPECTIVE

ISSUE 2020, No. 13

Cambodia | 11th December 2020

E-Government in Cambodia: Transformation in the Digital Age

TOUCH Darren[a], Master of Public Policy and Global Affairs

Executive Summary

- The COVID-19 pandemic is forcing governments around the world to harness and embrace e-government to deliver services effectively and efficiently. With social distancing and quarantine measures adopted to stop the spread of the virus, digital solutions have become vital for governments to continue their operation.

- Before the pandemic, Cambodia was undergoing a digital transformation towards e-government; however, COVID-19 has renewed and reinforced the role of digital government in the delivery of public services and the development of innovative efforts aimed at managing this unprecedented crisis.

- Cambodia has what it takes to be a digital nation and a champion of e-government, regionally and internationally, which supports other least developed countries in their digital transformation.

- This paper provides several recommendations to the Royal Government of Cambodia (RGC) on how to advance the development of e-government.

[a] **TOUCH Darren** is a Research Fellow at the Centre for Inclusive Digital Economy (CIDE) at the Asian Vision Institute (AVI) and a Schwarzman Scholar at Tsinghua University.

សេចក្តីសង្ខេបអត្ថបទ

- ជម្ងឺរាតត្បាតសកលកូវីដ-១៩ កំពុងបង្ខំឱ្យរដ្ឋាភិបាលប្រទេសនានានៅជុំវិញពិភពលោកបំពាក់ និងឱបក្រសោបយករដ្ឋាភិបាលអេឡិចត្រូនិច ដើម្បីបម្រើសេវាសាធារណៈប្រកបដោយ ប្រសិទ្ធភាព និងប្រសិទ្ធផល។ ជាមួយនឹងវិធានការគម្លាតសង្គម និងចត្តាឡីស័កដែលត្រូវបានអនុវត្តដើម្បីបញ្ឈប់ការរីករាលដាលរបស់វីរុសនេះ ដំណោះស្រាយឌីជីថលបានក្លាយជាជម្រើសដ៏មានសារៈសំខាន់មួយសម្រាប់រដ្ឋាភិបាលក្នុងការបន្តប្រតិបត្តិការរបស់ខ្លួន។
- នៅមុនពេលមានជម្ងឺរាតត្បាតសកល ប្រទេសកម្ពុជាបានកំពុងធ្វើការផ្លាស់ប្តូរឌីជីថលឆ្ពោះទៅរករដ្ឋាភិបាលអេឡិចត្រូនិច។ ទោះបីជាយ៉ាងណាក៏ដោយ ជម្ងឺកូវីដ-១៩បានបន្ត និងពង្រឹង តួនាទីរបស់រដ្ឋាភិបាលឌីជីថលក្នុងការផ្តល់សេវាសាធារណៈ និងការអភិវឌ្ឍនៃកិច្ចខិតខំប្រឹងប្រែង ប្រកបដោយនវានុវត្តន៍ដែលមានគោលដៅគ្រប់គ្រងវិបត្តិដែលមិនធ្លាប់មានពីមុនមកនេះ។
- ប្រទេសកម្ពុជាមានធនធានគ្រប់គ្រាន់ដើម្បីក្លាយជាប្រទេសឌីជីថល និងជាអ្នកជ្រោមជ្រែងទៅលើរដ្ឋាភិបាលអេឡិចត្រូនិចទាំងនៅក្នុងតំបន់និងនៅលើឆាកអន្តរជាតិ ដែលគាំទ្រដល់ប្រទេសអភិវឌ្ឍន៍តិចតួចដទៃទៀតនៅក្នុងការផ្លាស់ប្តូរឌីជីថលរបស់ពួកគេ។
- អត្ថបទនេះផ្តល់នូវអនុសាសន៍មួយចំនួនដែលរាជរដ្ឋាភិបាលកម្ពុជាអាចអនុវត្ត ដើម្បីជំរុញការអភិវឌ្ឍរដ្ឋាភិបាលអេឡិចត្រូនិចរបស់ខ្លួន។

Introduction

The COVID-19 pandemic is forcing governments around the world to harness and embrace e-government to deliver services effectively and efficiently. With social distancing and quarantine measures adopted to stop the spread of the virus, digital solutions have become vital for governments to continue their operation. Globally, many governments are exploring new ways to virtually engage and provide clear, up-to-date information to the general public. COVID-19 has become a litmus test for the e-government vision, structures, tools, and applications in which countries have invested over the past years. Nations that invested heavily into e-government before the pandemic started were not only well equipped to shift their services online with limited face-to-face interactions but were also able to innovate and develop innovative governance solutions.

E-government, also known as digital government, allows governments to use modern and emerging technologies to embrace good governance principles and achieve policy goals. Today, governments face pressure from the general public to increase their bureaucratic performance while being responsive to the needs of citizens. E-government is often conceptualised as the government's usage of Information and Communication Technologies (ICTs) to improve and integrate structures, operations and workflows to reduce financial costs and transactions times, optimise resource allocation and create sustainable solutions (Twizeyimana and Andersson 2019). E-government can strengthen and restore the trust of citizens in their government (UN E-Government Knowledgebase n.d.).

The pandemic has presented unprecedented challenges and opportunities for the development of e-government in Cambodia. Before the pandemic, Cambodia was undergoing a digital transformation towards e-government; however, COVID-19 has renewed and reinforced the role of digital government in the delivery of public services and the development of innovative efforts aimed at managing this unprecedented crisis. Ultimately, it has accelerated the embrace of e-government by nations around the world. If Cambodia solidifies this innovative digital ethos, these shifts hold the potential to not only recalibrate and modernise its public service and the ways it operates but also strengthen trust between the government and its people. This paper examines the development of e-government in Cambodia and offers policy proposals the country can adopt in order to realise its vision of becoming a highly digital nation.

Growing Digital Landscape in Cambodia

As digital technology is transforming the world, Cambodian society has quickly embraced this digital opportunity. Within recent years, Cambodians have greater access to the Internet due to the country's efforts to expand and upgrade its telecommunication infrastructure. For instance, according to the Telecommunication Regulator of Cambodia (TRC), approximately 16.1 million people had access to the Internet in 2019, indicating an increase of 20% compared to the previous year (Khmer Times 2020). As of 2020, Cambodia has made substantial progress in upgrading its telecommunication infrastructures by installing approximately 50,000 kilometres of fibre optic cables throughout the country and two submarine cables connecting Cambodia with Thailand, Malaysia and 17 other countries in Asia, Africa and Europe. Furthermore, Cambodia is moving beyond 4.5G mobile service by testing and deploying 5G services. With growing digital connectivity, further infrastructure investment is needed in addition to complementary governmental regulations, skills and institutions needed to sustain the country's digital momentum.

Increasing access to the Internet has transformed Cambodian society by driving economic growth, enhancing connectivity, and fostering access to greater information. For instance, Cambodian riders no longer haggle over the costs of a motorbike or tuk-tuk service, as they can now utilise mobile apps such as Grab and PassApp, which provide users with an upfront fare. Facebook has proven to be more than just a 'social network.' It has become a pervasive presence in Cambodian society with approximately 7.8 million users or 46.3% of the entire population using the platform for commercial, entertainment, news, and other purposes (NapoleonCat n.d.).

Likewise, customers can access their financial accounts online through 24/7 e-banking platforms, effectively reducing the need for in-person services. Led by a young, tech-savvy generation, Cambodia's emerging businesses and start-ups are increasingly becoming more digital. Industry 4.0 will transform Cambodia's manufacturing sectors through modification of production and the future of work. Unsurprisingly, Cambodians have been quick to adopt and adapt themselves to the digital revolution.

Cambodia has made progress in utilising e-government as part of public sector reform and transformation to enhance interactions between the state and society. The development of e-government in Cambodia began in 2000, which was led by the National Information

Communication Technology Development Agency (NiDA) under the Council of Ministers. Notably, the most significant e-government initiatives include the Government Administrative Information System (GAIS), Provincial Administrative Information System (PAIS), Financial Management Information System (FMIS), Human Resource Management Information System (HRMIS), Identification System, Electronic Visa System, Tax Payment System, Business Registration System, Certificate of Origin Management System, Automated System for Customs Data and National Single Window System.

In 2016, Prime Minister Hun Sen announced that the Royal Government of Cambodia (RGC) was moving towards e-government, which was a priority of the Rectangular Strategy Phase III 2013–2018 (Chheang 2016). The Ministry of Post and Telecommunications (MPTC)'s working group is responsible for drafting a digital government policy framework that aligns with the RGC's digital economy policy. This working group aims to create a plan to promote the usage of digital technology within the public sector (May 2020). The first draft of the E-Government Strategic Plan 2018–2023 aligns well with the ICT Masterplan 2020 and Telecom-ICT Policy 2020. With the digital economy prioritised in the Rectangular Strategy Phase IV 2018–2023, the RGC acknowledges that e-government must be developed in parallel with a whole-of-government approach. Although it has received growing attention within the public policy community, the in-depth application and implementation of e-government in Cambodia are still in their early phase.

According to the E-Government Development Index (EGDI) released by the United Nations Department of Economic and Social Affairs (2020), Cambodia has been recognised as a leader in digital government development among developing nations, advancing from the middle to high rank in 2020. Globally, Denmark (1st), the Republic of Korea (2nd), and Estonia (3rd) are recognised leaders, while the Republic of Korea (2nd), Singapore (11th), and Japan (14th) have the highest EGDI rankings in Asia (United Nations Department of Economic and Social Affairs, 2020). Most of Cambodia's e-government initiative consists of a simple one-way flow of information from the government to the citizenry through websites and social media platforms such as Facebook.

Despite ranking 124th, COVID-19 has not only renewed the RGC's commitment to making e-government a priority during the pandemic but has also illustrated its ability to be digitally innovative and agile (Chea 2020). For instance, the Ministry of Education, Youth and Sport (MOEYS) launched the e-learning portal encouraging students affected by school closure to study online. The Ministry of Interior's General Department of Immigration's Foreigners Present in Cambodia System app is used to grant visa extensions to foreigners unable to leave the country. Currently, more than 160,000 foreigners from 183 countries have registered themselves through the app (Khorn 2020). Cambodian Minister of Economy and Finance Aun Pornmoniroth noted that "COVID-19 has placed significant pressure on the nation's telecommunications system because of social distancing and other health measurements put in place. This has required converting governance from old analogue systems to new digital ones" (Khorn 2020). In light of COVID-19, the RGC was able to employ innovative digital solutions to problems created by the pandemic.

By regional and global comparison, Cambodia's e-government is incipient. Efforts are siloed and fragmented. Within the RGC, considerable progress has been made in some ministries while others have fallen behind. Progress in e-government development will depend on the RGC's adoption of a strategic and integrated whole-of-government approach, which positions Cambodia's public service to take full advantage of the digital age and to increase accountability, collaboration, openness, and transparency. Cambodia's e-government challenges include, but are not limited to, a digital literacy gap, inadequate IT infrastructure, and a lack of tech talent to design, implement, use, and manage e-government systems. To fully participate in this digital future, the country needs to establish a bold vision for e-government and commit significant and sustained resources to fostering local talent.

Fostering a Bold Vision for E-Government

In addition to the E-Government Strategic Plan, the RGC should also put forward a bold vision for e-government that builds momentum towards the transformative change in Cambodia's public service. A bold vision can provide energy and direction that emphasise the necessity of transformative change in all executive ministries and agencies. To realise this vision, national leadership is of paramount importance. For many leading e-government countries, the vision propelling e-government is part of a larger, more ambitious vision. Oftentimes, the vision seeks to transform these countries into 'smart' or 'digital' nations with societal-wide benefits.

A bold and clear vision for the future could ensure that the development and implementation of e-government are embedded in the RGC's strategic thinking and the mindsets of its public servants and citizens. Two goals can guide Cambodia towards successful e-government. The first is to strengthen and modernise the country's public administration and services through digital technology while the second is to support the development of an inclusive digital economy through digital business and digital citizenship.

Unlike countries where innovation and the application of technology are led by the private sector, Singapore has led digital innovation and implementation by putting in place policies, strategies, processes, and organisational structures that allow the government to be digital at its core.

In 2014, the Singaporean government unveiled the Smart Nation Initiative, which puts forward a vision for the use of digital innovation and technology to benefit the country and its people in driving sustainability and liveability. Prime Minister Lee Hsien Loong said, "Our vision is for Singapore to be a Smart Nation – A nation where people live meaningful and fulfilled lives, enabled seamlessly by technology, offering exciting opportunities for all" (Smart Nation and Digital Government Office 2018). In building a Smart Nation, the Singaporean government has emphasised a whole-of-nation approach composed of three pillars: Digital Government, Digital Economy, and Digital Society. Every year, the country sets milestones on specific areas that need to be improved and digitised, permitting their citizens, businesses, and public servants to adapt, learn, and innovate. According to the Initiative, the "priority is to harness technology to address national challenges and drive transformation in key domains: health, education, transport, urban solutions, and finance" (Smart Nation and Digital Government Office 2018).

The Smart Nation and Digital Government Group (SNDGG) was created in May 2017 to serve as a central, coordinating entity within the government that drives the development and implementation of e-government (Smart Nation and Digital Government Office 2018). Housed under the Prime Minister's Office, the SNDGG has gained increasing prominence and attention by senior political leaders and public servants. Moreover, it is led by a permanent secretary responsible for Smart Nation and Digital Government, illustrating the importance that e-government plays within the RGC's agenda. Since 2017, SNDGG has launched five Strategic National Projects such as the National Digital Identity, E-payments, Moments of Life, Smart Nation Sensor Platform and Smart Urban Mobility.

The transition to a digital government will require Cambodia to adopt a similar coordinating body, operating under either the Council of Ministers or the Prime Minister's Office. Cambodia has made progressive steps towards the development and implementation of e-government policy through the ICT Masterplan 2020, Telecom-ICT Policy 2020, and E-Government

Strategic Plan (in development). Missing from its masterplan, framework, strategic plan, and policy is the vision of digital transformation. The lack of a clear and bold vision challenges the ability of the RGC officials and the general public to think strategically towards e-government. As such, we need a vision that embraces a whole-of-nation approach, builds momentum both inside and outside of the RGC, empathises planning and budgeting of e-government in a strategic, systematic way and effectively guides the country towards becoming a smart nation.

Digital Capacity Building

Building a digitally competent public service sector will require significant and sustained investment by the RGC. To build a digital government, the RGC needs digital engineers and specialists in coding, software engineering, artificial intelligence, machine learning, the Internet of Things, and much more. In essence, Cambodia needs to compete with tech companies such as Google and Facebook to attract talent in building in-house expertise within the public sector to support e-government development. One of the challenges the public service will have to overcome in competing with the tech giants for digital talent is to ensure compensation is competitive and attractive. Alternatively, as found in many countries like the US, the private sector could be the primary provider of digital solutions for e-government development and implementation through a public-private partnership model.

Despite the progress made, Cambodia tech sector is still nascent in comparison to its regional Southeast Asian neighbours such as Thailand and Vietnam. According to Cambodia's first tech start-up report by Raintree Cambodia and Smart Axiata, *Startup Kingdom: Cambodia's Vibrant Tech Startup Ecosystem in 2018,* high-skilled technical talent, while increasing, is not in abundant supply. The report found that there was a lack of mid to senior-level technical talent with project management and executive experience. Moreover, out of 118 public and private high education institutions, only about 30% offer IT and engineering programmes, resulting in approximately 2,000 to 5,000 new technology graduates per year (Khern 2019).

To become an upper-middle-income country by 2030 and a high-income country by 2050, Cambodia's socio-economic development depends on high-quality education and life-long learning with an emphasis on science, technology, engineering, and mathematics (STEM). The success of Cambodia's e-government will depend on the country's ability to produce and sustain high-skilled tech workers.

Although the ICT Masterplan 2020 identified the need to strengthen and provide ICT training to public servants, a critical component that is needed is the public service's ability to attract, recruit, and retain tech talent. First, the RGC will need to further incorporate digital literacy and technical training into the education system to create a pipeline of tech students. In particular, with governmental support, institutions of higher education should expand programmes that produce a talented pool of engineers, software developers, and coders. Second, the RGC will have to compete with businesses and start-ups in recruiting technical talent – or technologists – into the public sector. Recognising the need for tech talent, the Singaporean government revised its Human Resources scheme to match attractive salaries offered by the private sector and has expanded its talent search from domestic recruitment to the international level (Khern 2019). Moreover, to attract tech talent from the private sector, Singapore launched the Smart Nation Fellowship programme, which allows Singaporeans to collaborate on digital or engineering solutions with the central government from three to six months (Gov Tech Singapore n.d.). Within the public service, tech talent can join a variety of governmental agencies to gain exposure to Singapore's e-government transformation and innovation. Although the Singaporean government seeks to build in-house digital capacity, it emphasises the need to work with the private sector to ensure that the designs of digital products and services are of high-quality.

In the US, former CEO of Google Eric Schmidt is leading a federal initiative to launch the US Digital Service Academy that would provide the US Federal Government with a new generation of tech workers. Unlike graduates from top universities such as Stanford University and Massachusetts Institute of Technology, the graduates would be trained in coding, cybersecurity, and artificial intelligence along with education about government duty and service (Canales 2020). Founded in 2014 by former President Barack Obama, the US Digital Service Academy would serve as a pipeline for the US Digital Service and bring together the best engineering, design, and public service talent to change the US Federal Government's approach to technology.

Embracing e-government will require substantial investments by the RGC: what gets financed, gets done. The direction Singapore and the US is taking is highly intentional and deliberative with the state's fiscal resources to support its e-government developments. Unfortunately, Cambodia does not have the same fiscal advantages, but it is a vital principle to embrace. Whether it is competing for talent by offering competitive compensation or building a digital service academy, both will come with substantial costs and investments. However, there are opportunities for the costs to be shared through a public-private partnership model. Nevertheless, the guaranteed outcome must always serve the public good.

Forming Regional and International Partnerships

There is no silver bullet or standardised approach to e-government development. Cambodia needs a "Made-In-Cambodia" solution that captures the localised context and situation with support from regional and international partners, who can share their best practices and expertise. Through regional and international partnerships, Cambodia can learn from developed countries where e-government is well-established. Several countries such as Singapore and South Korea have partnered with Cambodia to help sow new talents in ICTs. Through the Singapore Cooperation Enterprise and Temasek Foundation International, Cambodian public servants engaged with and learned from Singapore's experience in ICTs through various workshops in 2018 (Singapore Cooperation Enterprise and Temasek Foundation International 2018). In December 2019, Cambodia and South Korea signed a memorandum of understanding to cooperate on a one-year development plan for e-government (South Korean Ministry of Interior and Safety 2019). Within regional and international fora, Cambodia could also serve as a champion in supporting e-government transformation among developing countries. As part of its foreign policy, Cambodia should put forwards a Smart Nation agenda, which encompasses e-government as part of its bilateral and multilateral diplomatic engagements.

Driving E-Government Forward

The COVID-19 pandemic has renewed and re-vitalised the significance of e-government for countries around the world as countries harness and embrace e-government to deliver public services effectively and efficiently. In the case of Cambodia, COVID-19 has not only renewed the RGC's commitment to making e-government a priority during the pandemic but has also illustrated its ability to be digitally innovative and agile in responding to pressing challenges facing its society. Cambodia has what it takes to be a digital nation and a regional and global champion of e-government which supports other least developed countries in their digital transformation. Although e-government will require substantial investments, its benefits will outweigh the costs. Therefore, Cambodia must remain steadfast in its development of e-government.

To develop and implement e-government, the RGC should:

- Develop a clear and bold vision for e-government that allows public servants and citizens to understand and support the digital transformation in Cambodia’s public service;
- Ensure the E-Government Strategic Plan takes a whole-of-government approach that emphasises the digital direction of governmental programmes and services;
- Incorporate digital literacy and technical training in the education system to create a pipeline of students entering the tech sector;
- Work with higher education institutions to expand programmes that produce a talent pool of engineers, software developers, and coders;
- Recruit, retain, and reskill tech talent in the public sector to develop in-house digital/tech capabilities and advance e-government projects;
- Collaborate with the private sector to enhance and expand e-government development within the country;
- Build regional and international partnerships to advance Cambodia’s e-government agenda; and
- Serve as an e-government champion amongst least developed countries, regionally and internationally, as part of Cambodia’s foreign policy.

The opinions expressed are the author’s own and do not reflect the views of the Asian Vision Institute.

References

Canales, Katie. 2020. "Ex-Google CEO Eric Schmidt Is Working to Launch a University That Would Rival Stanford and MIT and Funnel Tech Workers Into Government Work." *Business Insider*. Accessed December 1, 2020. https://www.businessinsider.com/google-eric-schmidt-us-digital-service-academy-2020-7.

Chea, Vannak. 2020. "Government Declares E-Governance Now A Top Priority Amid Pandemic." *Khmer Times*. Accessed December 1, 2020. https://www.khmertimeskh.com/708895/government-declares-e-governance-now-a-top-priority-amid-pandemic/.

Chheang, Vannarith. 2016. "Cambodia Embarks on E-Government." *Khmer Times*. Accessd December 1, 2020. https://www.khmertimeskh.com/36107/cambodia-embarks-on-e-government/.

Gov Tech Singapore. n.d. "Smart Nation Fellowship Programme." *Gov Tech Singapore.* Accessed August 13, 2020. https://www.tech.gov.sg/careers/smart-nation-fellowship-programme/.

Khern, Ng Chee. 2019. "Digital Government, Smart Nation: Pursuing Singapore's Tech Imperative." *Civil Service College - Singapore.* Accessed December 1, 2020. https://www.csc.gov.sg/articles/digital-government-smart-nation-pursuing-singapore's-tech-imperative#notes.

Khmer Times. 2020. "Internet Subscribers in Cambodia Grows 20 Percent to 16.1 Million in 2019." *Khmer Times*. Accessed December 1, 2020. https://www.khmertimeskh.com/50698943/internet-subscribers-in-cambodia-grows-20-percent-to-16-1-million-in-2019/.

Khorn, Savi. 2020. "App Logs 160,000 Foreigners." *The Phnom Penh Post*. Accessed December 1, 2020. https://www.phnompenhpost.com/national/app-logs-160000-foreigners.

May, Kunmakara. 2020. "Ministry to Prepare the Country for Digitalisation." *The Phnom Penh Post*. Accessed December 1, 2020. https://www.phnompenhpost.com/business/ministry-prepare-country-digitalisation.

NapoleonCat. n.d. "Facebook Users in Cambodia—April 2019." NapoleonCat. Accessed August 14, 2020. https://napoleoncat.com/stats/facebook-users-in-cambodia/2019/04.

Organisation for Economic Co-operation and Development (OECD). n.d. "Implementing E-Government in OECD Countries: Experiences and Challenges." *OECD.* Accessed August 13, 2020. http://www.oecd.org/mena/governance/36853121.pdf.

Raintree Cambodia. 2019. "Startup Kingdom: Cambodia's Vibrant Tech Startup Ecosystem in 2018." *Raintree Cambodia*. Accessed December 1, 2020. https://www.raintreecambodia.com/research.

Singapore Cooperation Enterprise and Temasek Foundation International. 2018. "Singapore Cooperation Enterprise and Temasek Foundation International to Support Second Programme in Infocommunication Technology in Cambodia." *Singapore Cooperation Enterprise and Temasek Foundation International*. Accessed December 1, 2020. https://www.temasekfoundation-international.org.sg/file/our-newsroom/news-releases/2018/news-release-19nov2018-sce-tf-intl-to-support-second-prog-in-ict-in-cambodia-web-.pdf.

Smart Nation and Digital Government Office. 2018. "Smart Nation: The Way Forward Executive Summary." *Smart Nation and Digital Government Office.* Accessed December 1, 2020. https://www.smartnation.gov.sg/docs/default-source/default-document-library/smart-nation-strategy_nov2018.pdf?sfvrsn=3f5c2af8_2.

Smart Nation and Digital Government Office. 2020. "Smart Nation and Digital Government Group (SNDGG)." *Smart Nation Singapore*. Accessed August 12, 2020. https://www.smartnation.gov.sg/why-Smart-Nation/sndgg.

South Korean Ministry of Interior and Safety. 2019. "Korea and Cambodia Signed MOU On E-Government." *South Korean Ministry of Interior and Safety*. Accessed December 1, 2020. https://www.mois.go.kr/eng/bbs/type001/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000019&nttId=74942.

Twizeyimana, Jean D, and Annika Andersson. 2019. "The Public Value of E-Government – A Literature Review." *Government Information Quarterly* 36 (2), 167–78. https://doi.org/10.1016/j.giq.2019.01.001.

UN E-Government Knowledgebase. n.d. "E-Government." *UN E-Government Knowledgebase*. Accessed August 13, 2020. https://publicadministration.un.org/egovkb/en-us/About/UNeGovDD-Framework.

United Nations Department of Economic and Social Affairs. 2020. "E-Government Survey 2020 Digital Government in the Decade of Action for Sustainable Development." *United Nations Department of Economic and Social Affairs*. Accessed December 1, 2020. https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020 UN E-Government Survey (Full Report).pdf.

AVI PERSPECTIVE

ISSUE 2021, No. 02

Cambodia | 11th December 2020

Digital Data Governance in Cambodia: Progress and Prospect

CHHORT Chhorravuth[a], BA in Economics and Innovation
CHHEANG Vannarith[b], PhD in Asia Pacific Studies

Executive Summary

- Digital data governance is a means to secure a safe data flow by developing and enhancing information security, data protection and privacy, as well as inter-operability through digital adoption and connectivity.
- Cambodia has started introducing policy and legal frameworks in support of digital data governance since 2014. While some achievements have been made, there are remaining impediments that need to be addressed and room to be improved.
- In rolling out digital data governance, the main challenges that Cambodia is facing include the lack of agile policy instruments, robust legal frameworks, efficient institutions, qualified human resources, and digital infrastructure.
- This article proposes that Cambodia enhance policy coordination and institutional synergies among key ministries and government agencies. It needs to develop a legal framework, invest more in human capital development in digital government and infrastructure, strengthen public-private partnership in innovation, and support local enterprises especially MSMEs in technology adoption and digital entrepreneurship development.

[a] **CHHORT Chhorravuth** is a Research Associate of the Centre for Inclusive Digital Economy (CIDE) at the Asian Vision Institute (AVI).
[b] **CHHEANG Vannarith** is President of AVI.

សេចក្តីសង្ខេបអត្ថបទ

- អភិបាលកិច្ចទិន្នន័យឌីជីថលគឺជាមធ្យោបាយមួយ ដើម្បីធ្វើឱ្យលំហូរទិន្នន័យប្រកបដោយការការពារ និងសុវត្ថិភាព តាមរយៈការអភិវឌ្ឍនិងការពង្រឹងសន្តិសុខព័ត៌មាន ការការពារនិងភាពឯកជននៃទិន្នន័យ និងការពង្រឹងអន្តរប្រតិបត្តិការតាមរយៈការអនុវត្តនិងការភ្ជាប់ឌីជីថល។
- ប្រទេសកម្ពុជាបានចាប់ផ្តើមដាក់ចេញនូវគោលនយោបាយ និងក្របខ័ណ្ឌច្បាប់ក្នុងការគាំទ្រដល់ការគ្រប់គ្រងលើអភិបាលកិច្ចទិន្នន័យឌីជីថល ចាប់តាំងពីឆ្នាំ ២០១៤ មកម្ល៉េះ។ ខណៈពេលដែលសមិទ្ធផលមួយចំនួនត្រូវបានបង្កើតឡើង ឧបសគ្គដែលត្រូវដោះស្រាយក៏នៅតែមាន។
- បញ្ហាប្រឈមធំៗ ដែលប្រទេសកម្ពុជាកំពុងប្រឈមមុខក្នុងការដាក់ចេញនូវអភិបាលកិច្ចទិន្នន័យឌីជីថល រួមមានកង្វះឧបករណ៍គោលនយោបាយដោយសកម្ម ក្របខ័ណ្ឌច្បាប់ដ៏រឹងមាំ ស្ថាប័នដែលមានប្រសិទ្ធិភាព ធនធានមនុស្ស និងហេដ្ឋារចនាសម្ព័ន្ធឌីជីថល។
- អត្ថបទនេះ លើកឡើងពីការស្នើសុំឲ្យកម្ពុជា គួរតែបង្កើនការសម្របសម្រួលគោលនយោបាយ និងការរួមបញ្ចូលស្ថាប័ន ក្នុងចំណោមក្រសួងសំខាន់ៗជាមួយទីភ្នាក់ងាររដ្ឋាភិបាល។ កម្ពុជាចាំបាច់ត្រូវបង្កើតក្របខ័ណ្ឌច្បាប់ វិនិយោគបន្ថែមលើការអភិវឌ្ឍមូលធនមនុស្សនៅក្នុងរដ្ឋាភិបាលឌីជីថលនិងហេដ្ឋារចនាសម្ព័ន្ធ ពង្រឹងភាពជាដៃគូរង្វាងវិស័យសាធារណៈនិងឯកជនក្នុងការច្នៃប្រឌិត ព្រមទាំងគាំទ្រសហគ្រាសក្នុងស្រុកជាពិសេស MSMEs ក្នុងការទទួលយកបច្ចេកវិទ្យាថ្មី និងការអភិវឌ្ឍសហគ្រាសឌីជីថល។

Digital Data Governance Development

Digital Data Governance (DDG) plays a critical role in providing secure and safe data flow through the development and enhancement of information security, data protection and privacy, the verification and authentication of digital identification, as well as inter-operationality. The Cambodian government has been actively promoting digitalisation since 2014. For instance, the ICT Master Plan was issued in 2014 with four strategic objectives: empowering people, enrich e-services, enhancing capabilities, and ensuring connectivity. In 2015, the Law on Telecommunications was adopted, and in 2016 the policy on Telecom/ICT Development 2020 was launched. In 2017, the sub-degree on digital signature and the sub-degree on a mechanism to implement the Universal Service Application were adopted.

According to the Telecommunication/ICT Development Policy 2020, the government aims to achieve 100% of broadband coverage in urban areas and 70% in rural areas, 80% of internet penetration rate, 10% of IoT or connected to devices in the network. However, these targets have not been fully achieved due to key barriers to digital development. According to Cambodia's telecommunication regulator, digital infrastructure remains underdeveloped, especially the Next Generation Services, lacking skilled staff and an adequate legal framework, and the digital government remains fragmented (Im 2019).

The Covid-19 pandemic has accelerated the speed of digital transformation in Cambodia. The Cambodian government and private economic operators have adapted to and adopted digital technology to make their services and products more efficient and cost effective. Technology adoption has become a matter of survival for some industries. The government launched online business registration in June 2020. Three different ministries and institutions are integrated into the same platform called Cambodia Data Exchange (CamDX)- Ministry of Commerce, Ministry of Labour and Vocational Training, and General Department of Taxation. The remaining challenges are company name check (taking up to three business days), and each shareholder and director needs to sign the draft articles of association. Digital signature will help solve the problem. The government is updating the registration portal including a function to update company information after approval, allowing IT systems of other ministries or institutions to link with the CamDX platform.

The government has the ambition to develop a functional digital economy by 2023- but it is hard to realise. It tentatively defines digital economy as "a part of economic output derived primarily from digital technologies with a business model based on digital goods and services" (Kong 2019). The government is working on several important policy and legal frameworks- expected to be concluded and adopted in the near future- to facilitate and manage digital transformation, including digital government policy frameworks, digital economy policy, and cybercrime law. Meanwhile, it is also developing digital infrastructure and capacity building programmes.

The main challenge for digitalisation in Cambodia is insufficient digital infrastructure. Digital government adoption is shallow and fragmented. Business digital adoption remains slow with a small local market for digital business. ICT skills and literacy remain low, and Khmer script contents and analysis are still complex (Kong 2019). Besides, there is a lack of legal instruments, institutional frameworks, and support mechanisms to build an ecosystem to enable digitalisation in a safe, inclusive, and effective manner. Management and protection of the economic operators, consumers, and intermediaries' identity are crucial in promoting national and international digital trade.

The level of awareness and understanding of DDG remains low in both the public and private sectors, given it is a relatively new concept for the Cambodian stakeholders. There has not been a sub-degree requiring government agencies to work with DDG lead agency in developing the digital data governance framework at the national level yet. The digital adoption at private firms and public institutions remains low although it is making some good progress. The lack of institutions, law and regulations, and human resources is the key constraint.

State Agencies Responsible for Digital Data Governance

The Ministry of Post and Telecommunications (MPTC) plays a leading role in developing a digital government policy framework and other law and regulations governing the digital economy. Some different key policy and legal instruments, including the National Internet Gateway (NIG) sub-decree, are in the final stage of stakeholder consultation. The data protection law discussion is still ongoing (it might take a few more years to be concluded and adopted). The (NIG) is established to facilitate and manage internet connections to enhance internet traffic and national revenue collection effectiveness and efficiency. As a necessity, NIG will be based in multiple locations. It will facilitate cross border connectivity and improve domestic traffic. Having NIG would save the internet traffic connections cost up to 30 per cent.

The NIG does not aim to generate additional revenues for the MPTC from active telecom operators but to generate revenues from non-compliant operators.

The MPTC is drafting a law on cybersecurity to deal with increasing cybersecurity threats and incidents. The draft law is aimed to establish basic principles and measures to prevent, manage and respond to cyber threats at the institutional, regulatory, and national levels. It also aims to regulate owners of critical information infrastructure (CII), cybersecurity service providers, and digital service providers, as well as to build on local cybersecurity capability. Regarding regional cooperation on cybersecurity, Cambodia supported in principle the Cyber Norms as the mechanism to reduce risks in the ICT sector. The country is willing to cooperate with other ASEAN Member States and dialogue partners to strengthen regional cybersecurity. In this connection, the ASEAN-Singapore Cybersecurity Centre and ASEAN-Japan Cybersecurity Capacity Building Centre should provide more capacity building programmes on cybersecurity to less developed economies like Cambodia.

The MPTC is also developing a digital government policy framework, which will be released sometimes in 2021. The policy aims to modernise government systems and public service delivery through digital technologies. Efficiency, transparency, accountability, and inclusion are the core principles of the digital government. The ministry is also developing a new postal law (replacing the 2002 postal law), the law on cybersecurity, radio frequency allocation plan, 5G roadmap, telecoms infrastructure improvement and Sihanoukville-Hong Kong submarine cable project. In terms of capacity building, the ministry has provided training programmes to provincial officials across the country and upgraded the National Institute of Post, Telecoms, and ICT (NIPTICT) to be Cambodia Academy of Digital Technology (CADT) in 2021.

In November 2020, the MPTC and the General Department of Taxation (GDT) discussed measures to collect tax on digital services provided by major tech companies not registered in Cambodia such as Amazon, Alibaba, Facebook and Google. The ministry is also developing CII protection to safeguard internet traffic and provide additional cybersecurity for GDT's existing IT infrastructure. The MPTC and GDT plan to draft regulations and build technical capacity for tax digital advertisements and services. A national Big Data Hub being developed by the MPTC is essential to integrate and share information among government institutions at both national and subnational levels. In December 2020, the MPTC started multi-stakeholder consultation meetings on "Digital Service Tax" for foreign tech firms that do not register in Cambodia.

The Ministry of Interior has drafted cybercrime law- the process started in 2016 with the technical support from the Department of Justice of the United States- to be adopted by the end of this year or early next year. Currently, it is in the final phase of stakeholder consultation. There have been more than 60 multi-stakeholder consultation meetings with the government, the private sector, and civil society representatives. According to the cybercrime law, the Ministry of Interior is the competent authority to deter, prevent, and suppress offences, and the judicial police officers under the National Police Commissariat are authorised to investigate crimes. The competent authority is authorised to grant an online business permit, certificate, or licence and to suspend or revoke that permit, certificate, or license if such an online business operator commits an offence.

The Ministry of Interior launched a public service platform called "One Window Service Mechanism" in 2008 with the World Bank's support. In 2003, the pilot projects were implemented in two provinces with the financial backing of several German Foundations (Rhein-Sieng-Kreis, Konrad-Adenauer Foundation, BBJ Services) and Soleto city from Italy. From 2004 to 2007, the European Union supported the project. The platform plays a critical role in enhancing public service delivery at the sub-national level (at the district level) by providing efficiency and accessibility to public service, promotion of transparency and accountability, as well as receiving feedback and complaints from the users. The service is gradually expanding across the country.

The Ministry of Economy and Finance formed a working group on Digital Economy in 2018 to draft a comprehensive digital economy for Cambodia. The working group consists of three sub-groups: inter-ministerial committee, working group, and a technical working group. The Supreme National Economic Council (SNEC) is in charge of drafting a Digital Economy policy framework. The government has been working on strengthening and expanding the digital economy's foundation in both hard and soft infrastructure, developing human capital and skills, as well as developing legal and regulatory frameworks. It would take about five years to prepare the groundwork and digital readiness and another five to ten years to build a technology-driven market. The digital economy policy framework is expected to be released this year.

There are three phases (foundation phase, adoption phase, and transformation phase) and five strategic elements in the digital economy policy framework.

1. Digital infrastructure development focusing on digital connectivity, digital payment infrastructure, logistics and delivery services.

2. Digital government developing focusing on digital key enablers, public service digitalisation, and data-driven governance.

3. Digital business development focusing on SMEs' digital adoption and transformation, start-up and entrepreneurship ecosystem, and digital value chain.

4. Digital literacy and capability development focusing on digital leadership, digital talent pools, and digital citizens.

5. Digital trustworthiness focusing on laws and regulations, regulators and institutional capacity, cybersecurity, and consumer trust.

The Ministry of Industry, Science, Technology, and Innovation was created in March 2020 (formerly the Ministry of Industry and Handicraft) to enable Cambodia to grasp the Fourth Industrial Revolution's opportunities. The ministry is drafting Tech Transfer Law to promote the transfer of technologies from Foreign Direct Investment to local companies and staff, and other policy frameworks on science, technology, and innovation. The Department of STI Data Management under the ministry is also involved in developing Data Centre, Cybersecurity, and Digital Data Governance. However, there is no clear guideline or roadmap on the policy development of DDG yet.

The Ministry of Commerce has taken concrete steps to promote digital transformation. An automation system was adopted in the online application of the Certificate of Origin (CO) in 2015, including e-ATIGA Form D and online business registration in 2020. The online business registration website, also known as the Single Portal, is developed by the Ministry of Economy and Finance using the Cambodia Data Exchange (CamDX) system. CamDX is a unified way of data exchange; a distributed system based on collaboration; a platform that handles data security, authenticity and integrity; a suitable APIs for easing interoperability; and a platform designed to be scaled up.

The online business registration services of namely the Ministry of Commerce, Ministry of Labour and Vocational Training, and General Department of Taxation are integrated into this Single Portal. The Ministry of Economy and Finance facilitates, regulates and simplifies the process. The Ministry of Interior allows CamDX to verify data of Khmer National ID cards. The Council for the Development of Cambodia (CDC) provides investment data. The Single Portal’s benefits are only eight working days needed to get business license/certificates, single data entry, and one-time payment for the registration fee.

Data Protection

There is no law or sub-degree on data protection and privacy in Cambodia yet. We can find only some legal references to data protection in various laws and sub-degrees. For instance, Section II of the Civil Code provides provisions on personal rights. The following are the definitions of some key terms.

- Concept of personal rights

Personal rights include the rights to life, personal safety, health, freedom, identity, dignity, privacy, and other personal benefits or interests.

- Right to an injunction

Where there is a danger of unlawful infringement of a personal right or a danger that such an infringement that has already occurred will unlawfully continue or be repeated, the personal right holder may demand to enjoin such infringement.

- Right to damage

The provisions of Articles 11 (Right to an injunction) and 12 (Right to demand elimination of the effect of an infringing act) shall not prevent a person who has suffered an infringement of a personal right from seeking damages for any harm sustained from such infringement in accordance with the provisions regarding tortious acts.

The Law on Telecommunications (Article 65) stipulates that subscribers shall have basic rights among others to "indemnity for damages caused by telecommunications operators and related person in case of the breach of contract." (adopted in 2015). The MPT ICT License (Article 27) states, "All ICT and Telecommunication operators and all relevant person must protect personal information, security, and strategy of using their ICT and Telecommunication System." (adopted in 2017). The draft Cybercrime Law (Article 10) states, "Service providers shall maintain the confidentiality of computer data and traffic data as stipulated in this law unless authorised by the court." Concerning Identify Theft on the Internet, Article 44 of the draft law states:

> Any person who intentionally uses without authorisation the name, photo, identity, sign or other personal identifying information (PII) of another person to create an online account, website, or email account or social media accounts with the intent to harm the interest of the owner; defraud or intimidate or threaten other; shall be punishable by a term of imprisonment from 1 (one) month to 3 (three) years and a fine from 1 million to 6 million Riels.

Also concerning the Identity Theft, Article 22 of the E-Commerce Law states, "No person shall use identity, record, electronic signature, electronic address, password, or particulars of other individuals dishonestly or without authorisation in commercial and non-commercial transactions in electronic systems." And on Data Protection, Article 32 reads:

1. Those who electronically store private information shall use all means to ensure that such information is safely protected at all reasonable circumstances in order to avoid the loss, access, use, modification, leakage, disclosure of such information, unless otherwise authorised by the information owners or other lawfully authorised parties.

2. The individuals shall not interfere in the electronic system, access, download, copy, extract, leak, delete or modify data stored by other persons in a dishonest manner and without authorisation.

The sub-degree on Digital Signature, adopted in 2017, aims to safely and efficiently manage and promote digital signature. Chapter 8 of the sub-degree provides conditions and rules regarding the violation of a digital signature. Article 32 states that keeping or using the password of others' digital signature without written permission from the holder of the digital signature faces punishment. The Ministry of Post and Telecommunications is the only Trust Service Provider (TSP). MPTC handles Root Certificate Authority and provides a license to Certificate Authority. Certificate Authority is an entity that issues digital certificates, public key certificates, and identity certificates. Digital Certificate is used to prove ownership of a public, includes key information, the owner's identity (subject), and the digital signature of the issuer (an entity that has verified certificate's contents). Root Certificate is a digital certificate that is identified the Root Certificate Authority. The digital signature must be issued by Certificate Authority or Retailing Agency, registered with MPTC as TSP.

E-Commerce

E-commerce in Cambodia has been remarkably developed over the past five years, but it is still at an early stage. In 2019, E-commerce shared 0.51% of GDP accounted for US$162.8 million, in which domestic e-commerce was at 6% (air ticket 90% and online shopping 10%) and cross-border e-commerce at 94% (electronic equipment 21.2%, tourism services 20.9%, online platform 16,9%, online shopping 7.6%, social network 6.7%, and others 26.7%) (Kong 2019). The number of online shopping users is small but growing.

With a rising middle class and young population, Cambodia has a huge potential in developing e-commerce. Currently, e-commerce in Cambodia is relatively limited compared with other ASEAN member countries. It is estimated that in 2020 there are about 7.8 million users. It is forecasted that by 2024, the number of users will reach more than 10 million. The key challenges are consumer's trust in the system, online payment gateways, consumer protection and service, as well as delivery services.

The Law on E-Commerce and the Consumer Protection Law adopted in 2019 are the most important legal instruments in facilitating and regulating e-commerce. The Law on E-Commerce has the following objectives:

- To determine the authenticity, accuracy and reliability of electronic forms.
- To promote the legal framework and business development to perform electronic commerce safely.
- To prevent and put a crackdown on the act causing damage to data and information systems.
- To eliminate obstacles that prevent electronic commerce performance and arise out of requirement uncertainty for written letters or signatures.
- To facilitate the filing of the documents via the electronic system with public institutions and promote the public institutions' effective service provision using reliable electronic records.
- To create rules, provisions and standards in connection with authenticity and accuracy of electronic records.

The laws have not been effectively enforced yet as some e-commerce operators operate without proper registration and compliance.

In August 2020, a sub-degree was issued for the implementation of the e-commerce law. The sub-degree applies natural persons, sole proprietorships, legal entities, and branches of foreign companies engaged in business activities via the electronic platform in Cambodia. Business activities that need to apply for a license are (1) e-commerce web services; (2) e-commerce platforms; (3) online shop services; (4) online auction services; and (5) other similar services provided through software or smart devices for e-commerce. Activities that need a permit are (1) business through electronic platform; and (2) use of social media or electronic platform for the supply, sale or purchase of goods and services. Activities that are not required to get license or permit are (1) booking services that do not require a deposit or payment by customers or consumers; (2) sales of goods or services with a turnover smaller than that of a small taxpayer (smaller than USD62,500); (3) sales of goods or services through family-owned or seasonal businesses; (4) sales of own artwork (goods or services); (5) private tutoring; (6) education on the national religion; (7) tutoring provided by associations or non-governmental organisations without earning profits, whether directly or indirectly, and activities or operations of state institutions in the provision of public services.

In November 2020, e-commerce strategy was launched to (a) enhance the business environment, regulatory framework and institutional coordination; (b) raise SME capabilities and improve public-private coordination and partnership; (c) strengthen domestic and cross-border logistics; (d) enhance ICT infrastructure, financial inclusion and digital literacy for e-commerce to growth in the hinterland; and (e) develop responsive skills-infrastructure for e-commerce. Regarding skill development, the strategy aims to reduce the skills-mismatch issues and improve digital entrepreneurship support for e-commerce start-ups, especially youth and women.

Digital Payments

The main constraints in Cambodia's financial sector include (1) limited financial inclusion due to the lack of reasonably priced credit in local currency and weak consumer protection mechanisms; (2) the need for a functional financial stability framework; and (3) weaknesses in key financial sector infrastructure relative to international norms and standards. Strengthening the legal framework and upgrading financial market infrastructure and systems for clearing, payments, and settlement are the priority reform areas that the government needs to carry out (ADB 2019, 4–5).

Digital payments in Cambodia have been improved significantly over the last three years. In 2019, digital payments through mobile apps accounted for about 10 per cent. The National Bank of Cambodia (NBC) has taken several measures to gradually build the foundation and strengthen the payment systems over the last decade. In 2008, the NBC issued a *Prakas* on cheque standard to make all cheques used in the banking system uniformed and standardised to ensure a smooth and efficient inter-bank clearing and settlement. In 2009, the National Clearing House's interim solution was introduced to assist data delivery in a fast and secure manner. In 2012, the NBC started the National Clearing System to clear checks and electronic payments faster and easier. In 2020, it launched Project Bakong Next Generation Payment System.

Project Bakong aims to address interconnectivity and interoperability across platforms of payment operators, attain efficiency in payment systems, promote financial inclusion and ease Khmer Riel cash payment. Financial inclusion is the primary objective of the NBC. One of the key measures to promote financial inclusion is to promote a cashless society where financial transactions, money transfer and mobile banking are accessible and affordable to every citizen. Bakong is peer-to-peer fund transfer service available to retail customers of local banks, financial institutions, and payment services providers in Cambodia. There have been so far 17 banking partners.

Although some process has been made, key challenges remain in the digital payment system including the low public trust in online transactions and fees. Social behaviour and perception need to be changed, and education and capacity building on financial literacy and competencies need to be enhanced. Promoting financial inclusion is a long-term effort, which requires multi-stakeholder engagement and partnership building-public-private-people partnership.

Digital Talent Base

STEM education in Cambodia remains at a nascent stage. Some of the main challenges and constraints are traditional teacher-centred approach, little integration of information and communication technology, obsolete content, poorly equipped libraries and laboratories, and compromised STEM programmes (CDRI 2019). Moreover, ICT professionals are limited. In

2015, the national government introduced the New Generation Schools (NGS) reform, intended to develop students' cognitive competencies in STEM (Science, Technology, Engineering, and Mathematics), ICT (Information and Communications Technology) and critical thinking.

The government has received capacity building support from various development partners on digital data governance. USAID implemented "development innovations" project, from 2013–2019, to help Cambodian CSOs, technology companies, social enterprises and young innovators design and use ICT solutions as well as employ innovative processes to tackle development challenges. Under the project, there are four services and programmes: Innovation Support Projects, Technology Coaching, ICT Solution Projects, Research and Toolkit.

In 2013, the Ministry of Post and Telecommunications created the National Institute of Post, Telecommunications, and Information Communication Technology (NIPTIC) to provide training programmes on Computer Science, Telecoms and Networking, E-Commerce, and research and development. There are three Centres, namely Tech Centre, Innovation Centre, and the Professional Training Centre. The Tech Centre's research focus is AI, Data Science, IoT, Cloud Computing, GovTech, EduTech, AgriTech, FinTech, and HealthTech.

In 2019, the Ministry of Economy and Finance established TECHO Start-up Centre to support start-ups to grow through capacity building, mentorship, networking, and financing. ICT solutions and innovation are the centre’s core training programmes. Several NGOs and social enterprises are providing technical support to Cambodian stakeholders in developing ICT solutions. For instance, Digital Divide Data (DDD), an international social enterprise, has offered capacity building and job opportunities to hundreds of local Cambodians. The Asia Foundation, an international organisation, has launched TEK4Good programme to provide an open co-working space for tech start-ups. There are several other capacity building programmes on digital technology and management.

Entrepreneurship

Entrepreneurship has been regarded as a key engine of growth. In 2006, the Ministry of Labour and Vocational Training established the National Institute of Entrepreneurship and Innovation to provide capacity building on entrepreneurship and innovation, small business development, start-ups development, ICT application in small business, and performance improvement for entrepreneurs.

In 2019, the Ministry of Economy and Finance found Khmer Enterprise (KE)- an implementing unit of Entrepreneurship Development Fund- to mobilise, invest and manage resources to support the development of a vibrant entrepreneurial ecosystem and to provide financial and non-financial support to related entrepreneurial ecosystem builders, including entrepreneurs, innovative start-ups, SMEs and partner institutions. In May 2020, the UNDP Cambodia and Khmer Enterprise launched a joint training programme on entrepreneurship development focusing on incubation, acceleration, and the sharing of best practices. The Ministry of Economy and Finance provides the fund for this programme under the Entrepreneurship Development Fund.

The government, together with financial institutions, launched SMEs Co-Financing Scheme in February 2020 to support small and medium enterprises by providing affordable and accessible financing, value-added services, and technical support to enhance SMEs' productivity. The scheme initially raised a combined $100 million, with $50 million coming from the SME Bank Cambodia and another $50 million from 33 financial institutions. The bank started operation in November 2020 to finance SMEs in key priority sectors, including food manufacturing and processing, manufacturing of local consumer goods, waste recycling, the production of goods for the tourism sector and making finished products, spare parts or assembling parts to supply other manufacturing, research and development associated with information and technology, as well as the supply of IT-based services and enterprises located in SME cluster zones and enterprise development in cluster zone.

The main challenges faced by entrepreneurs are a lack of capital, support networks, market access, technology, human capital, as well as digital literacy and skills. Corruption and lack of transparency and accountability remain the key issues need to be seriously addressed in order to improve business and investment climate in the country. In addition, special attention should be given to women entrepreneur development. According to the White Paper released by the Cambodia Women Entrepreneurs Association (CWEA) in 2020, it proposed two policy recommendations in addressing the challenges and constraints faced by women entrepreneurs. Firstly, creating a favourable environment for women entrepreneurs in getting access to information and knowledge. Secondly, promoting public awareness on gender equality and the elimination of false belief concerning gender issue.

Policy Recommendations

Policy coordination

Inter-agency and intra-agency coordination are critical in digital data governance. The Ministry of Post and Telecommunications, the leading agency in DDG, needs to create a platform or mechanism to promote dialogue between and among state agencies responsible for DDG. Currently, there are five ministries involving in DDG at varying degrees, namely the Ministry of Post and Telecommunications; Ministry of Economy and Finance; Ministry of Industry, Science, Technology and Innovation; Ministry of Commerce; and Ministry of Interior. A national Big Data Hub needs to be developed by the MPTC, and it will play a crucial role in integrating and sharing data at the national and sub-national levels so that a more coordinated and integrated digital data governance can be promoted, which in turn could promote good governance and accelerate an agile civil service in the digital era.

Digital transformation

Digital adoption and transformation have been identified as the key drivers for governance reforms and the economic operators to stay competitive and scale up their business. However, there is a lack of knowledge and human resources in adopting digital technology at both the public and private sectors. The government and the private sector can develop a roadmap on digital transformation, including smart manufacturing.

Technical specifications

Capacity building on DDG and digital transformation must strengthen the government's institutional and bureaucratic capacity, business development, and economic operators' management. More capacity support is needed for women entrepreneurs, especially in digital skills such as online business registration, e-commerce, online banking and outreach to stakeholders, as well as digital tools to access updated information and knowledge.

Legal framework

The legal frameworks on DDG are still lacking. Data protection and privacy laws are crucial in DDG. The future adoption of the cybercrime law, cybersecurity law, and National Internet Gateway will contribute to the development of regulatory regime on DDG.

Enforcing laws and regulations is another key issue. Therefore, improving transparency and accountability of the state agencies is crucial. The economic operators need to be informed and trained on the implications of the DDG-related laws and regulations on their business operations.

E-commerce

Capacity building on e-commerce is essential. Legal framework and policy on data protection and privacy are needed to create a conducive environment for e-commerce. It is paramount for Cambodia to adopt and maintain transparent and effective consumer protection measures and other measures conducive to the development of consumer confidence. Moreover, it also needs to adopt a legal framework that can ensure the protection of personal information of the users of e-commerce.

Human capital development

Cambodia needs to invest more resources in promoting digital skills and literacy; reskilling and upskilling for employment; and strengthening women entrepreneurship skills and digital competencies. The Cambodian government should work with development partners to develop training programmes for both trainers and trainees. The training modules should be tailored to local needs while addressing the skill gaps.

Supporting MSMEs

Capacity building on technology adoption among MSMEs is essential to enable MSMEs to access skills and knowledge, technology solutions, and expertise. In this respect, seeking large technology companies to provide digital skills and competencies for MSMEs can be one solution. Capacity needs assessment should be conducted to assess the state of digitalisation and skills gap among MSMEs before the training programmes commence. According to this preliminary survey, the key skills needed are online business registration, digital marketing, online communication, and product and service innovation.

Supporting digital entrepreneurship

Promoting digital entrepreneurship is crucial to enable and empower local entrepreneurs to develop themselves and their communities. Digital entrepreneurship refers to enterprises' development and advancement by embracing digital technology, including digital platforms, services, and tools.

Enhancing public-private partnerships

Public-private partnerships (PPPs) in science, technology, and innovation play a critical role in making research and innovation more agile and responsive to the fast-changing nature of technologies, society, and innovation. The public and private sectors in Cambodia should explore and build institutional partnerships to share the risk, reward, and responsibility for shared investments. The modalities of partnerships can include collaborative research programmes, innovation procurement, technology extension, and commercialisation programmes.

The opinions expressed are the author's own and do not reflect the views of the Asian Vision Institute.

References

Asian Development Bank (ADB). 2019. "Cambodia, 2019–2023 —Inclusive Pathways to a Competitive Economy." https://www.adb.org/sites/default/files/institutional-document/534691/cps-cam-2019-2023.pdf

2020. "Economic Indicators for Cambodia." https://www.adb.org/countries/cambodia/economy

Cambodian Development Resource Institute (CDRI). 2019. "Building STEM Literacy in Cambodian Higher Education." *Cambodia Development Review* 22(4). https://cdri.org.kh/wp-content/uploads/cdr18-4e-2.pdf

Im, Vutha. 2019. "Digital Connectivity in Cambodia. Telecommunication Regulator of Cambodia." https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2019/RRITP2019/ASP/Digital%20Connectivity%20in%20Cambodia.pdf

Kong, Mari. 2019. "Presentation on Digital Economy. Cambodia's Working Group on Digital Economy, Ministry of Economy and Finance." https://set.odi.org/wp-content/uploads/2019/11/Presentation-on-Concept-Note-of-DE.pdf

AVI COMMENTARY

ISSUE 2021, No. 02

Cambodia | 18th January 2021

Cambodia Goes Digital: Delivering Online Public Services via a Local Data Exchange Platform

KONG Marry[a]*, PhD*

On 15th June 2020, the Royal Government of Cambodia (RGC) officially launched the Cambodia Data Exchange platform (CamDX) and the online business registration platform which runs through it. This is an effort to ease the business registration process and create an attractive atmosphere for investments in the Kingdom of Cambodia. Not much later, to ease the travelling of foreign investors and businesspersons to the country, the RGC unveiled the online Validation Application on Payment Guarantee/Invitation (VAPGI), which also operates through CamDX in early August.

The online business registration and VAPGI services are the first two products that run through CamDX. Soon, more public services will join and take advantage of this local data exchange platform. As it is going digital, what does the adoption of digital government services mean for Cambodia in the 21st century?

What Drives CamDX?

In Cambodia, public service delivery almost always involves paper documents, which prove work inefficiency and prolong document processing. When the processing is inter-ministerial, citizens have to re-fill repetitive information on printed documents repeatedly. To complete one public service that involves multiple ministries, travelling from one ministry to another has become a norm for the general public.

[a] **H.E. KONG Marry** is an Under Secretary of State of the Ministry of Economy and Finance.

Inspired by the experience of Estonia’s X-Road, the move to build an in-house data exchange platform came as Cambodia’s response to the challenges posed by paper-based government services. CamDX allows multilateral data to be securely exchanged between governmental institutions based on six main principles: distribution, security, reliability, no data ownership, ease of use and heterogeneity. Instead of the movement of people from one ministry to another, CamDX emphasises the movement of data.

Case Study: Delivering Online Business Registration Service

The first online service operating through CamDX is the online business registration, which involves five institutions, namely, Ministry of Interior (MOI), Ministry of Commerce (MOC), General Department of Taxation (GDT), Ministry of Labour and Vocational Training (MLVT) and Council for the Development of Cambodia (CDC). The service is backed by Sub-Decree No. 84 S.E on Business Registration through Information Technology System.

Rather than involving multiple paper-based and semi-online application forms with different ministries, the whole registration process is now online in one single portal from filling in information to paying for the services. With a click of submission, the data will be sent to multiple ministries simultaneously via the local platform. Complete registration with MOC, GDT and MLVT takes only eight working days. Once each institution approves the application, the Single Portal issues digital certificates for the applicants without a face-to-face meeting. These digital certificates have legal value for which the companies can use. Additionally, the registration fee has also been reduced by 40%.

The provision of online customer service makes sure that every applicant has a seamless experience of the service. Despite the user-friendly and user-driven approach being used in the current system design, those who are not eloquent at technology may find online registration a challenge. A support taskforce made up of officials from all participating ministries has been created to assist the general public via hotline call, live chat, email and social network to ensure all applicants’ experience on the Single Portal is with minimal hiccups.

Almost six months after the launch, this online service has made significant progress. At the time of this writing, around 2,500 companies have been successfully registered with eight working days being the average duration to get an application approved by MOC, GDT and MLVT. Likewise, around 3,000 company names have been licensed via the platform. The total capital investment size is approximately six trillion riels, while the total size was only approximately two trillion riels in early October.

Offering a public service online comes with a price. With the experience for the online business registration, to digitalise a public service does not simply mean to put the service online. If the complexity of the service procedure remains, being online alone does not make much difference. As for the Single Portal for business registration, months were spent to understand the service's procedure and discuss inter-ministerially how it can be simplified. Without the compromise and mutual willingness of all institutions involved, the service would have been nowhere. This is an effort to reduce the processing time, cut down cost and encourage people to register their business digitally.

Yet, this price is worth spending for. Digitalising business registration service brings much more than a lower fee, shorter processing time and more simplified procedure. Since all payments are made online and no face-to-face meeting between officers and applicants is involved, the Single Portal brings greater transparency to the public service. Applicants no longer need to spend time and money to travel from one place to another, resulting in better accessibility and work efficiency. With a high risk of infection resulting from handlings of physical documents and in-person meeting during the COVID-19 pandemic, digitalisation becomes the go-to solution.

Conclusion

Cambodia's digital transformation comes with struggles and rewards. Investment in time and effort has been tremendous to ensure that business registration can go online with efficiency and effectiveness and that CamDX can be utilised to its fullest capacity. As a result of this investment, Cambodia has achieved a faster online service with a cheaper fee, more simplified procedure, greater transparency and better accessibility. During the challenging period of the COVID-19 pandemic, digital transformation becomes the most suitable solution – making it easier for both service providers and service receivers and reducing the risk of infection from physical meeting and paper documents. It should be understood that today's investment is a commitment to a better tomorrow. Hence, digitalisation should not be an option, but a fundamental step to adapt to a new digital society and catch up with global trends.

The views expressed are the author's own and do not reflect the views of the Asian Vision Institute.

AVI POLICY BRIEF

ISSUE 2019, No. 16

Cambodia | 22nd December 2019

ICT Policy and Regulations: How Cambodia can Learn from India

TRIPATHI Geeta[a]

Executive Summary

- Emerging Information and Communication Technologies (ICT) such as Artificial Intelligence (AI), Internet of Things (IoT), and Cloud Computing are major drivers for maximizing productivity across all fields.

- With a forward-looking government and entrepreneurial youth, Cambodia will develop higher quality information infrastructure, a technically skilled workforce, and spread digital literacy to their citizens at all levels, crucial for bridging the digital divide between rural and urban areas.

- Cambodia can learn from India's ICT development policy frameworks, to transform into a knowledge economy. The ICT sector enabled India to emerge from several economic challenges, while simultaneously building one of the largest and most skilled digital workforces internationally.

- This paper will highlight the aforementioned policies and achievements of India, while providing cooperation opportunities for Cambodia to build its ICT workforce and infrastructure, along with the policies and regulations required for support.

[a] **TRIPATHI Geeta** is a Research Fellow at the Centre for Inclusive Digital Economy (CIDE) at the Asian Vision Institute (AVI).

សេចក្ដីសង្ខេបអត្ថបទ

- បច្ចេកវិទ្យាទំនាក់ទំនងនិងព័ត៌មានដែលកំពុងផុសឡើងដូចជា បញ្ញាសិប្បនិម្មិត អាយអូធី និងការគណនាក្នុងលំហជាកត្តាជំរុញចំបងសំរាប់ផលិតភាពអតិបរមារាល់គ្រប់វិស័យ។
- ដោយមានរដ្ឋាភិបាលដែលមើលទៅមុខ និងយុវជនដែលមានសហគ្រិនភាព កម្ពុជានឹងបង្កើតហេដ្ឋារចនាសម្ព័ន្ធដែលមានគុណភាពខ្ពស់ កំលាំងពលកម្មដែលមានជំនាញបច្ចេកទេស និងចំនេះដឹងឌីជីថលដែលសាយភាយទៅពលរដ្ឋគ្រប់លំដាប់ថ្នាក់ សារៈសំខាន់ក្នុងការភ្ជាប់បំណែងចែកឌីជីថលរវាងជនបទនិងទីក្រុង។
- កម្ពុជាអាចរៀនពីឥណ្ឌាស្ដីពីក្របខ័ណ្ឌបង្កើតគោលនយោបាយបច្ចេកវិទ្យាទំនាក់ទំនងនិងព័ត៌មានដើម្បីប្រែក្លាយទៅជាសេដ្ឋកិច្ចចំណេះដឹង។
- វិស័យបច្ចេកវិទ្យាទំនាក់ទំនងនិងព័ត៌មាន បណ្ដាលឲ្យឥណ្ឌាស្ទុះឡើងពីបញ្ហាប្រឈមសេដ្ឋកិច្ចមួយចំនួន ក៏ដូចជាការផ្ដល់ព្រមគ្នាមួយ ក្នុងកម្រិតធំបំផុត និងកំលាំងពលកម្មដែលមានកម្រិតជំនាញបច្ចេកទេសខ្លាំងក្នុងកម្រិតអន្តរជាតិ។ អត្ថបទនេះនឹងរំលេចពីសមិទ្ធិល និងគោលនយោបាយដែលបានលើកឡើងរបស់ឥណ្ឌា ក៏ដូចជាផ្ដល់ឱកាសទំនាក់ទំនងសំរាប់កម្ពុជា ដើម្បីបង្កើតហេដ្ឋារចនាសម្ព័ន្ធ និងកំលាំងពលកម្ម លើវិស័យច្ចេកវិទ្យាទំនាក់ទំនងនិងព័ត៌មាន ដោយមានការគាំទ្រពីគោលនយោបាយនិងបទប្បញ្ញត្តិ។

Introduction

The rapid growth of technology and its adaptations by several nations over the last 30 years with Information and Communications Technology (ICT) has brought the world closer together. Over the years, ICT has been one of the enablers for India's growth story, making it digitally empowered with better standards of living and giving it an advantageous position in the service sector accessible to the global economy. The concurrent increases in its ICT talent pool have also propelled their industry into becoming a major player both at the domestic and international level, adopting a growing role for ICT development in the ASEAN region. In recent times, India has also embarked on its collaboration in ICT development with Cambodia, which is the fastest growing economy in the ASEAN region. Cambodia is taking several steps towards Industry 4.0 and working towards its digital transformation, as a long-term vision for the future development and prosperity of its people.

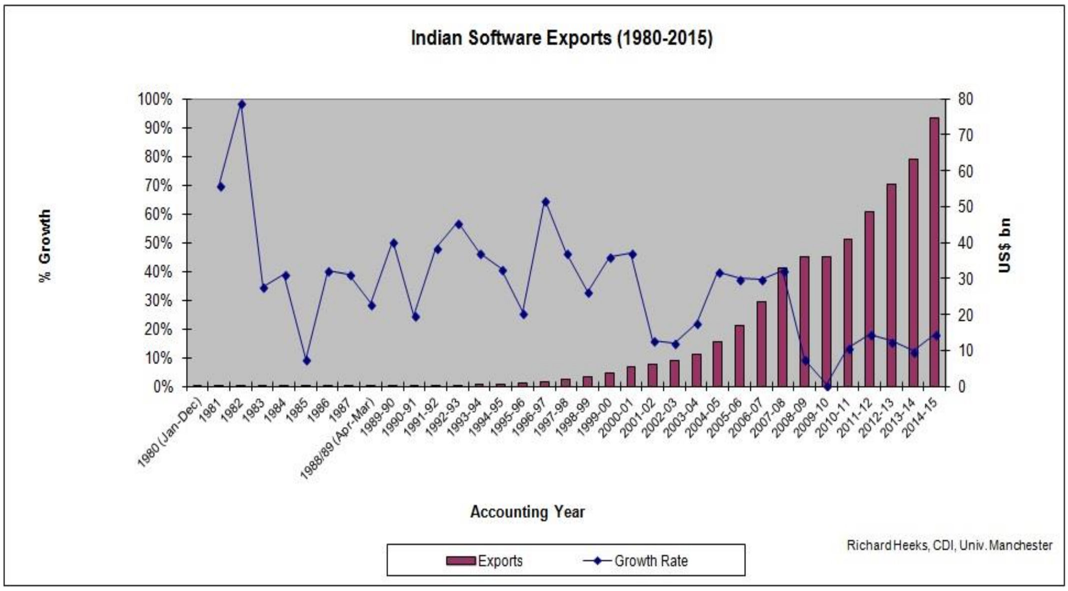
The Memorandum of Understanding (MOU) between India and Cambodia includes broad areas of cooperation such as ICT policy, spectrum management, ICT application for disaster management, cybersecurity and incident response. A separate MOU has also been signed between the Centre for the Development of Telematics (C-DOT), a leading research institution in India and Telecom Cambodia, which will address the deployment of advanced telecommunications technology and wireless solutions in rural areas. This also includes the creation of Smart Villages in the Kingdom. The National Informatics Centre (NIC) in India is developing e-governance applications, also establishing a Joint Working Group (JWG) with Cambodia. Parallely, the Ministry of Electronics & IT (MeitY) of the Government of India has also set up a sustainable IT Infrastructure for Advanced IT Training using conventional and virtual classrooms, and e-learning technologies in Phnom Penh. India is also offering opportunities for doing Doctoral Programs with premier institutes such as the Indian Institutes of Technology for Cambodian engineers. As India and Cambodia are collaborating in various areas, the ICT development story of India can be examined by Cambodian policymakers for helping its sustainable growth towards a digital economy.

India's Policy Initiatives and Evolution of ICT Sector

The ICT growth story in India gained its visibility starting from 1986 with the establishment of C-DOT that revolutionized Public Call Office (PCO) in the rural areas and then MTNL (Mahan agar Telephone Nigam Limited), helping the spread of telecommunications networks.

Computerization was introduced by reducing taxes and tariffs for computers, telecommunications, and the modernization of railways. The National Policy of Education was also announced to modernize education and expand higher education in India with the setup of rural education. The Centre for Development of Advanced Computing (C-DAC) was also established with its first High Performance Computing (HPC) mission in 1988 and the subsequent delivery of the PARAM series of supercomputers. C-DAC has been a frontrunner in the ICT revolution of India and has core competencies towards research and development in several ICT domains and is working towards several initiatives today in the ASEAN region. This was followed by the economic liberalization in 1991. The size of the Indian IT and IT-enabled service industry grew from USD 100 million to USD 1 billion, from the beginning to the end of the 1990s. Software Technology Parks were established, where the industry embraced the quality movement — first with ISO 9001, an international standard for quality management systems, and then with the Software Engineering Institute – Capability Maturity Model (SEI-CMM). By 1999, 50% of the SEI-CMM Level 5 organizations in the world were from India. Indian IT majors were listed on Indian and global business indexes all at the same time. With liberal policies introduced in India, multinational corporations (MNCs) such as IBM and GE set up their large-scale offshore development projects in the country. The Y2K framework, transitioning from the year 1999 to 2000, opened up huge opportunities for Indian ICT professionals, as the predominant knowledge force in the global IT space and since then, there has been no looking back. This was further enhanced with the rise of the telecommunications sector with major players like Bharti Airtel, Reliance, and other private players like Vodafone entering into the Indian market, who are currently catering to more than 90% of the mobile subscriber base, making it the largest market for mobile applications and devices. To date, India is also a major exporter of software products and has shown significant growth according to the statistics mentioned below, under the FY 1980-2015 and FY 2018:

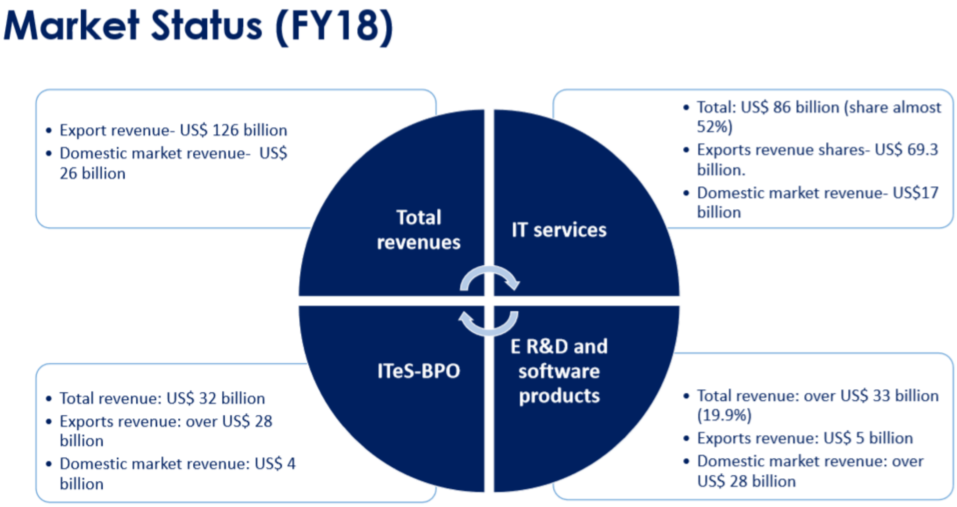
(a)



Richard Heeks, CDI, Univ. Manchester

And the current growth status as represented below:

(b)



Market Status (FY18)

Total revenues

- Export revenue- US$ 126 billion
- Domestic market revenue- US$ 26 billion

IT services

- Total: US$ 86 billion (share almost 52%)
- Exports revenue shares- US$ 69.3 billion.
- Domestic market revenue- US$17 billion

ITeS-BPO

- Total revenue: US$ 32 billion
- Exports revenue: over US$ 28 billion
- Domestic market revenue: US$ 4 billion

E R&D and software products

- Total revenue: over US$ 33 billion (19.9%)
- Exports revenue: US$ 5 billion
- Domestic market revenue: over US$ 28 billion

Figure 1: Indian Software Exports a Growth Story

To promote innovation and entrepreneurship, the National Knowledge Network (NKN) was established in 2009. This high-speed fibre optic network established an interconnection of around 30,000 to 40,000 educational and research institutes, including global research networks in the US, EU, Singapore and Japan. The goal is to enable real time collaboration and research. Currently, around 1606 institutes that are connected via the NKN. The other initiatives for public infrastructure include the National Optic Fibre Network (NOFN) connecting 625,000 villages to improve telecommunications in India connecting 245,000 villages. Cambodian educational and research institutes can also be part of this network for building its human resource and technical capacity.

India-Cambodia Cooperation for Digital Transformation

As part of striving for inclusive development by Cambodian policymakers, they can examine policies and programmes under the umbrella of Digital India for key initiatives on digital ID like Aaadhaar, digital payment via Aaadhaar-based Direct Benefit Transfer, and the digital delivery of services, providing access to government services at the doorstep of citizens through the Common Services Centres. Harnessing the benefit of Cloud Computing with an ambitious initiative - GI Cloud Meghraj could accelerate the delivery of e-services in the country, while optimizing ICT spending of the government. Cambodia can also work with the Centres of Excellence (COEs) for applications of Internet of Things (IoT) in agriculture, medical devices, financial technology and cybersecurity solutions, as initiatives by the Government of India via NKN to initiate research collaboration. Some other initiatives under the National Policy of Electronics involve creating an ecosystem for the manufacturing of electronic products. These initiatives in the year 2014 has led India to be the 2nd largest manufacturer of mobiles in the world, while also building human capacity through Skill India programs. Envisaging the importance of Artificial Intelligence (AI) as part of the National Policy of Software Products 2019, a national centre on AI, along with COEs being established. These COEs are also being supported under the various Startup India initiatives, also for which Cambodia can collaborate with its current opportunities for the ICT Development Program 2050 and entrepreneurship programmes that promote young leaders in the nation.

Policy Options: Accelerating ICT Growth in Cambodia

ICT has played a vital role towards India’s digital revolution and growth as a knowledge economy. Over the years with several government awareness programmes, opportunities (this also includes FDI models for ease of business) have been created for improving the ICT infrastructure in the country. This has rapidly reduced the digital gap between urban and rural

India making it now the second largest internet user in the world. This has led to growth of its ICT industry and high demand for a skilled ICT workforce, under several *skill development* initiatives creating employment opportunities at both a domestic and global level, with India's huge talent pool of ICT professionals. With better government delivery services through *e-governance* initiatives for its citizens at both centre and state level, India also improved in GDP per capita income and continues to show progress in improving its HDI, Human Development Index. The Kingdom of Cambodia as part of the ASEAN region, is also growing as a knowledge economy and is showing similar potential to India with its enthusiastic and talented young professionals and brilliant students, who are currently pursuing their professional degrees in ICT subjects in local and international universities. It is recommended to pursue several initiatives parallelly, which will be required where Cambodia can establish COEs, with the Institutes of National Importance (INI) to carry out innovation and identify requirements related to the e-governance deliverables for citizens of different provinces. In addition, it will be key to identify ICT infrastructure requirements, the related power generation, and distribution needs for these provinces in Cambodia. As India and Cambodia have already started their cooperation for ICT Development in Cambodia, a Joint Working Group (JWG) can be formulated to expand its cooperation and development with specific sectors of ICT, creating opportunities and boosting Industry to Industry collaboration between India and Cambodia, and their respective ICT workforces. The proposed COEs, including schools in remote provinces of Cambodia, can be connected via satellite with the National Knowledge Network (NKN) for human capacity building and academic collaboration in ICT education and research, as part of an exchange programme with India. New ICT schemes will be formulated in the Cambodia-India JWG, which will give opportunities for the Cambodian ICT workforce and industry to create its demand at domestic and global levels, enabling Cambodia to develop a sustainable digital economy at an international standard.

The opinions expressed are the author's own and do not reflect the views of the Asian Vision Institute.

AVI POLICY BRIEF

ISSUE 2019, No. 14

Cambodia | 25th November 2019

Steps to Develop a National Cybersecurity Strategy

HENG Pheakdey[a], PhD

Executive Summary

- Information and Communication Technologies (ICTs) are the catalysts for economic and social transformation. However, the economy and society are becoming more vulnerable to cyberthreats and cyberattacks.

- To fully realise the promises of ICTS, the national government needs to develop and implement cybersecurity strategy. Here are five suggested steps: initiation, situational analysis and risk assessment, strategy drafting, implementation plan, and monitoring and evaluation plan.

- International norms for cyberspace need to be implemented at a national level. Policymakers must therefore keep the goals of international norms in mind when developing their national cybersecurity strategy and associated policies.

[a] **HENG Pheakdey** is an Advisor to the Asian Vision Institute and Founder and Chairman of the Enrich Institute.

សេចក្តីសង្ខេបអត្ថបទ

- បច្ចេកវិទ្យាព័ត៌មាន និងគមនាគមន៍ (ICTs) គឺជាកាតាលីករជំរុញការផ្លាស់ប្តូរសេដ្ឋកិច្ច និងសង្គម។ ប៉ុន្តែទោះជាយ៉ាងនេះក្តី ប្រព័ន្ធសេដ្ឋកិច្ច និងសង្គម កំពុងកាន់តែងាយនឹងទទួលរងគ្រោះពីការគម្រាមកំហែង ក៏ដូចជាការវាយប្រហារតាមប្រព័ន្ធ Cyber។
- ដើម្បីទាញយកអត្ថប្រយោជន៍អោយបានពេញលេញពីវិស័យ ICTs នេះ រដ្ឋាភិបាលថ្នាក់ជាតិចាំបាច់ត្រូវធ្វើការអភិវឌ្ឍ និងអនុវត្តនូវយុទ្ធសាស្ត្រសន្តិសុខ Cyber (Cybersecurity Strategy)។ ហើយនេះគឺជាជំហានទាំង ៥ ដែលរដ្ឋាភិបាលអាចធ្វើការពិចារណាក្នុងការអនុវត្ត គឺ៖ (១) កិច្ចផ្តួចផ្តើម (២) ការវិភាគអំពីស្ថានការណ៍ និងការវាយតម្លៃទៅលើហានិភ័យ (៣) ការតាក់តែងសេចក្តីព្រៀងយុទ្ធសាស្ត្រ (៤) ផែនការអនុវត្ត និង(៥) ផែនការត្រួតពិនិត្យ និងវាយតម្លៃ។
- បទដ្ឋានអន្តរជាតិសម្រាប់លំហ Cyber (cyberspace) ចាំបាច់ត្រូវតែអនុវត្តនៅកម្រិតថ្នាក់ជាតិ។ ដោយហេតុផលនេះ អ្នកបង្កើតគោលនយោបាយចាំបាច់ត្រូវរក្សាឲ្យបាននូវគោលដៅនៃបទដ្ឋានអន្តរជាតិទាំងនោះ ខណៈពេលដែលពួកគាត់អភិវឌ្ឍបង្កើតយុទ្ធសាស្ត្រសន្តិសុខ Cyber រួមទាំងគោលនយោបាយពាក់ព័ន្ធនានា។

Introduction

Undoubtedly, Information and Communication Technologies (ICTs) have significantly transformed the way we work and live. The internet, for example, has become the foundation of modern business, vital services and infrastructure, social networks and the global economy as a whole.

Our economies get more and more dependent on digital infrastructure, but technology remains inherently vulnerable. The confidentiality, integrity and availability of ICT infrastructure are being threatened by rapidly evolving cyberthreats, including electronic fraud, theft of intellectual property and personal identifiable information, disruption of services, and loss or destruction of property.

The transformational potential of ICTs and the Internet as a catalyst for economic growth and social development is at a critical juncture where national confidence and faith in the use of ICTs are being eroded by cyber insecurity.

To fully realize the promises of technology, governments must match their national economic goals with their national security objectives. If the security risks associated with the proliferation of ICT-enabled networks and internet technologies are not properly balanced with robust national cyber security policies and resilience measures, countries will neither be able to achieve economic growth nor meet their national security goals.

That is why developing and implementing a National Cybersecurity Strategy is critical for a nation to improve the security of its digital infrastructure, which will ultimately contribute to its broader socio-economic aspirations. This paper aims to provide important steps that a country can follow in order to draft an effective national cybersecurity strategy.

The Benefits of Developing a National Cybersecurity Strategy

A national cybersecurity strategy is a plan of actions designed to improve the security and resilience of national infrastructures and services. It is a high-level top-down approach to cybersecurity, which establishes a range of national objectives and priorities that should be achieved in a specific timeframe.

Such a strategy is vital for managing national-level cybersecurity risks and for developing appropriate regulations to support those efforts. Developing vision, goals and priorities allows policymakers to look at cyber security in a holistic way through a national digital ecosystem, rather than at a specific sector, goal, or threat. Thus, it enables them to be dynamically strategic. Priorities for national cybersecurity policies vary by countries. Therefore, while the priority of one country may be on mitigating critical infrastructure threats, others may focus on defending intellectual property, cultivating confidence in the online environment, or improving public understanding of cyber security. Others may focus on a mixture of these things.

Having a strong national cybersecurity strategy also helps to promote private sector growth and create a more competitive business environment. E-commerce, for example, will grow due to a more secure digital environment, which will in turn allow more competition bringing huge benefits to the consumers. Such a strategy also plays a critical role in drawing foreign investment. With the prevalence of intellectual property on the on-line domain today, businesses want to ensure that they will be able to protect their assets if they come under any attack.

Steps to Develop a National Cybersecurity Strategy

This section outlines five recommended phases to develop an effective national cybersecurity strategy.

Phase 1: Initiation

The initiation phase provides the foundation for an efficient strategy drafting process. This step focuses on the procedures, timelines and identification of key stakeholders that should be involved in the development of the strategy.

Selecting a champion is a critical first step in this phase. The strategy development process should be coordinated by a single, competent authority which will then appoint an individual to be responsible and accountable for leading the overall project. If no such authority exists, consider setting up a national cybersecurity agency. The agency should be supported by a steering committee whose main role is to provide guidance and ensure the quality of the work. Details about the roles, establishment and membership of the steering committee should be clearly defined from the outset.

In addition to the steering committee, a broad advisory committee comprising of diverse relevant stakeholders should also be formed, and the members should be engaged to contribute to the process. The stakeholders may include ICT companies, critical-infrastructure operators, academic experts, and non-governmental organizations working on raising cybersecurity awareness and preparedness, amongst others.

Once the various institutional arrangements are put in place, the Project Lead shall draft a plan for developing the National Cybersecurity Strategy, which will be reviewed and approved by the Steering Committee. The Strategy development plan should lay out major steps and activities, key stakeholders, timelines and resource requirements. It should specify how and when relevant stakeholders will be expected to participate in the development process to contribute input and feedback. It should also identify human and financial resources needed, and where these could be procured. Particular attention should be placed on securing long-term funding for the full lifecycle of the project, including its development, implementation and refinement.

Phase 2: Situational Analysis and Risk Assessment

In order to be effective, the National Cybersecurity Strategy needs to reflect the country's current cybersecurity circumstances. To this end, an evaluation of the country's current cybersecurity strengths and weaknesses should be undertaken, and relevant materials should be consulted in collaboration with relevant stakeholders across government, private sector and civil society.

Part of this analysis may include the identification of assets and services critical to the proper functioning of the society and economy, and the mapping of existing national laws, regulations, policies, programs and institutions related to cyber security.

Data on existing national cybersecurity programs, regional and international initiatives, private sector projects, ICT and cyber-education and skill-development programs, and digital R&D activities should be collected. Other data that should also be collected for analysis include statistics on Internet penetration, ICT adoption, and technology development; and perspectives on potential ICT and cybersecurity patterns and challenges.

Built on the collected information, an assessment of risks facing the nation related to digital dependency must be conducted. This can be accomplished through defining national digital assets, both public and private, their interdependencies, vulnerabilities and risks, and assessing the probability and potential impact in an event of a cyberattack.

Phase 3: Strategy Drafting

Based on the situational analysis and risk assessment, the Project Lead, in collaboration with the Steering Committee, should initiate the drafting of the Strategy. Dedicated working groups could be created either to focus on specific topics or to draft different sections of the strategy.

The strategy will set out the overall direction for cyber security for the country; express a clear vision and scope; set goals to be accomplished within a specific timeframe; and prioritise them in terms of impact on society, the economy and infrastructure.

The strategy also needs to determine the mandates of the various entities responsible for implementing and establishing cybersecurity policies and regulations within the state. In particular, it should identify the roles and duties of the agencies responsible for collecting intelligence on risks or vulnerabilities, reacting to security attacks, and improving preparedness and handling emergencies.

To ensure that the final strategy is based on a shared vision, the draft strategy should be disseminated across a large stakeholder community, not only restricted to those who engaged in the development process. External feedback can be collected through a variety of engagement mechanisms, including online consultation, validation workshops, and additional working groups.

Phase 4: Implementation Plan

Once the strategy is finalised and approved by the government, an action plan shall be developed to implement it. The National Cybersecurity Strategy outlines the goals and the results the nation wishes to achieve across the different focus areas. The action plan should identify specific programs within each focus area that will help to achieve such goals. These could include planning cybersecurity drills, establishing safety guidelines for critical infrastructure, and creating an incident management system, among others.

While the development of the strategy shall be led by a single authority, its implementation cannot be the sole responsibility of one entity alone. Instead, it requires engagements and coordination with a range of different stakeholders across the government, as well as support from civil society and the private sector. Therefore, when priority projects have been identified, specific government entities are then selected as owners of each of the initiatives. These government entities would be responsible and accountable for the execution of each particular program delegated to them, and they are required to coordinate their efforts with other relevant stakeholders during the implementation process.

In assigning the initiatives to different institutions, it is important to understand their respective mandates, capacity and resources. When required, support must be provided to help project owners to identify and secure the required resources in accordance with administrative financial structures of the country.

Another critical element of the Action Plan is the design of common criteria and key performance indicators that measure each of the actions being implemented. Clear deadlines for implementation should also be defined. These indicators and timeframe will facilitate the evaluation of the success of the initiatives during and after their implementation.

Phase 5: Monitoring and Evaluation Plan

To ensure successful monitoring and evaluation of the execution of the strategy, the government will need to create an independent entity accountable for tracking and reviewing the progress and challenges of the implementation.

The establishment of baseline metrics and key performance indicators (KPI) by near-term, mid-term and long-term objectives helps reinforce the governance and management mechanisms. Continuous reviews of the implementation plan (i.e. what is going well and what is not going well) help inform the strategy. Good governance frameworks for execution of the plan should also clearly define accountability and responsibility for ensuring successful implementation.

This approach will ensure that the relevant stakeholders are held accountable to the commitments set. It will also ensure that any obstacles in the execution are recognised or detected early on. It will thus allow the government either to correct the situation or to change its plans accordingly on the basis of the lessons learned in the implementation process.

Conclusion

Developing a holistic cybersecurity strategy is critical for a nation to prevent and respond to cyber risks in our increasingly interconnected world. This paper has outlined five basic steps for policymakers to consider in developing their country's national cybersecurity strategy. It should be noted that a country's national policies shall enable that country to collaborate effectively with international partners and to design and comply with existing international obligations. To be truly effective, international norms for cyberspace will need to be implemented at the national level. Policymakers must therefore keep the goals of international norms in mind when developing their national cybersecurity strategy and associated policies.

The opinions expressed are the author's own and do not reflect the views of the Asian Vision Institute.

Definition of useful cybersecurity terms

Access Control Mechanism: Security measures designed to detect and deny unauthorized access and permit authorized access to an information system or a physical facility.

Active Attack: An actual assault perpetrated by an intentional threat source that attempts to alter a system, its resources, its data, or its operations.

Advanced Persistent Threat: An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception).

Critical Infrastructure: The systems and assets, whether physical or virtual, so vital to society that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters.

Cyber Exercise: A planned event during which an organization simulates a cyber disruption to develop or test capabilities such as preventing, detecting, mitigating, responding to or recovering from the disruption.

Cybersecurity: The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.

Cyberspace: The interdependent network of information technology infrastructures, that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Data Integrity: The property that data is complete, intact, and trusted and has not been modified or destroyed in an unauthorized or accidental manner.

Digital Forensics: The processes and specialized techniques for gathering, retaining, and analysing system-related data (digital evidence) for investigative purposes.

Distributed Denial of Service: A denial of service technique that uses numerous systems to perform the attack simultaneously.

Dynamic Attack Surface: The automated, on-the-fly changes of an information system's characteristics to thwart actions of an adversary.

Enterprise Risk Management: A comprehensive approach to risk management that engages people, processes, and systems across an organization to improve the quality of decision making for managing risks that may hinder an organization’s ability to achieve its objectives.

Information and Communication(s) Technology: Any information technology, equipment, or interconnected system or subsystem of equipment that processes, transmits, receives, or interchanges data or information.

Information System Resilience: The ability of an information system to: (1) continue to operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (2) recover effectively in a timely manner.

Interoperability: The ability of two or more systems or components to exchange information and to use the information that has been exchanged.

Passive Attack: An actual assault perpetrated by an intentional threat source that attempts to learn or make use of information from a system, but does not attempt to alter the system, its resources, its data, or its operations.

Red Team: A group authorized and organized to emulate a potential adversary’s attack or exploitation capabilities against an enterprise’s cybersecurity posture.

Red Team Exercise: An exercise, reflecting real-world conditions, that is conducted as a simulated attempt by an adversary to attack or exploit vulnerabilities in an enterprise's information systems.

Situational Awareness: Comprehending information about the current and developing security posture and risks, based on information gathered, observation and analysis, and knowledge or experience.

Spoofing: Faking the sending address of a transmission to gain illegal [unauthorized] entry into a secure system.

System Integrity: The attribute of an information system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Traffic Light Protocol: A set of designations employing four colors (RED, AMBER, GREEN, and WHITE) used to ensure that sensitive information is shared with the correct audience.

Vulnerability: A characteristic or specific weakness that renders an organization or asset (such as information or an information system) open to exploitation by a given threat or susceptible to a given hazard.

AVI PERSPECTIVE

ISSUE 2022, No. 01

Cambodia | 15th February 2022

Cybersecurity Legislation: Policy Instrument to Improve Cybersecurity Readiness and Resilience

SANG Sinawong[a]*, PhD*
KONG Phallack[b]*, LLM, LLB, & DDS*
OU Phannarith[c]*, MBA*
CHHEM Siriwat[d]*, Master in Digital Technology Management*

Executive Summary

- ❖ Advancements in digital technology applications, coupled with high digital adoption rates, have resulted in increased interconnectivity and more efficient communication – ultimately boosting the economy and benefitting the society in Cambodia. However, increased digital adoption and interconnectivity correspondingly lead to more potential cybersecurity risks.
- ❖ Cambodia may learn from cybersecurity resolutions of international organisations and cybersecurity laws of established nations in ASEAN, Asia, and beyond to reinforce national cybersecurity legislation as a policy instrument to improve cybersecurity readiness and resilience for the government, companies, organisations, and individuals.
- ❖ The key factor for cybersecurity legislation in Cambodia should be to establish a compliance regime to raise the safety and security bar, to strengthen and improve the cybersecurity resilience of Critical Information Infrastructure (CII) sectors – which are related to national security, the economy, and society. These essential services provided

[a] **SANG Sinawong** is Advisor to the Centre for Inclusive Digital Economy (CIDE) at the Asian Vision Institute (AVI).
[b] **KONG Phallack** is a Professor and Attorney at Law.
[c] **OU Phannarith** is Professor of Cybersecurity, Research Fellow at CIDE, Top ASEAN CSO30 and Top 100 Global CISO.
[d] **CHHEM Siriwat** is Director of CIDE, AVI.

by governments and firms, used by citizens, all rely on the communication and storage of essential or confidential information. As such, CIIs must be protected in order to maintain the effective operation of a nation.

សេចក្តីសង្ខេបអត្ថបទ

- ភាពជឿនលឿនរួមជាមួយនឹងអត្រាភាគរយខ្ពស់នៃការប្រើប្រាស់បច្ចេកវិទ្យាឌីជីថល បានធ្វើឲ្យមានការកើនឡើងនូវការប្រាស្រ័យទាក់ទងគ្នាទៅវិញទៅមក និងមានប្រសិទ្ធភាពជាងមុន ហើយបានជំរុញឲ្យមានការកើនឡើងនៃសេដ្ឋកិច្ច និងបានផ្តល់អត្ថប្រយោជន៍ដល់សង្គមកម្ពុជាផងដែរ។ ក៏ប៉ុន្តែការកើនឡើងនៃការប្រើប្រាស់បច្ចេកវិទ្យាឌីជីថល និងការប្រាស្រ័យទាក់ទងគ្នាទៅវិញទៅមកនេះ អាចនាំមកនូវហានិភ័យកាន់តែច្រើនទាក់ទងនឹងសន្តិសុខសាយប័រ។
- កម្ពុជាអាចសិក្សាទៅលើដំណោះស្រាយសន្តិសុខសាយប័ររបស់អង្គការអន្តរជាតិ និងច្បាប់សន្តិសុខសាយប័រដែលបង្កើតឡើងដោយប្រទេសជាសមាជិកអាស៊ាន បណ្តាប្រទេសនៅតំបន់អាស៊ី និងតំបន់ផ្សេងៗទៀត ដើម្បីរៀបចំ និងប្រែក្លាយច្បាប់សន្តិសុខសាយប័ររបស់ខ្លួនទៅជាឧបករណ៍គោលនយោបាយមួយ ក្នុងការធ្វើឱ្យប្រសើរឡើងនូវភាពរួចរាល់ និងភាពធនផ្នែកសន្តិសុខសាយប័រសម្រាប់រដ្ឋាភិបាល ក្រុមហ៊ុន អង្គភាព និងបុគ្គល។
- កត្តាសំខាន់សម្រាប់ច្បាប់សន្តិសុខសាយប័រនៅកម្ពុជា គួរពិនិត្យលើការបង្កើតរបបអនុលោមភាព ដើម្បីបង្កើនសុវត្ថិភាព និងសន្តិសុខ ក្នុងគោលបំណងពង្រឹង និងកែលម្អភាពធន់សន្តិសុខសាយប័រនៃហេដ្ឋារចនាសម្ព័ន្ធព័ត៌មានសំខាន់ៗ (CII) ដែលទាក់ទងនឹងសន្តិសុខជាតិ សេដ្ឋកិច្ច និងសង្គម។ សេវាសារវន្តសំខាន់ៗទាំងនេះដែលផ្តល់ដោយរដ្ឋាភិបាល និងក្រុមហ៊ុននានា ហើយដែលត្រូវបានប្រើប្រាស់ដោយប្រជាពលរដ្ឋ គឺពឹងផ្អែកភាគច្រើនទៅលើការតភ្ជាប់ទំនាក់ទំនង និងការរក្សាទុកនូវព័ត៌មានសំខាន់ៗ និងសំងាត់។ ហេតុដូច្នេះហើយ CII ត្រូវតែទទួលបានការការពារ ដើម្បីរក្សាបាននូវប្រសិទ្ធិភាពនៃប្រតិបត្តិការរបស់ប្រទេសមួយ៕

Introduction

Rapid digital technological developments and the Fourth Industrial Revolution are prompting governments around the world, including the Royal Government of Cambodia (RGC), to optimise and modernise current Information and Communications Technology (ICT) systems by adopting new digital technologies such as the Internet of Things (IoTs), cloud computing, big data analytics, and Artificial Intelligence (AI). The advancement of new digital technologies has transformed the delivery of government services, business operations, and communication – from traditional methods to modern digital platforms.

However, this adoption and advancement of digital technologies have created new opportunities for criminals to exploit online vulnerabilities and attack countries' Critical Information Infrastructure (CII). Governments, firms, and individuals increasingly rely on information stored and transmitted over advanced communication networks. The costs associated with cyberattacks are significant – in terms of revenue loss, the breaching of sensitive data, damage to equipment, denial-of-service attacks, and network outages. The future growth and potential of the online information society are in danger from growing cyber threats (Schjølberg 2008). Consequently, the aforementioned threats have reached the global agenda of governments, businesses, international organisations, and communities worldwide.

In Cambodia, there have been several cyberattacks on government and business websites since 2002. For example, the Ministry of Foreign Affairs and International Cooperation (MFAIC), the National Election Committee, the Cambodian National Police, the Ministry of National Defence, and the Supreme Court have all been previously compromised (Nguon and Srun 2019). Moreover, in November 2018, several of Cambodia's largest Internet Service Providers (ISPs) were hit by large-scale DDoS (Distributed-Denial of Service) attacks, lasting for several days. As a result, Internet users experienced difficulties accessing online services (Cimpanu 2018).

Recognising the increase of cyberattacks and the importance of managing its adverse effects, the RGC has emphasised cybersecurity as one of the top priorities of the Rectangular Strategy Phase 4 (Royal Government of Cambodia 2018). Moreover, the RGC has developed its Industrial Development Policy 2015–2025, emphasising ICT as a driving factor to shift from an agricultural to an industrial-based economy (Council of Ministers 2015). To ensure the safety of the use of ICT in reaching its goals, the RGC has laid out a national legal framework to defend against cybercrime. In addition, the RGC also established a framework for the enhancement of cybersecurity, namely the ICT Masterplan 2020, where measures and initiatives were introduced to improve cybersecurity capacity. The Telecom-ICT Development Policy 2020, which was adopted in April 2016, is another instrument to boost cybersecurity initiatives in Cambodia (KOICA 2014; Royal Government of Cambodia 2020). This paper offers background knowledge on the concepts of cybersecurity legislation in the region and around the world, suggesting key pillars for Cambodia's national cybersecurity law in the future.

There are relevant laws and regulations with provisions related to cybersecurity issues such as the Criminal Code, Law on Telecommunications, E-Commerce Law, Consumer Protection Law and Sub-decree on 'Digital Signature'. However, no cybersecurity law exists in Cambodia yet. As such, on 8th June 2020, the Ministry of Post and Telecommunications (MPTC) established a working group to draft the Law on Cybersecurity in Cambodia. This working group was tasked to draft the Law on Cybersecurity, research relevant cybersecurity laws in the region and beyond, and cooperate with relevant ministries and stakeholders to ensure that the draft law is aligned with national and international legal standards. Prior to developing the draft law, the working group prepared the following concept note to create a common understanding of the concepts of cybersecurity, which will act as the foundation for drafting the Law on Cybersecurity in Cambodia.

Concepts of Cybersecurity

According to the International Telecommunication Union (ITU), cybersecurity plays an essential role in developing ICT and Internet services. Enhancing cybersecurity and protecting CIIs are essential to each nation's security and economic well-being. Making the Internet safer (and protecting Internet users) has become integral to developing new services and governmental policies. Deterring cybercrime is an essential component of a national cybersecurity and CII protection strategy. In particular, this includes the adoption of appropriate legislation against the misuse of ICT for criminal purposes and activities intended to affect the integrity of national CIIs. At the national level, this is a shared responsibility requiring coordinated actions related to the prevention, preparation, response, and recovery of incidents from government authorities, the private sector, and citizens. At the regional and international level, this entails cooperation and coordination with relevant partners. The formulation and implementation of a national framework and strategy for cybersecurity thus require a comprehensive approach. Cybersecurity strategies – for example, the development of technical protection systems or the education of users on cybersecurity practices – can help reduce the risk of cybercrime. Therefore, the development and support of cybersecurity strategies are vital elements in the fight against cybercrime (Gercke 2009).

In simple terms, cybersecurity is defined as measures taken to protect a computer or computer system (as on the Internet) against unauthorised access or attack (Merriam-Webster n.d.). As of now, there is no common or universal definition of cybersecurity. However, the ITU (2008) defines cybersecurity as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, as well as organisations and user assets". Organisation and user assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of security properties of these aforementioned assets against relevant security risks in cyberspace. The general security objectives comprise of the following: Availability; Integrity, which may include authenticity and non-repudiation; and Confidentiality" (Gercke 2009).

The term cybersecurity is often confused with cybercrime. According to Longman Dictionary of Contemporary English (n.d.), cybercrime is defined as any criminal activity that involves the use of a computer or the Internet. According to the Budapest Convention on Cybercrime, cybercrime is defined as any illegal behaviour directed by means of electronic operations that target the security of computer systems and the data processed by them. On the other hand, the term can be described as computer-related acts for personal financial gain or harm to others, including forms of identity-related crime and computer content-related acts (Council of Europe 2001).

To reiterate, there are underlying differences between cybersecurity and cybercrime. However, there are certainly overlapping similarities as well. Cybersecurity involves protecting computer systems connected to the Internet, whereas cybercrime involves criminal activities using computers or the Internet. Cybersecurity helps to protect systems or educate users to prevent becoming victims of cybercrime, which in turn reduces the risk of cybercrime. Cybercrime incidents occur when cybersecurity is breached. For that reason, cybercrime is seen as a consequent failure of cybersecurity. Therefore, cybersecurity is the core element in the fight against cybercrime.

Table 1: Cybersecurity vs Cybercrime

	Cybersecurity	**Cybercrime**
Definition	Measures taken to protect a computer or computer system (as on the Internet) against unauthorised access or attack	Criminal activities that involve the use of a computer or the Internet
Attack Type	Technical, computer-focused	Non-technical, human-focused
Target Victim	Infrastructure, government, businesses	Individuals, families
Example	Malware, denial-of-service	Cyberbullying, Internet scams

(Source: CDRI (2020))

In Cambodia, three key ministries are working on cyber-related issues. Cybercrime is under the jurisdiction of the Ministry of Interior (MOI), while the Ministry of Foreign Affairs and International Cooperation (MFAIC) is responsible for cyber diplomacy and matters related to international cybersecurity, such as international cyber-norms, confidence-building measures, and the effects of cybersecurity on international relations. Meanwhile, national cybersecurity is the responsibility of MPTC. Under MPTC, the Information and Communications Technology Security Department houses Cambodia’s Computer Emergency Response Team (CamCERT), whose missions include awareness and outreach, quality assurance and digital forensics, standards and risks, and digital authentication within public key infrastructures. One of CamCERT’s roles is incident reporting, where public and private individuals can report any security breach that they have encountered and, in turn, they will receive technical assistance from CamCERT to help them mitigate the issues. Incident coordination, security advisory and tips and alerts are also among the services that CamCERT offers (CamCERT n.d.).

Furthermore, according to the Cambodia Digital Economy and Society Policy Framework 2021–2035 adopted by the RGC in 2021, the government aims to establish a Digital Security Committee chaired by the Prime Minister. The Committee fulfils its function as Etat-Major to the National Digital Economy and Society Council, as the central command in charge of security management in the digital space to protect users' interests and resist attacks. Furthermore, the Committee will respond to all areas that require technical support and capability and the management of national social security. Responsibilities include coordinating, directing, preparing, implementing, monitoring and evaluating the implementation of policies, strategies, measures, technical standards and action plans related to security in the digital space, including cybersecurity, cybercrime and national security. The Committee will be in charge of cybersecurity, cybercrime and national security (Supreme National Economic Council 2021).

Development of Legal Framework on Cybersecurity

The United Nations General Assembly (UNGA) adopted several resolutions related to cybersecurity, namely resolution 55/63 dated January 2001 (combating criminal misuse of information technology), resolution 56/121 dated January 2002 (combating criminal misuse of information technology), resolution 57/239 dated January 2003 (creation of a global culture of cybersecurity), resolution 58/199 dated January 2004 (creating of a global culture of cybersecurity and the protection of critical information infrastructure), and resolution 64/2011 dated March 2010 (creating of a global culture of cybersecurity and taking stock of national effort to protect critical information infrastructure) (United Nations General Assembly 2010).

As part of this global effort, on 17th May 2007, the ITU launched the Global Cybersecurity Agenda (GCA) alongside partners from governments, industries, regional and international organisations, and academic and research institutions. The GCA consists of seven main goals (Gercke 2009) and five strategic pillars: 1) Legal Measures; 2) Technical and Procedural Measures; 3) Organizational Structures; 4) Capacity Building; 5) International Cooperation (ITU 2007). In addition to this agenda, in 2008, the ITU issued Recommendation X.1205 (04/08) on the Overview of Cybersecurity (ITU 2008).

At the regional level, the Association of Southeast Asian Nations (ASEAN) adopted the ASEAN Leaders' Statement on Cybersecurity Cooperation in 2018 (ASEAN 2018). Furthermore, on 2nd October 2019, ASEAN Member States (AMS) discussed the establishment of the ASEAN Cybersecurity Coordinating Committee (ASEAN Cyber-CC) at the 4th ASEAN Ministerial Conference on Cybersecurity (AMCC) in Singapore. Tentatively, the ASEAN Cyber-CC strives to promote cross-sectoral and cross-pillar cooperation among ASEAN sectoral bodies on efforts to strengthen cybersecurity in the region, facilitate cross-sectoral discussions to promote policy coherence across sectors and strengthen ASEAN's centrality in the region's cybersecurity architecture, and enhance the alignment of regional cybersecurity policy, while considering national operational considerations (CSA Singapore 2019).

With ASEAN's dialogue partners, heads of AMS, and the United States gathered in Singapore on 15th November 2018 on the occasion of the 6th ASEAN-U.S. Summit, issuing the ASEAN-United States Leader's Statement on Cybersecurity Cooperation to share the vision of a peaceful, secure and resilient regional cyberspace that serves as an enabler of economic progress, enhanced regional connectivity, and betterment of living standards for all. In 2019, ASEAN finalised the ASEAN-EU Statement on Cybersecurity Cooperation to promote the importance of adopting and implementing regional cyber confidence-building measures to increase inter-state cooperation, transparency, predictability, stability, and strengthen international peace and security. These measures aim to reduce misunderstandings, misperceptions, miscalculations, and the risk of conflict stemming from the use of ICTs, including capacity- and awareness-building in the protection of CIIs (ASEAN 2019).

Based on a study, there are only two countries in ASEAN that have already adopted both a Cybercrime Law (Computer Misuse Act) and a Cybersecurity Law namely Singapore (Computer Misuse Act, 1993 and revised 2007, 2013, 2017 and Cybersecurity Act, March 2018), and Thailand (Computer Crime Act, June 2007 and Cybersecurity Act, May 2019). Whereas Vietnam only has a Law on Cybersecurity (January 2019), Malaysia only has a Computer Crime Act (1997), the Philippines only has a Cybercrime Prevention Act (2012), Laos PDR only has a Law on Prevention and Combating cybercrime (2015), Brunei only has a Computer Misuse Act (2007), and Myanmar is still in the process of drafting its Cybercrime Law. Cambodia will be the third country in ASEAN to have both a Cybercrime Law and Cybersecurity Law.

Review of Cybersecurity Laws in Selected Countries

Cybersecurity laws of six countries were selected and reviewed due to their contextual similarities with Cambodia, despite varying levels of development. Furthermore, the foundational concepts of their cybersecurity laws will be considered and adapted into the draft Law on Cybersecurity in Cambodia.

In Japan, the Basic Cybersecurity Act (Japanese Law Translation 2020) was promulgated on 12th November 2014. The Act aims to promote cybersecurity policy by stipulating basic principles of national cybersecurity policy; clarifying the responsibilities of the national and local governments and other concerned public parties; detailing essential matters for cybersecurity-related policies such as the formation of a cybersecurity strategy; and establishing a cybersecurity strategic headquarters, among other things. In 2018, the Act was amended to set up a council that discusses the promotion of cybersecurity measures. The council will consist of national government agencies, local governments, CII operators, cyberspace-related business entities, and educational and research institutions (Japanese Law Translation 2020). The Basic Cybersecurity Act of Japan stipulates the definition of cybersecurity; the basic principles, the responsibilities of national and local government; responsibilities of CII operators; cyberspace-related business entities; responsibilities of educational and research organisations; efforts of the people; legislative measures; development of administration organisations; cybersecurity strategy; basic policy; cybersecurity strategic headquarter and supplementary provision (Japanese Law Translation 2020).

In China, the Cybersecurity Law of the People's Republic of China was promulgated on 1st June 2017 to maintain network security, safeguard cyberspace sovereignty, national security and public interests, protect the legal rights and interests of citizens, corporations and other organisations, and promote the healthy development of information technology in the economic and social sectors. The Cybersecurity Law of China establishes General Provisions; Support and Promotion of Cybersecurity; Network Operations Security (General Provisions, Operations Security for Critical Information Infrastructure); Network Information Security; Monitoring, Early Warning, and Emergency Response; Legal Responsibility and Supplementary Provisions (Creemers et al. 2018).

In Singapore, the Cybersecurity Act of Singapore came into force on 31st August 2018. The Act has four main purposes. First, it provides a proper security framework to protect CII from unauthorised access or cyberattacks. Second, it empowers the Cybersecurity Commissioner to promptly investigate and respond to cybersecurity threats and incidents. Third, a cybersecurity information sharing mechanism is established under the Act to help the government and owners of computer systems to respond to cyberattacks more effectively. Finally, the Act provides two types of licenses. These licenses are prioritised because the license holders have access to their clients' sensitive information. The Act applies to CIIs, computers and computer systems located wholly or partly in Singapore (CSA Singapore 2018). The Cybersecurity Act of Singapore enshrines Preliminary; Administration; Critical Information Infrastructure; Responses to Cybersecurity Threats and Incidents; Cybersecurity Service Providers; and General (Republic of Singapore 2018).

In Vietnam, the Law on Cybersecurity was promulgated on 1st January 2019 to regulate activities for protecting national security and ensuring social order and safety in cyberspace and the responsibilities of agencies, organisations, and individuals involved. The scope of this Act covers the Protection of Information Systems Critical for National Security, Prevention of and Dealing with an Infringement of Cybersecurity, Protective Activities, Guarantees Relating to Cybersecurity Protective Activities, Responsibilities of Agencies, and Organisations and Individuals. The governing scope of this legislation is broad, as any domestic or foreign entities providing services related to telecommunication networks and the Internet are covered by this legislation. This includes providers of value-added services to the cyberspace in Vietnam (such as social networks, search engines, online advertising, e-commerce websites/marketplaces, cloud services, online games/applications and OTT services) ("Cyberspace Service Providers"). The Cybersecurity Law of Vietnam includes General Provisions; Protection of Cybersecurity of Information Systems Critical for National Security; Prevention of and Dealing with Infringement of Cybersecurity; Cybersecurity Protective Activities; Guarantees Relating to Cybersecurity Protective Activities; Responsibility of Agencies, Organisations and Individuals; and Implementing Previsions (National Assembly of Vietnam 2018).

In Estonia, the Cybersecurity Act was promulgated on 23rd May 2019 to provide requirements for the maintenance of state and local authorities' network and information systems essential for the functioning of the society, liability and supervision, as well as the prevention and resolution of cyber incidents. Furthermore, the law explores single points of contact and competent authorities, principles of ensuring cybersecurity, cyber incident registry, the exercise of state and administrative supervision, violations of requirements of Act, proceedings, identification of service providers, provisions governing the amendment of other Acts, and entry into force of Act. The Cybersecurity Act of Estonia provides General Provisions;

Obligations for Ensuring Cybersecurity; Ensuring Cybersecurity; State and Administrative Supervision; Liability; and Implementing Provisions (Riigi Teataja 2018).

In Thailand, the Cybersecurity Act of Thailand was promulgated on 24th May 2019 to protect, prevent, cope with, and mitigate the risk of cyber threats on computer networks, the Internet, telecommunication networks, general satellite services, and CII, for both government agencies and private organisations, in order to maintain national security and public order in Thailand. The scope of this Act covers the operations of maintaining cybersecurity from both inside and outside the country of Thailand, which affects national security, economic security, martial security, and public order in Thailand (main sectors that are covered by this Act consist of computer networks, the Internet, telecommunication networks, or satellite services). (Thai Government Gazette 2019). The Cybersecurity Act of Thailand sets out Committees (National Cybersecurity Committee, Cybersecurity Regulating Committee); Office of the National Cybersecurity Committee; Maintaining Cybersecurity (Policies and Plans, Management, Critical Information Infrastructure, Coping with Cyber Threats); Penalty Provisions; and Transitory Provisions.

Policy Recommendations for Cambodia’s Cybersecurity Legislation

Given the above review of global and regional Cybersecurity development, especially on its legislation, Cambodia’s cybersecurity legal framework should take into consideration the following policy recommendations:

1. Structure a national cybersecurity governance framework. Cybersecurity is a cross-sectoral issue in the digital era, ranging from technical, economic, political, and national security. Therefore, an establishment of a high-level coordinating body to ensure the security of all sectors in the context of cyberspace is essential;

2. Strengthen the national cybersecurity framework for Critical Information Infrastructure (CII) through cyber risk assessment and compliance regimes. Most digital systems are now interconnected either locally or internationally. Due to their size and complexity, Cambodia cannot ensure their absolute security;

3. Establish cybersecurity service licensing entities to approve trustworthy, credible, and competent cybersecurity service providers. This entity should be regulated under a robust and well-rounded regulatory regime;

4. Start a Cybersecurity Development Fund with investment from the public and private sectors. These allocated funds would support cybersecurity operations in the public sector and nation-wide cybersecurity capacity building, in order to boost national cyber-defence capability;

5. Develop a cybersecurity professional licensing regime to foster trust and ethical practices. The designated person in charge of cybersecurity functions and services should be qualified with certain expertise and skills in order to access, protect and identify critical security loopholes within applications and systems;

6. Ensure mandatory reporting of cybersecurity incidents. To deal with cybersecurity incidents effectively, relevant authorities must be informed immediately of their existence. However, most cyberattacks or incidents are not reported to respective authorities. A reporting regime must be established for cybersecurity incidents, in order to prevent them from further spreading; and

7. Incentivise MSMEs to actively invest in cybersecurity resilience via governmental incentive mechanisms, which will ultimately contribute to safeguarding cyberspace at the national level. Cybersecurity requires significant investment, which MSMEs might not be able to afford, but would be mutually beneficial in the big picture context of cybersecurity in Cambodia.

Conclusion

In conclusion, this perspective paper provides a foundational background on the concepts of cybersecurity legislation worldwide and provides key suggestions for Cambodia's future cybersecurity law. With the rapidly developing digital economy in Cambodia, businesses and public services are all undergoing digital transformation – moving online and integrating with cyberspace. Although this paradigm shift towards digital transformation results in higher productivity and improved efficiency, being interconnected with cyberspace also creates risks and vulnerabilities against cyber threats and attacks. As such, robust cybersecurity legislation is of paramount importance to protect Cambodia's CIIs, consumers, and citizens.

The opinions expressed are the author's own and do not reflect the views of the Asian Vision Institute.

References

Association of Southeast Asian Nations (ASEAN). 2018. “ASEAN Leaders’ Statement on Cybersecurity Cooperation.” *ASEAN*, April 27. https://asean.org/asean-leaders-statement-on-cybersecurity-cooperation/

Association of Southeast Asian Nations (ASEAN). 2019. “ASEAN-EU Statement on Cybersecurity Cooperation.” *ASEAN*, August 1. https://asean.org/wp-content/uploads/2021/09/ASEAN-EU-Statement-on-Cybersecurity-Cooperation-FINAL.pdf

Cambodia Computer Emergency Response Team (CamCERT). n.d. “What We do.” *CamCERT*. https://www.camcert.gov.kh/en/what-we-do/

Cambodia Development Resource Institute (CDRI). 2020. “Cybergovernance in Cambodia: A Risk Based Approach to Cybersecurity.” *CDRI*, January 10. https://cdri.org.kh/publication/cybergovernance-in-cambodia-a-risk-based-approach-to-cybersecurity.

Cimpanu, Catalin. 2018. “Cambodia’s ISPs Hit by Some of the Biggest DDoS Attacks in the Country’s History.” *ZDNet*, November 8. https://www.zdnet.com/article/cambodias-isps-hit-by-some-of-the-biggest-ddos-attacks-in-the-countrys-history/.

Council of Europe. 2001. “Convention on Cybercrime.” *Council of Europe*, November 23. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561.

Council of Ministers. 2015. “Cambodia Industrial Development Policy 2015 – 2025.” Phnom Penh: Royal Government of Cambodia.

Creemers, Rogier, Paul Triolo, and Graham Webster. 2018. “Translation: Cybersecurity Law of the People’s Republic of China (Effective June 1, 2017).” *New America*, June 29. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/

Cyber Security Agency of Singapore (CSA Singapore). 2019. “ASEAN Member States Agree to Move Forward on a Formal Cybersecurity Coordination Mechanism.” *CSA Singapore*, October 2. https://www.csa.gov.sg/news/press-releases/amcc-release-2019

Cyber Security Agency of Singapore (CSA Singapore). 2018. “Cybersecruity Act.” *CSA Singapore*. https://www.csa.gov.sg/legislation/cybersecurity-act

Gercke, Marco. 2009. “Understanding Cybercrime: A Guide for Developing Countries.” *International Telecommunication Union*, April. https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf.

International Communication Union (ITU). 2007. “Global Cybersecurity Agenda.” *ITU*. https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx.

International Communication Union (ITU). 2008. *“Recommendation ITU-T X.1205”. ITU.*

Japanese Law Translation. 2020. “The Basic Act on Cybersecurity.” *Japanese Law Translation*, October 12.

Korea International Cooperation Agency (KOICA). 2014. “Cambodian ICT Masterplan 2020.” *KOICA*.

Longman Dictionary of Contemporary English. n.d. “Cybercrime.” *Longman Dictionary of Contemporary English*. https://www.ldoceonline.com/dictionary/cybercrime

Merriam-Webster. n.d. “Cybersecurity.” *Merriam-Webster*. https://www.merriam-webster.com/dictionary/cybersecurity

National Assembly of Vietnam. 2018. “Law on Cybersecurity.” Hanoi: National Assembly of Vietnam.

Nguon, Somaly, and Sopheak Srun. 2019. “Cambodia v. Hackers: Balancing Security and Liberty in Cybercrime Law.” *Konrad Adenaeur Stiftung*, January 27. https://www.kas.de/en/web/kambodscha/single-title/-/content/cambodia-v-hackers-balancing-security-and-liberty-in-cybercrime-law

Republic of Singapore. 2018. *“CYBERSECURITY ACT 2018.”* Singapore.

Riigi Teataja. 2018. “Cybersecurity Act.” *Riigi Teataja*, May 9. https://www.riigiteataja.ee/en/eli/523052018003/consolide

Royal Government of Cambodia. 2018. *“Rectangular Strategy Phase 4.”* Phnom Penh: Royal Government of Cambodia.

Royal Government of Cambodia. 2020. *“Cambodian ICT Development Plan 2020.”* Phnom Penh: Royal Government of Cambodia.

Schjølberg, Stein. 2008. “Report of the Chairman of HLEG.” *International Telecommunication Union*. https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf

Supreme National Economic Council. 2021. *“Cambodia Digital Economy and Society Policy Framework 2021-2035.”* Phnom Penh: Royal Government of Cambodia.

Thai Government Gazette. 2019. *“Cybersecurity Act, B.E. 2562 (2019).”* Bangkok: Thai Government Gazette.

United Nations General Assembly. 2010. *“UN Resolutions Related to Cybersecurity”*. New York: United Nations.

AVI COMMENTARY

ISSUE 2019, No. 14

Cambodia | 14th December 2019

Understanding the Digital Economy in Cambodia

NGOV Meng Yu[a]

Over the last two decades, Cambodia has experienced high economic growth at an average of 7% of Real GDP. This success is mostly credited to the traditional 'export-led' growth model. However, this model has its weakness in promoting further economic development for Cambodia. It is not equipped with the right characteristics to enlarge sector diversity and leaves the economy vulnerable to price fluctuation and uncertainty of global demand. Integration of digital technology is the additional driver needed to allow Cambodia to realise its long-term ambition to become an upper-middle-income and higher-income country by 2030 and 2050, respectively.

Reliable internet connection and telecommunications network infrastructure are a foundation for development and transforming Cambodia into a digital economy. Internet connection is the basic mechanism for digital economy to operate efficiently. In the present, basic digital infrastructure has been growing in Cambodia; a mobile broadband as a measure of mobile cellular subscription in Cambodia grew from less than 10 per 100 inhabitants in 2005 to 125 in 2016. In contrast, fixed broadband subscriptions are estimated to be 0.6 per 100 inhabitants in 2016, revealing that Cambodia is underperforming compared to the wider regional (ASEAN). The low internet subscription price, lack of physical landline infrastructure in the rural area, and a large amount of smartphone penetration in Cambodia are determinant factors of mobile broadbands dominant the internet market in Cambodia.

Substantial progress in basic digital infrastructure is an opportunity for Cambodia to develop the digital economy; however, barriers to its provision for the next generation of innovators

[a] **NGOV Mengyu** is a Research Fellow at the Centre for Inclusive Digital Economy (CIDE) at the Asian Vision Institute (AVI).

may be limited for the aforementioned reasons. The mobile revolution showed the opportunities for leapfrogging, within which Cambodia has increased mobile connectivity, bypassing the need for building a physical landline. The next transformation will be required more than basic digital technology improvement.

Human capital development will improve the productivity level of the country; highly educated workers will be the group endorsing industry 4.0. The United Nations (UN) global adoption index measures the spread of technological adoption amongst the organisations, businesses and people in comparison to the global scale. The UN ranked Cambodia in the lower group in comparison with the wider Asia Pacific region; the index demonstrated that both public and private institutions are mostly not ready for the digital transition. This readiness is plagued by the low digital literacy gap amongst Cambodians. The low digital literacy rate may disrupt the Cambodian labour market; a shift from labour-intensive production to more automated production techniques will make Cambodia's labour market vulnerable. As a consequence, it prevents Cambodia from absorbing the full potential of digital transformation.

Cost reduction and reliance on the internet and intranet, have influenced and challenged traditional business models and private sector operations. The digital economy can help businesses capture the additional value-added via the implication of platformisation. This is a form of the digital market platform that allows businesses and SMEs to offer their goods and services effectively to broader consumers. E-commerce startups are growing in Cambodia; BookMeBus is one such business founded locally by Mr. Chea Langda. BookMeBus strikingly captures the niche market in Cambodia, through facilitating consumer purchase of transport tickets with its online platform. This platform acts as an intermediary to ease product allocation more efficiently and broaden the market. Therefore, the digital economy accelerates economic development through assisting consumers at large, bringing new innovation into the market.

In preparation for transforming Cambodia into a digital economy by 2023, RGC realised that digital literacy and institutional regulation are needed to improve the readiness of technological adoption in Cambodia. The Ministry of Education, Youth and Sport of Cambodia actively revises the curriculum framework for general and technical education. The latest revision of the general education framework is tailored towards the inclusion of 21st Century skills, primarily focusing on integrating information communication and technology (ICT) into the curriculum. Such an arrangement appears to empower human resource productivity. Despite the progression in curriculum revision, the education and digital literacy gap still persists amongst Cambodians, even if the higher education system is well equipped compared to lower education system. Limitations of regional standards of ICT knowledge, create mismatches of jobs and quality in Cambodia.

Internet technology within the digital economy requires a completely new governance that coordinates and regulates activities across all economic sectors, while managing cyber threats risks. Hence, with well-designed e-commerce regulations from the government, it may occasionally ease the adoption of digital transformation and innovation, via the impact of better procurement practice on market development.

The above discussion may offer some policy options for Cambodia to benefit from the transition into a digital economy. To mitigate some of the challenges, future policies should address the institutional framework to regulate the practice of e-commerce within a national framework of cyberspace governance, as an initial step to bolster direct investment into the sector and the prevention of cyber threats. Technological skill shortage is a primary concern, with calls for a reform of the education system and professional training to raise awareness of digital technologies.

The views expressed are the author's own and do not reflect the views of the Asian Vision Institute.

AVI COMMENTARY

ISSUE 2020, No. 03

Cambodia | 13th March 2020

State of E-Commerce in Cambodia

OUCH Richard[a]

E-commerce development has been gaining traction within the Kingdom of Cambodia, especially within these past few months. The government has enacted several laws and regulations related to e-commerce, while internet penetration rates and e-commerce revenue numbers continue to trend upwards. With these drivers, it is almost certain that e-commerce will play a major role in Cambodia's development.

In 2018, internet penetration rates were an estimated 48.8% of the population, or 8 million internet users. Though the use of technology would appear to lean heavily towards the younger crowd, the e-commerce market demographics are quite diverse. In 2019, out of the 6.68 million users, over half of the users were between the ages of 25 and 44, whereas only 18% were of ages 18 to 24, and 45-54 years old. Additionally, there is an almost-even split between male and female users.

The growth of online payment gateways, such as Pi Pay, WingPay, and PayWay, alongside a growing knowledge of digital technology, has helped enable Cambodian SMEs to enter the digital economy on their own accord, conducting business-to-consumer and business-to-business transactions through multiple platforms. Such examples include Fannow and Phzar, most of which integrate the aforenoted payment methods into their website. However, according to a report from Geeks in Cambodia, usage of online payment gateways, as well as ownership of a finance account, are still relatively low. Only 22% of adults, aged 15+, own a financial account; and only 3.8% make online purchases or pay bills online.

[a] **OUCH Richard** is a Research Fellow at the Centre for Inclusive Digital Economy (CIDE) at the Asian Vision Institute (AVI).

Though usage of online payment gateways is low, when calculating e-commerce revenue, cash-on-delivery payment is included in the process of e-commerce, which is showing growth. According to Statista, 2019 revenue was at an estimated $262 million USD, which is more than double the amount in 2017. If current trends are to continue, revenue can double yet again by 2024, with the sales of fashion and electronic goods estimated to dominate the market.

The most prominent platform for conducting e-commerce in Cambodia is the social media platform, Facebook. The platform hosts more than 8.8 million users in Cambodia, which is more than half of the total population in 2019. Facebook contains an array of tools and features that enables sellers and vendors alike to sell their goods or services: Facebook groups, pages, and the marketplace. Sponsored ads can also be purchased, displaying an advertisement of their choice or linking straight to the business's page. Livestreams are commonly used, where products or services are advertised and sometimes sold live to hundreds or thousands of viewers. Some transactions are made through Facebook messenger, where buyers and sellers perform the transaction, albeit usually paying with cash-on-delivery.

In November 2019, the government enacted two major laws pertaining to e-commerce in Cambodia: The e-commerce Law, and the Law on Consumer Protection. The e-commerce Law reportedly "regulates domestic and cross-border e-commerce activities in Cambodia, establishes legal certainty for electronic transactions, and enacts a number of important protections for consumers", whereas "The Consumer Protection Law establishes rules to guarantee the rights of consumers and to ensure that businesses conduct commercial competition in Cambodia fairly." These laws setup the legal foundation for e-commerce to truly flourish, offering a safety net for both consumer and sellers alike. However, until these laws are put into practice, e.g. a court dispute between a seller and buyer within social media or other online platforms, it is difficult to gauge how effective they will be.

It is without a doubt that e-commerce will become a mainstay of Cambodia as the country develops further into the future. However, cash remains the primary source of payment, as digital literacy and trust in online forms of payment remain a challenge. Despite these hurdles, e-commerce market indicators, such as internet penetration and revenue numbers, are expected to continue its growth well into the future. The government has also acknowledged this with their own efforts to add robust and forward-looking regulations.

The views expressed are the author's own and do not reflect the views of the Asian Vision Institute.

AVI POLICY BRIEF

ISSUE 2019, No. 13

Cambodia | 9th November 2019

Digital Trade Facilitation in Cambodia: Progress and Future Priority

SOK Kha[a]

Executive Summary

- In Cambodia, merchandise trade has become a key growth driver following the adoption of an outward-looking approach which focuses on liberalising the economy to increase trade activities and attract foreign investment. Major trade bottlenecks remain; however, whereby import-export activities are relatively costly with excessive and time-consuming documentation process and low trade logistics performance amongst others. These have given rise to the significance of trade facilitation reforms.

- Cambodia has taken rigorous trade facilitation reforms. Observable improvements have been taking place. They are good signs demonstrating the government's commitments to ASEAN and WTO agreements, i.e., ASEAN Trade in Goods Agreement (ATIGA) and WTO Trade Facilitation Agreement (TFA).

- The reforms have also brought about progress in the implementation of digital trade facilitation measures in the Customs and Ministry of Commerce. Cambodia has also scored relatively well in the UN Global Survey on Digital and Sustainable Trade Facilitation with regards to the application of modern ICT to trade-related services. However, reform momentum must pick up to ensure a full-fledged digital trade facilitation.

[a] **SOK Kha** is a Research Fellow at the Asian Vision Institute (AVI).

- The priorities should include the establishment and effective implementation of certain legal and regulatory frameworks as well as the establishment of the full-functioning National Trade Facilitation Committee (NTFC) as a main coordinating structure for speeding up the implementation of digital trade facilitation measures.

សេចក្តីសង្ខេបអត្ថបទ

- នៅក្នុងប្រទេសកម្ពុជា ពាណិជ្ជកម្មទំនិញបានក្លាយទៅជាកម្លាំងចលករដ៏សំខាន់មួយនៅក្នុងកំណើនសេដ្ឋកិច្ច បន្ទាប់ពីមានការអនុម័តឲ្យប្រើប្រាស់នូវវិធីសាស្ត្រសម្លឹងមើលពិភពខាងក្រៅ ដែលផ្តោតសំខាន់ទៅលើសេរីភាវូបនីយកម្មសេដ្ឋកិច្ចដើម្បីបង្កើនសកម្មភាពពាណិជ្ជកម្ម និងទាក់ទាញវិនិយោគទុនបរទេស។ យ៉ាងណាមិញ ឧបសគ្គ ឬរបាំងពាណិជ្ជកម្មមួយចំនួននៅតែបន្តកើតមាន ដែលធ្វើឲ្យសកម្មភាពនាំចេញនាំចូលហាក់មានការចំណាយខ្ពស់ រួមជាមួយនឹងដំណើរការបែបបទឯកសារមានលក្ខណៈស្មុគស្មាញ និងប្រើប្រាស់ពេលវេលាយូរ ក៏ដូចជាប្រតិបត្តិការដឹកជញ្ជូនទំនិញមានភាពទន់ខ្សោយនៅឡើយ បើប្រៀបធៀបនឹងប្រទេសដទៃ។ កត្តាទាំងនេះបានធ្វើឲ្យកំណែទម្រង់កិច្ចសម្របសម្រួលពាណិជ្ជកម្មមានសារៈសំខាន់យ៉ាងខ្លាំង។
- កម្ពុជាបានដាក់ចេញនូវកំណែទម្រង់កិច្ចសម្របសម្រួលពាណិជ្ជកម្មដ៏ម៉ឺងម៉ាត់។ កំណែលម្អគួរឲ្យកត់សម្គាល់ជាច្រើនបានកើតឡើង។ កំណែលម្អទាំងនោះបានបង្ហាញពីសញ្ញាណវិជ្ជមាន ដែលបង្ហាញពីការប្តេជ្ញាចិត្តរបស់រដ្ឋាភិបាលចំពោះកិច្ចព្រមព្រៀងនានាជាមួយ អាស៊ាន និងអង្គការពាណិជ្ជកម្មពិភពលោក ឧទាហរណ៍ដូចជា កិច្ចព្រមព្រៀងការដោះដូរពាណិជ្ជកម្មទំនិញអាស៊ាន (ATIGA) និងកិច្ចព្រមព្រៀងលើកិច្ចសម្របសម្រួលពាណិជ្ជកម្មអង្គការពាណិជ្ជកម្មពិភពលោក (TFA)។
- កំណែទម្រង់ជាច្រើនក៏បានបង្កើតឲ្យមានផងដែរនូវវឌ្ឍនភាពក្នុងការអនុវត្តវិធានការនៃកិច្ចសម្របសម្រួលពាណិជ្ជកម្មឌីជីថលនៅផ្នែកពន្ធគយ និងក្រសួងពាណិជ្ជកម្ម។ កម្ពុជាក៏ទទួលបានចំណាត់ថ្នាក់ល្អនៅក្នុងការស្ទង់មតិជាសកលរបស់អង្គការសហប្រជាជាតិស្តីពីកិច្ចសម្របសម្រួលពាណិជ្ជកម្មឌីជីថល និងពាណិជ្ជកម្មប្រកបដោយចីរភាព ដែលពាក់ព័ន្ធទៅនឹងការអនុវត្តបច្ចេកវិទ្យា ICT ទំនើបចំពោះសេវាពាណិជ្ជកម្មនានា។ យ៉ាងណាមិញ កម្លាំងចលករនៃកំណែទម្រង់ចាំបាច់ត្រូវតែជំរុញដើម្បីធានាឲ្យបាននូវកិច្ចសម្របសម្រួលពាណិជ្ជកម្មឌីជីថលយ៉ាងពេញលេញមួយ។
- អាទិភាពនានាគួរតែរាប់បញ្ចូលនូវការបង្កើត និងការអនុវត្តបទដ្ឋានច្បាប់ និងបទបញ្ញត្តិមួយចំនួនប្រកបដោយប្រសិទ្ធិភាព រួមទាំងការបង្កើតគណៈកម្មាធិការជាតិសម្របសម្រួលពាណិជ្ជកម្ម(NTFC) ឲ្យដំណើរការពេញលេញ ជារចនាសម្ព័ន្ធចម្បងក្នុងការសម្របសម្រួល ដើម្បីពន្លឿនល្បឿននៃការអនុវត្តវិធានការសម្របសម្រួលពាណិជ្ជកម្មឌីជីថល។

Introduction

A Cambodian delegation from the Ministry of Commerce and Customs were among the participants at the Asia-Pacific Trade Facilitation Forum (APTFF) 2019, held in New Delhi. In collaboration with the Government of India as the host country, the Forum was co-organized by the United Nations Economic and Social Commission for Asia and the Pacific (ESCAP) and Asian Development Bank (ADB). The Forum focused on digital and sustainable trade facilitation measures by investigating opportunities and challenges from trade digitalization for sustainable development of the region.

As far as trade is concerned, the Cambodian government has given trade facilitation priorities to all leading sectors, which are making good steady progress. The areas of progress include particularly the adoption and application of modern ICT to trade-related services, including customs risk management, customs automation, national single window, and certificates of origin.

Despite the significant improvements, the annual Doing Business reports still rank Cambodia's poorly at 115 out of 190 economies globally on "Ease of Trading Across Borders". For this reason, this article aims to examine the progress and priorities relating to the acceleration of digital trade facilitation in Cambodia. It proceeds by first presenting the significance of trade facilitation in Cambodia before highlighting the progress and future priorities in Cambodia's digital trade facilitation implementation. The last section provides a concluding summary.

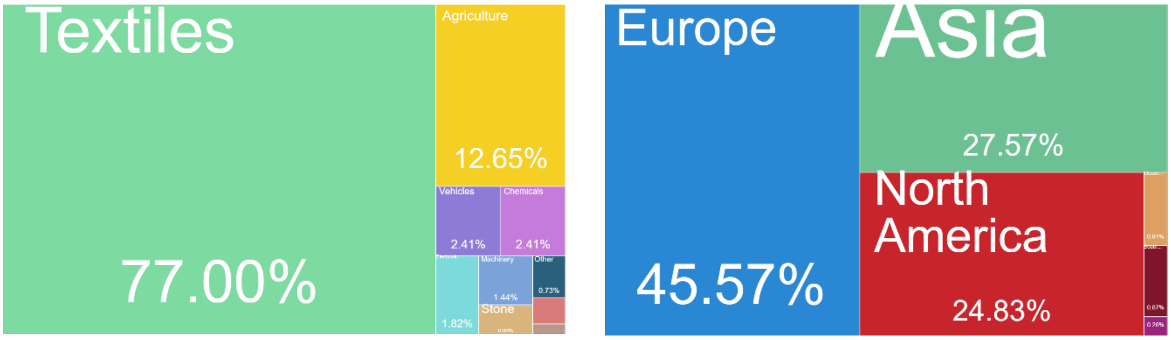
Significance of Trade Facilitation in Cambodia

Cambodia had been largely an agrarian country until the mid-1990s when the economy undertook a significant transition toward industrialization. The industrial sector has since been growing steadily, opening the country and the people to many new opportunities. The opportunities have created conditions contributing to the country's economic growth and development.

Merchandise trade has been the key growth driver, following the adoption of an outward-looking approach which focuses on liberalizing the country's economy to increase trade activities and attract foreign investment. For example, Cambodia joined the Association of Southeast Asian Nations (ASEAN) in 1999 and WTO in 2004. Broadly speaking, they are the two main multilateral institutions helping Cambodia to expand its export markets. Holding their memberships have enabled Cambodia to attract more foreign investors through greater, more secure access to overseas markets and the improvement of the country's business environment and international image.

Cambodia's industrialization process has thus far largely relied on trade preferential treatments such as the European Union's Everything But Arms (EBA) and the United States of America's Generalized System of Preferences (GSP), both of which grant Cambodia duty and quota preferential export access of goods to the EU and US markets. Cambodia's main merchandise export are apparel and footwear from the garment and textile industry, which has grown quickly to become the country's largest industrial sector. The government's efforts to accelerate and diversify trade have seen some success, with a surge in imports and exports of other goods. The merchandise export volume grew from US$1.5 billion in 2001 to US$16.5 billion in 2017. The largest export markets for Cambodia's products include the EU, the US, Japan, China, Canada, Singapore, Thailand, and Vietnam.[a]

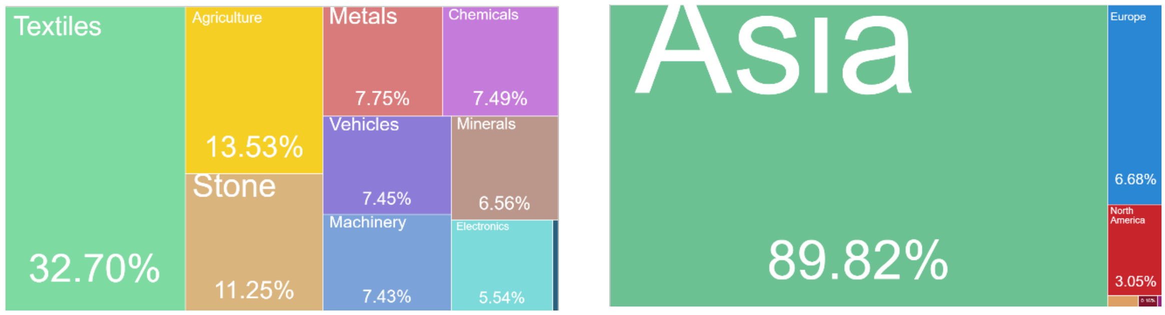
Figure 1: Cambodia's exported products and markets, 2017



Source: Atlas of Economic Complexity, Center for International Development.

The import volume also grew from US$1.5 billion to US$14.6 billion during the same period. Textiles and related garment industry inputs accounted for the largest share. The largest exporting countries to Cambodia include China, Thailand, Vietnam, Singapore, Japan, and South Korea.[b]

Figure 2: Cambodia's imported products and partners, 2017



Source: Atlas of Economic Complexity, Center for International Development.

Despite the significant improvements, major trade bottlenecks remain, whereby import-export activities are relatively costly with excessive and time-consuming documentation process and low trade logistics performance amongst others. A cross-country comparison study shows that ‘Ease of Doing Business’ in Cambodia still lacks behind its competitors. The fact that Cambodia was ranked poorly, at 115 out of 190 economies globally on Ease of Trading Across Borders,[c] is worrisome and means that further improvement measures, particularly trade facilitation reforms, must build up momentum.

Trade facilitation is significant because it is meant to expedite movement, clearance, and release of goods, including goods in transit. A sizable body of research have examined and provided strong evidences on positive linkages between trade facilitation, trade growth, and development. For example, various studies show that the improvement in port and information infrastructures, more rapid customs clearance time, or regulatory reforms to remove duplicative technical requirements on imports and exports have positive impacts on trade expansion and competitiveness.[d]

Indeed, trade facilitation has become even more crucial as Cambodia is looking for alternative market access abroad, particularly in the contexts that the country’s duty and quota preferential access privileges to traditional markets in the EU and the US under the EBA and the GSP that Cambodia enjoys as a Least Developed Country (LDC) will at some point come to an end.

Progress in Cambodia’s Digital Trade Facilitation Implementation

Following the accession to ASEAN and WTO, Cambodia has made rigorous reform efforts in trade facilitation. Observable improvements have been taking place, particularly in the application of modern information and communication technologies (ICT) to simplify and automate international trade procedures. This is commonly referred to as digital trade facilitation. The improvements are good signs demonstrating the government's commitments to the ASEAN and WTO agreements.

The key agreement within ASEAN is ATIGA, which has a number of chapters that deal directly with trade facilitation. For example, Chapter 5 describes the ASEAN Trade Facilitation Work Program, which covers measures related to customs, trade procedures, standards and conformance, sanitary and phytosanitary, and ASEAN single window. It also elaborates the ASEAN guiding principles on trade facilitation, i.e., transparency, communications and consultation, simplification, practicability and efficiency, non-discrimination, consistency and predictability, harmonization, standardization and recognition, modernization and use of new technology, and due process and cooperation.[e]

The WTO adopted TFA in 2014. The aim was to enable developing and least-developed countries to build their capacity and receive assistance needed to reap the full benefits of the agreement. In 2016, Cambodia ratified the WTO TFA, completed an assessment of its trade facilitation framework in light of TFA requirements, and developed a road map to implement the agreement. The country submitted its category A, B and C notifications regarding the implementation of the various provisions of the TFA to WTO in August 2017. As of September 2019, Cambodia had notified 60.9 percent under Category A, 19.3 percent under Category B, and 19.7 percent under Category C. Falling under Category C, which signifies assistance and support needs for capacity building and institutional reforms, are nine measures: (1) information available through internet, (2) notification, (3) pre-arrival processing, (4) electronic payment, (5) authorised operators, (6) perishable goods, (7) border agency cooperation, (8) national single window, and (9) transit.[f]

Cambodia's reform efforts have seen progress in the implementation of digital trade facilitation measures in the Ministry of Commerce and Customs. Reforms to automation of certain trade-related processes have kicked off one after another in these two leading agencies.

The Ministry of Commerce has an important role to play as a facilitator in advancing trade facilitation agenda in Cambodia, especially for those commitments that have been agreed under ASEAN and WTO agreements. The ministry has implemented online business registration and online Certificate of Origin (CO) application systems.

Cambodian Customs is another leading agency undertaking various reform and modernization programs to fulfil its missions of revenue collection, trade facilitation, and prevention of customs offences. They introduced the automated customs processing system called Automated System on Customs Data (ASYCUDA) in 2008 in order to facilitate export, import, and goods in transit. The ASYCUDA system is now implemented at all ports and checkpoints, and it covers all Single Administrative Declarations (SAD) and trade volume data.

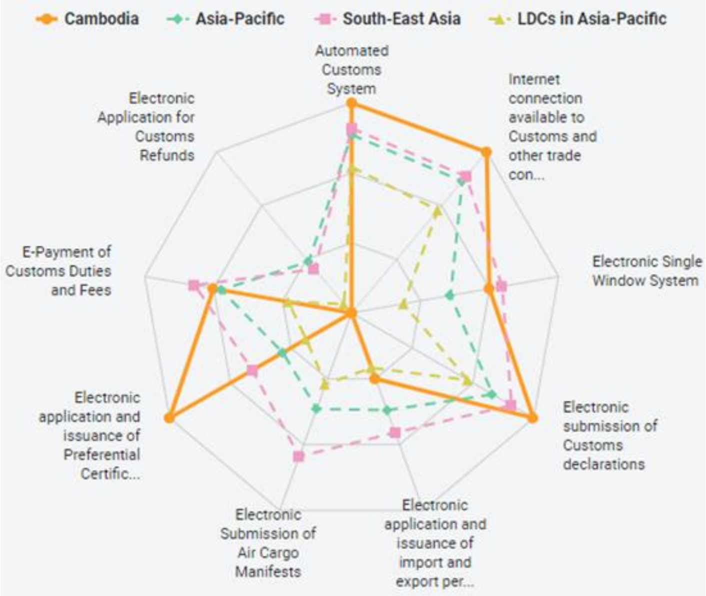
At the same time, e-Customs has also been developed by in-house resources to complement the ASYCUDA on certain procedures, including General Goods and Petroleum Product Transportation Permit Management Module, Customs Summary Declaration and De-minimis Module, International and National Customs Transit Module, Guarantee Deposit Management Module, Container Scanning Result Module, Petroleum Product Transport Document Management Module, QIP Transport Document Management Module, e-Payment Module, among others. Cambodian Customs has also launched mobile apps such as the Customs Tariff and Customs Clearance Handbook with the purpose of strengthening transparency in trade-related information.

Work to establish a fully operational and well performing Cambodia's National Single Window (CNSW) is ongoing. CNSW is built, managed, and operated by Customs. It is a trade facilitation automation platform for customs clearance procedures, which consolidates all documentation processes into a single, ICT-based submission for both importers and exporters. Cambodian Customs has advanced CNSW implementation significantly with the announcement of the completion of Phase 2 implementation on 1 July 2019. Traders can now, for instance, request Rules of Origin (RoO) Certificates required for tariff preferences in the ASEAN Economic Community (AEC).

The Ministry of Economy and Finance (MEF), to which Customs belongs, also launched Cambodia's National Trade Repository (NTR) portal in late 2015 to conform to ASEAN requirements and to respond to the mandates under the ASEAN NTM Work Program and WTO TFA. The NTR serves as "the official source for all regulatory information relevant to traders who wish to import goods into Cambodia or export to other countries", and it makes information related to trade legislation and policies available to a broad range of stakeholders.

On the macro view, Cambodia has also scored relatively well in the UN Global Survey on Digital and Sustainable Trade Facilitation in regard to the application of modern ICT to trade-related services. They include the internet connectivity at Customs and other trade control agencies, electronic submission of customs declaration, electronic application and issuance of CO, the automation of Customs systems, and electronic payment of customs duties and fees to a full-fledged electronic single window system.[g]

Figure 3: Application of modern ICT to trade-related services in Cambodia



Source: UN Global Survey on Digital and Sustainable Trade Facilitation (2019).

However, Cambodia's digital trade facilitation implementation has continued to face certain challenges – both legal and technical aspects. On the one hand, Cambodia lacks the legal and regulatory frameworks for electronic transactions and signatures as well as for accessing and sharing information and data. On the other hand, other trade-related agencies have not deployed the ICT system to simplify and automate their trade-related procedures. At the time of this writing, there is an overall absence of institutional coordinating mechanisms to address the challenges.

Future Priorities in Digital Trade Facilitation Implementation in Cambodia

There is an overall need to build a stronger reform momentum to push the digital trade facilitation implementation to a higher level. On the legal front, there has been some progress in enacting statutes and regulations governing electronic transactions and data sharing. They include e-commerce and consumer protection laws, cybersecurity and privacy laws, and data governance and data protection laws. Following 10 years in the making, the final drafts of the e-commerce and consumer protection laws were endorsed by the government in July 2019 and approved by the National Assembly in early October 2019.

Progress on other enabling legal frameworks need to move forward more rapidly. Implementing these laws require strong regulations, for which relevant ministries can be under-equipped to produce if they lack the understanding and fail to engage inputs from the private sector in a consistent and inclusive manner. Therefore, raising awareness and building a more comprehensive understanding among relevant government agencies about their legal responsibilities, with some reference to international models and best practices, are as much crucial as establishing legal and regulatory frameworks itself.

On the technical front, the lack of human capacity and financial resources as well as ambiguous attitude toward 'change' at other trade-related agencies make their adoption of ICT challenging. It highlights the needs for strong political support and leadership, effective inter-ministerial coordination and dialogues among all relevant agencies, and resource mobilization to support the development, management, and operation of ICT applications.

There have so far been multiple discussions related to the establishment of the National Trade Facilitation Committee (NTFC). This institutional coordinating mechanism is meant to coordinate trade-related policies, facilitate intra and inter-agencies collaborations, enhance accountability and transparency of trade-related government agencies, strengthen capacity on trade-related issues, develop feedback systems to receive complaints and record obstacles, and monitor and improve the overall trading environment. NTFC can also support trade-related agencies to set up their respective strategic plans to secure budget for their implementation of ICT system. However, at the time of writing this article, there has neither been a formal consensus on the role, duties and tasks of the NTFC, nor a government sub-decree creating it yet.

Conclusion

Embracing an open and liberal market economy where merchandise trade has become the key growth driver, Cambodia has made remarkable improvements in trade facilitations, whereby the government has made rigorous trade reform efforts, including the use of modern information and communication technologies to simplify and automate international trade procedures. However, certain legal and technical issues have constrained the implementation progress of digital trade facilitation.

In order to move forward, work for the establishment of NTFC must progress without any further delay. It must act as a coordinating platform for resource mobilisation to strengthen human, technical, and organizational capacity to enhance digital trade facilitation implementations. Some development programs are already in place, where Cambodia may consider leveraging its support (e.g.: UNCTAD Empowerment Program on National Trade Facilitation Bodies, EU-ASEAN Regional Integration Support (ARISE Plus). A full empowerment of the lead agencies and the encouragement of greater participation from both relevant public agencies and trader communities should also be promoted to secure a broader participation from relevant stakeholders. In conclusion, political support and long-term commitments from the top government executives are key to build and promote a full-functioning NTFC that will enable Cambodia to fully fulfil its trade liberalization and facilitation commitments.

The opinions expressed are the author's own and do not reflect the views of the Asian Vision Institute.

[a] World Integrated Trade Solution (WITS), World Bank.

[b] Ibid.

[c] Ease of doing business in Cambodia, World Bank Group. Available online at: https://www.doingbusiness.org/en/data/exploreeconomies/cambodia

[d] Assessing the Potential Benefit of Trade Facilitation: A Global Perspective, World Bank Policy Research Working Paper. Available online at: https://openknowledge.worldbank.org/bitstream/handle/10986/14733/wps3224TRADE.pdf

[e] ASEAN Trade in Goods Agreement (ATIGA), ASEAN. Available online at: http://investasean.asean.org/files/upload/Doc%2002%20-%20ATIGA.pdf

[f] WTO Trade Facilitation Agreement Facility. Available online at: https://www.tfadatabase.org/members/cambodia

[g] UN Global Survey on Digital and Sustainable Trade Facilitation, United Nations. Available online at: https://untfsurvey.org/economy?id=KHM

AVI POLICY BRIEF

ISSUE 2020, No. 03

Cambodia | 22nd February 2020

Digital Finance for Financial Inclusion in Cambodia

NGOV Meng Yu[a]

Executive Summary

- Financial inclusion is the key mechanism to enhance further economic development in Cambodia. Improving accessibility to finance at an affordable rate allows SMEs and entrepreneurs to actively capture the opportunities that arise from a fast-growing economy in Cambodia. Moreover, financial inclusion will help to improve social welfare in Cambodia.
- However, the traditional banking system has limitations to further bridge the financial inclusion gap. Digital Finance will help excel financial inclusion.
- Improving financial inclusion might cause disruption to current financial stability. Policy makers need to implement the right policies to ensure that the digital finance ecosystem will thrive and grow sustainably.
- Making prudent regulations and frameworks to ensure it is being practiced ethically and safely. Improving financial literacy is critical to nurture the financial ecosystem and protect the consumer.

[a] **NGOV Mengyu** is a Research Fellow at the Centre of Inclusive Digital Economy (CIDE) of the Asian Vision Institute (AVI).

សេចក្តីសង្ខេបអត្ថបទ

- ហិរញ្ញវត្ថុសម្រាប់ទាំងអស់គ្នាគឺជាយន្តការគន្លឹះនៅក្នុងការលើកកម្ពស់ការអភិវឌ្ឍសេដ្ឋកិច្ចកម្ពុជាឲ្យកាន់តែប្រសើរឡើង។ ការបង្កើនលទ្ធភាពនៃការទទួលបានហិរញ្ញវត្ថុនៅក្នុងអត្រាមួយសមស្របអនុញ្ញាតឲ្យសហគ្រាសធនតូចនិងមធ្យម (SMEs) ក៏ដូចជាសហគ្រិននានាចូលរួមយ៉ាងសកម្មក្នុងការចាប់យកឱកាសពីកំណើនសេដ្ឋកិច្ចដ៏ឆាប់រហ័សរបស់កម្ពុជា។ បន្ថែមពីនេះ ហិរញ្ញវត្ថុសម្រាប់ទាំងអស់គ្នានឹងជួយពង្រឹងសុខុមាលភាពសង្គមកម្ពុជា។
- ទោះបីជាយ៉ាងណាក៏ដោយ សមត្ថភាពរបស់ប្រព័ន្ធធនាគារបែបប្រពៃណីនៅក្នុងការបំពេញចន្លោះខ្វះខាតនៃហិរញ្ញវត្ថុសម្រាប់ទាំងអស់គ្នាគឺនៅមានកម្រិតនៅឡើយ។
- ការលើកកម្ពស់ហិរញ្ញវត្ថុសម្រាប់ទាំងអស់គ្នាអាចបង្កអស្ថិរភាពដល់ហិរញ្ញវត្ថុបច្ចុប្បន្ន។ អ្នកបង្កើតគោលនយោបាយត្រូវតែអនុវត្តនូវគោលនយោបាយដែលត្រឹមត្រូវដើម្បីធនាគារថា ប្រព័ន្ធហិរញ្ញវត្ថុឌីជីថលនឹងរីកចម្រើនលូតលាស់ប្រកបដោយចីរភាព។
- ត្រូវបង្កើតបទបញ្ញត្តិនិងក្របខ័ណ្ឌគតិយុត្តិដោយប្រុងប្រយ័ត្នដើម្បីជានាថា វាត្រូវបានអនុវត្តប្រកបដោយសីលធម៌និងសុវត្ថិភាព។ ការលើកកម្ពស់អត្រាអក្ខរកម្មហិរញ្ញវត្ថុគឺមានសារៈសំខាន់ណាស់នៅក្នុងការសម្រួលដល់ប្រព័ន្ធហិរញ្ញវត្ថុនិងការការពារអតិថិជន។

Introduction

Financial inclusion is the foundation point of socio-economic development. The importance of financial inclusion policy will serve to unlock the Sustainable Development Goals (SDG) in Cambodia, particularly in regard to SDG: 1 Poverty Reduction and SDG: 9 Industry, Innovation and Infrastructure. Hence, financial inclusion may bring the **sought-after** process of inclusive growth into Cambodia.

The purpose of financial inclusion is to include every person who is ***unbanked*** into the formal financial system and to optimally serve the ***underbanked*** group of people. The goal of financial inclusion is thus to ensure that individuals have equal opportunity and greater access to formal credit, saving, payment and insurance, all at an affordable cost.

The improvement of financial inclusion will enable access to credit all whilst promoting developments of the social and financial infrastructure available to the public. Thus, individuals have the financial system to turn to during times of economic turbulence to smooth out their consumption. Furthermore, Small and Medium Enterprises (SMEs) from all sectors have equal opportunities to participate in the Cambodian growth. This shows the foremost fundamental of financial inclusion; its function is not only about access to finance and savings, as this mechanism will also help alleviate the country social exclusion existing in the economy.

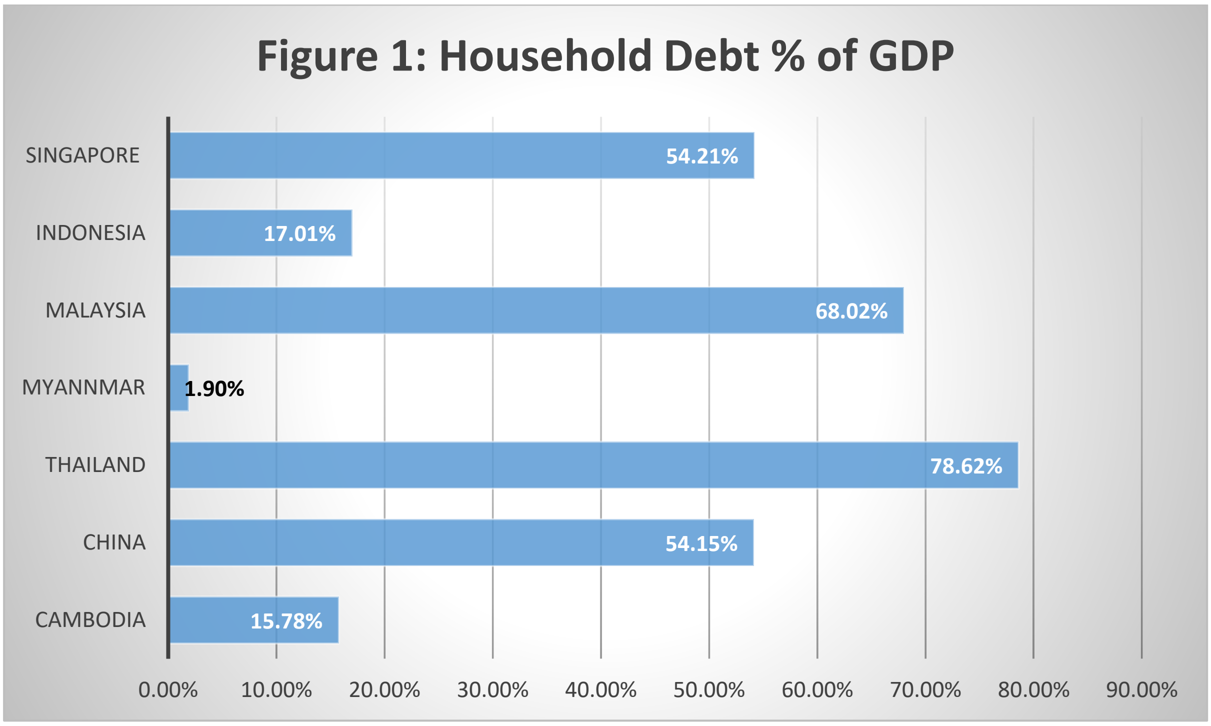
The Royal Government of Cambodia (RGC) and National Bank of Cambodia (NBC) have been focused on improving financial inclusion through the introduction of microfinance institutions (MFI) and strengthening credit scoring mechanisms. Nevertheless, SMEs with limited assets for collateral purposes and financial history are excluded from the services.

In consideration of the challenges amongst Cambodia SMEs and low-income households, the rise of digitalisation may give way to the rise of Fintech and peer-to-peer (P2P) lending platforms as an indirect alternative to the traditional banking system. Fintech firms have the potential to connect with this cash-based society and transfer it into a digital-based society, where daily transactions can be completed digitally. Such a transformation will require each individual to be connected with any form of financing system. The purpose of this policy brief is to evaluate the current financial inclusion in Cambodia, illustrating how digital finance may enhance financial inclusion and change individual saving behaviour. It will help identify the key challenges of financial inclusion and provide recommendations.

Current Stage of Financial Inclusion and Opportunities in Cambodia

Individual well-being is positively linked with individual access to credit and banking systems. As entrepreneurs and SMEs have creative ideas, accessibility of finance and valuable institutional consultant may empower entrepreneurs and SMEs towards expansion and participating in the growing economy.

Providing equal access to financial systems will create a multiplier effect in the economy. One of the key elements that can boost economic growth effectively is the utilisation of credit to boost consumption and accelerate production capability. Figure 1 illustrates household debt as a percentage of GDP, by comparing Cambodia's ratio to China and ASEAN nations. Cambodian Household debt ratio to GDP is estimated at around 15.78%. This ratio is relatively low compared to other countries, illustrating that the financial market in Cambodia is under-developed.



Source: IMF, Cambodia is draw from CEID

SMEs are the catalyst of innovations, since they lead to improving financial ability and piloting industrial progression. For Cambodia, SMEs alone account for at least 1.2 million of the Cambodian labour forces. 90% of 510,000 registered firms are categorised as SMEs[a].

Similarly, to all businesses, SMEs require additional capital in the form of credit for further expansion and operation. SMEs tend to have limited assets for collateral purposes, and the lack of banking, financial statements and credit records make them unpromising **and risky** candidates for the banks. Thereby, SMEs struggle to access credit from commercial banks. It is in this way that Fintech could be appropriately used to help excel SMEs in building up their financial statements and building their credit worthiness.

The RGC and NBC have been promoting Microfinance Institutions (MFI) to spread microcredit and improve financial inclusion amongst SMEs. MFI provides two large benefits; a relatively low-interest rate and longer loan repayment duration. The interest charge of MFIs is offered relatively lower compared to informal sources of financing. With a long duration of loan repayment, it will help free up the SMEs' cash flow. As indicated by the World Bank report in 2016, households with access to loans will increase their probability of engaging in economic activities and become an entrepreneur enterprise by 4% compared to households without access to such loans.

Regardless of the wide extension of MFIs in rural areas and the microcredit as a driving force of entrepreneurial and commercialisation activities for households, SMEs growth continues to suffer from the credit gap. The mismatch of deposit and demand for credit have widened the credit gap.

The Rise of Digital Finance

Digital finance applications may be the solution toward the ineffectiveness of the conventional banking system. Digital finance is a platform to ease businesses and individuals' daily transactions and payment purposes. In order to complete such transactions, individuals are forced to deposit cash in their account. Hence, digital finance has a potential effect in bridging the credit and saving gap in Cambodia's financial market. The ADB (2019)[b] predicts that the capitalisation of financial inclusion gap will see an improvement of 32% of GDP, with a potential growth of 1.7$ billion in electronic transaction flows between parties and, capable of mobilising an additional $500 million of saving[c].

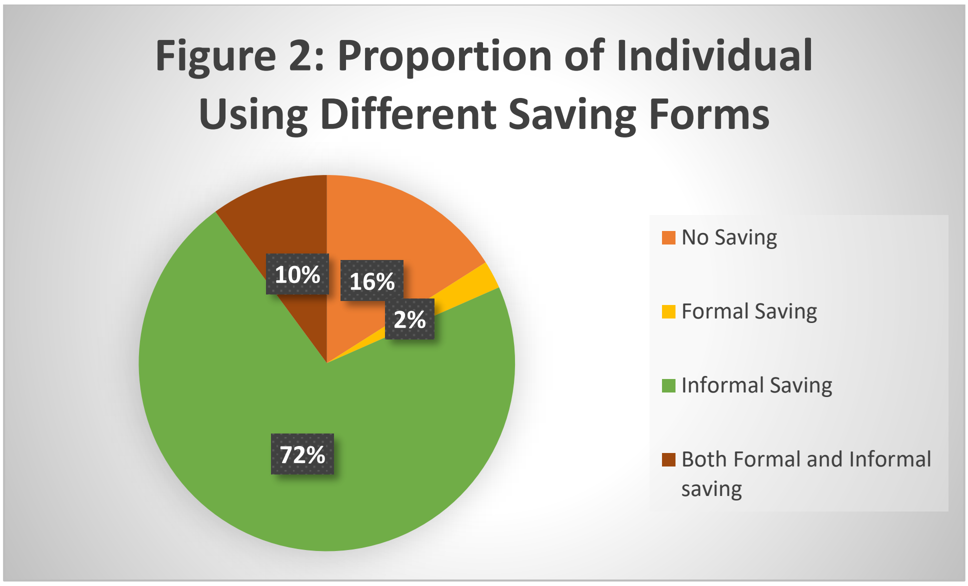


Figure 2: Proportion of Individual Using Different Saving Forms

Source: ADB[d]

Cambodia have been saving in various forms, as according to Figure 2, 16% of Cambodians have no saving behaviour and 72% of the population have been saving informally. Even if, the majority of Cambodians are participating in informal saving, this form of saving might not be sustainable and unable to promote saving behaviour amongst Cambodia. Informal savings could be saved in both liquid and illiquid assets. Saving in the illiquid assets are less flexible for the saver to convert those assets for their emergency needs[e]. As for making informal loans, saver might get exposed to liquidity risk and credit risk The practices of informal saving occur from one of the possibilities of the lack of connectivity and access to commercial banks and MFI branches. Digital finance provides convenience, accessibility, affordability and safety, all of which mitigates both the distance and transaction costs.

Financial Inclusion and Financial Stability

Inclusive financing through digital financial services will help diversify the financial sector and promote transparency of the monetary transmission mechanisms. Financial inclusion might come with financial instability. Thus, these challenges must be equipped with innovative regulations designed to protect financial stability in Cambodia.

Digital finance and P2P lending platforms might expose the specific group of individuals to further financial risks. Greater inclusion is associated with extensive borrowing from the individuals, as these practices will be extremely risky during a systematic event as it may disrupt the financial system. In fact, the lack in financial understanding can be held responsible for the mismanagement of money and financial planning. Cambodia's financial literacy rate is 11.8 out of the total possible score of 21[f]. This is well below the world average set at around 13.3. This is crucial toward maintaining financial stability, as there will be the higher probability that households will enter the vicious cycle called the debt trap[g]. The trade-off between financial inclusion and financial stability may be resolved through a well designed policy to foster further economic propensity.

Policy Recommendations

In the promotion of digital finance in Cambodia, different levels of strategies, innovation and regulations are needed. Government bodies and financial intermediaries need a wide range of approaches to intensify the practice of e-banking. Even though internet banking in Cambodia has expanded extensively, the P2P lending platform is still in the beginning stages of the ecosystem. Karprak is the only P2P lending platform in Cambodia to date.

Beyond the innovation of delivering products and services in the technological base, Cambodia needs to take the advantages of the new value in the digitalised age which is "Data". Modernising the individual 'credit score' through data monetarisation will allow traditional and modern banks to evaluate the creditworthiness of a larger pool of potential borrowers. The alternative method of credit scoring may be complementary to the conventional method of credit scoring.

Further, a stringent regulation framework needs to be prudent. Taking Indonesia as a case study for policy implications, where the state applied two frameworks being the 'principles base' and the 'collaborative approach' to regulate and facilitate the development of digital finance in Indonesia. With these two approaches, the policy aims to mitigate the proliferation of delinquent platforms in which they conduct business in an unethical style. Also, it aims to continuously keep control of the markets, assuring the ecosystem thrives. Although, the RGC and NBC have enacted E-commerce laws, consumer protection law and fintech regulations. The RGC and NBC need further framework in order to oversee the digital finance sector activities to thrive sustainably.

Beyond the points discussed above, financial education is crucial, in particular, Cambodia needs to buffer its financial literacy rate. Empirically[h], financial literacy is significant and positively correlated to improving financial inclusion. Financial education and general education teach individuals to be forward thinkers, and hence, it inspires saving behaviour amongst individuals. Educating the public with financial knowledge not only showcases the advantage of saving but educating the public on debt management and educating the public to invest smartly to prevent them from being indebtedness.

The opinions expressed are the author's own and do not reflect the views of the Asian Vision Institute.

[a] Pisei, Hin. "Ministry: SMEs Vital to Economy, but 95% Not Registered: Phnom Penh Post." Ministry: SMEs vital to economy, but 95% not registered | Phnom Penh Post. Post Media Co Ltd The Elements Condominium, Level 7 Hun Sen Boulevard Phum Prek Talong Sangkat Chak Angre Krom 12353 Phnom Penh Cambodia, August 25, 2019. https://www.phnompenhpost.com/business/ministry-smes-vital-economy-95-not-registered.

[b] Wyman, and Oliver. "Accelerating Financial Inclusion in South-East Asia with Digital Finance." Asian Development Bank. Asian Development Bank, April 5, 2019. https://www.adb.org/publications/financial-inclusion-south-east-asia-digital-finance.

[c] Wyman, and Oliver. "Accelerating Financial Inclusion in South-East Asia with Digital Finance." Asian Development Bank. Asian Development Bank, April 5, 2019. https://www.adb.org/publications/financial-inclusion-south-east-asia-digital-finance.

[d] Morgan, Peter J, and Long Q. Trinh. "Determinants and Impacts of Financial Literacy in Cambodia ...," June 2017. https://www.adb.org/sites/default/files/publication/325076/adbi-wp754.pdf.

[e] Ouma, Shem Alfred, Teresa Maureen Odongo, and Maureen Were. "Mobile Financial Services and Financial Inclusion: Is It a Boon for Savings Mobilization?" Review of Development Finance. No longer published by Elsevier, March 9, 2017. https://www.sciencedirect.com/science/article/pii/S1879933716301695.

[f] Morgan, Peter J, and Long Q. Trinh. "Determinants and Impacts of Financial Literacy in Cambodia ...," June 2017. https://www.adb.org/sites/default/files/publication/325076/adbi-wp754.pdf.

[g] Bopha, Phorn, Sokummono Khan, and VOA Khmer. "Cambodia's Debt Trap: Taking Out New Loans to Pay Back Old Loans." VOA. VOA Cambodia, September 11, 2019. https://www.voacambodia.com/a/cambodia-s-debt-trap-taking-out-new-loans-to-pay-back-old-loans/5074618.html.

[h] Morgan, Peter J, and Long Q. Trinh. "Determinants and Impacts of Financial Literacy in Cambodia ...," June 2017. https://www.adb.org/sites/default/files/publication/325076/adbi-wp754.pdf.

AVI COMMENTARY

ISSUE 2021, No. 07

Cambodia | 23rd April 2021

Facilitating Cross-Border E-Commerce through an Enhanced Postal and Customs Cooperation

SOK Kha[a]

Cambodia has experienced steady economic growth over the last two decades. Data from the Ministry of Economy and Finance shows the country maintained an average annual GDP growth rate of 7.7% from 2000 to 2019. The economy is driven by the private sector, where most businesses are small and family-run.

The context in which these businesses operate is dramatically changing due to the rapid technological and digital advancement and adaptation in the country over the past decade, with growing affordability and uptake of internet connectivity and smartphone-based value-added services. For instance, a report published by DataReportal suggests the number of internet users stood at 9.7 million in January 2020, a 1.3-million rise from the preceding year. Alongside, the e-commerce activities have trended upward significantly with the growth in tech start-up activities accompanied by increasing numbers of online payment gateways such as Wing Pay, ABA's PAYWAY, ACLEDA E-Commerce Payment Gateway, among others. A report by Statista highlights the revenue in the e-commerce market in Cambodia, expected to grow at an annual rate of 8.98% from 2021 to 2025.

Moreover, the enactment of the E-Commerce Law in November 2019 and the E-Commerce Strategy in November 2020 adds an even stronger momentum, providing an institutional, legal, and regulatory framework for electronic transactions and for accessing and sharing information and data in e-commerce transactions.

[a] **SOK Kha** is a Research Fellow at the Centre for Governance Innovation and Democracy (CGID) at the Asian Vision Institute (AVI).

The e-commerce turnout is expanding beyond Cambodia's national border, with small Cambodian e-traders engaging mostly with the international delivery of small packages. The flourishing of international postal items has illustrated this. For example, the Express Mail Service or EMS packages accounted for 47% of Cambodia Post's revenue in 2019, with the volume increasing by around 43% and 38% for outbound and inbound, respectively, from 2017.

In a previous AVI publication, the author highlighted that Cambodia had made remarkable improvements in digital trade facilitation, using modern information and communication technologies to simplify and automate cross-border trade procedures. Similar improvements are called for in response to the uptrend of cross-border e-commerce. Specifically, an enhanced cooperation of Cambodia Post and the Customs administration or the General Department of Customs and Excise of Cambodia (GDCE) will facilitate the movement of small packages across Cambodia's border.

This is particularly critical now than ever before when certain countries enforce new laws and regulations that require the Electronic Advance Data (EAD) for the postal items arriving at their soil. Those countries include the members of the European Union, the US, China, Russia, among others. The enforcement implies that Cambodia's postal shipments to the markets in those countries risk being returned or destroyed by their customs administrations as per their respective regulation, i.e., the EU-Import Control System and the US Stop Act, which come into effect in early 2022.

As a workaround, Cambodia needs to enable the EAD, allowing advanced data exchange of critical customs and security information of the postal shipment (i.e., sender, contents, and value) electronically between Customs Declaration System (CDS) of the Cambodia Post and ASYCUDAWorld (AW) of GDCE.

AW is the automated customs processing system implemented by GDCE at all ports and checkpoints to capture and process customs declaration data of export and import consignments. While the CDS, a system developed by the UPU Postal Technology Centre for its member postal operators, including Cambodia, can capture declaration data of the postal shipments, the linkage between CDS and AW is currently lacking. So, why is it both important and necessary for Cambodia to have a fully operational EAD? Overall, enabling the EAD will facilitate the cross-border movement of Cambodia's small package exports and imports. At least three reasons stand out.

First, it ensures the regulatory compliance of the outbound postal shipments to EAD countries. Without it, Cambodia's exporters risk having their postal items returned or destroyed due to security and safety measures imposed by certain destination countries. Second, the rapid growth in cross-border e-commerce puts increasing pressure on GDCE. It is the leading government agency responsible for revenue collection from the imports of low-value goods subject to duties and taxes. Besides revenue collection, GDCE has an equally high responsibility to prevent the importation of prohibited items from entering Cambodia. That means all merchandise imports, regardless of their value, are subjected to risk assessment and, where appropriate, checked by customs officials as part of the wider risk management process. Efficiency in this process can be improved if the capturing and processing of the customs declaration data of the import shipments can be carried out against risk selection criteria before their arrival. That also means expedited customs clearance procedures of postal items imported into Cambodia. Third, it contributes to progressing Cambodia's commitments under Article 7.1 on the Pre-Arrival Processing and Article 7.4 on Risk Management of the WTO Trade Facilitation Agreement (TFA).

In conclusion, establishing a fully operational EAD will strengthen the government's efforts in employing modern information and communication technologies in their reforms around cross-border trade facilitation, while at the same time benefiting Cambodia's private sector, which increasingly embraces the global e-trade and digital economy.

The views expressed are the author's own and do not reflect the views of the Asian Vision Institute.

AVI COMMENTARY

ISSUE 2021, No. 01

Cambodia | 11th January 2021

Digital Services Tax: Making the Case for Cambodia

SUN Molika[a], BA

Digital Economy and Corporate Tax

The digital economy makes people, organisations, devices, data and processes more connected via technologies and the Internet of Things (IoT). Hyper-connectivity has changed the way we live and do businesses. Traditionally, to sell a product or service, a physical store is needed and it should be located as near as possible to potential customers. However, with online businesses, a brick-and-mortar store is no longer a barrier. Online shopping, for instance, enables customers to review their buying options online and make payment via mobile banking. That being said, the digital business goes beyond this. Multinational technology companies, namely Google, Amazon, Facebook and Apple (GAFA), use technology and internet as input and platform to provide digital services to customers such as online advertisement, data transmission and sales of users' data. Since the way corporations earn their profits has changed, so has the way that tax is levied.

According to the Organisation for Economic Co-operation and Development (OECD), corporate incomes of a foreign enterprise are taxed on net incomes – gross incomes minus deductible tax expenses. This corporate tax is applicable in a jurisdiction only if that foreign enterprise has a permanent establishment where those incomes are generated. The term "Permanent Establishment" here is immensely salient in digital services tax (DST) because it determines whether or not a digital multinational company is subject to DST.

[a] **SUN Molika** is a Research Associate at the Centre for Inclusive Digital Economy (CIDE) at the Asian Vision Institute (AVI).

Permanent Establishment and Digital Services Tax

“Permanent Establishment” (PE) refers to the physical existence and ongoing revenue-generating activities of a business. As a business is taxed in a territory only if they have a PE there, the digital presence of a business has become a controversial issue. Many European governments have begun to realise the unjust practice of international taxation. While value is created by their citizens’ data, corporations are taxed by other countries (tax heaven).

Before diving deeper, the definition of “Digital Services Tax” (DST) must be defined. Simply put, DST is a tax charged on digital services that include but are not limited to search engines, social media platforms, online advertisement, online marketplace and sales of users’ data. For example, an individual in France uses Google to search for a tourist accommodation in Monaco. Once the user clicks on the commercial promotion of a resort in Monaco, France would treat revenues generated by this online advertisement as a DST, even though this transaction happened merely between Google and the resort in Monaco. As DST becomes a trending phenomenon among many nations around the globe, is it legally right to do so?

International Tax Law and Criticism

International tax law stipulates that corporate tax is applied to where a product is created rather than where consumers are physically located. Although the digital economy has enabled businesses to earn profits in foreign countries, they are not subject to corporate tax if they do not have a physical presence in that jurisdiction.

Unlike corporate tax whose tax base is net incomes, DST is structured to tax gross incomes, which has been criticised as an inefficient and anti-growth mechanism. For companies with slim profits, taxing gross incomes will be a huge loss for them because other associated costs such as deductible tax expenses are not subtracted before tax calculation. Thus, newly emerging businesses with insubstantial capitals might be hit by DST and discouraged to join the market. More importantly, as explained by the OECD, it is impossible to separate the digital economy from the traditional one. More and more production lines are connected to the Internet, so distinguishing which line shall fall under DST become a complicated task. To settle the debate, the OECD initiated a series of negotiations on DST participated by more than 130 countries and decided to require multinational companies to partially pay their income taxes where their consumers are located.

The US's Response and What to Expect

Since GAFA are originated in the United States, the US government will not stay quiet. After France decided to levy its DST on GAFA in July 2019, the US Trade Representative (USTR) investigated and found DST discriminatory under Section 301 of the US Trade Act of 1974. As such, the US is allowed to retaliate against this discriminatory action. To fight back, the US planned to impose $2.4 billion tariffs worth of cheese, cosmetic products, handbags and porcelain. Fortunately, this trade tension cooled down when France decided to postpone its tax collection to 2021 and kept working on the OECD's taxation on the digital economy. Even though this is a positive sign, the future is not promising as long as DST is being developed and levied by European countries. Therefore, the conflict of interests between the EU and the US might create tension in multilateral trade communities and eventually hurt international trade.

Digital Services Tax and Its Implication in Cambodia

Digital Services Tax is a viable idea for Cambodia to consider, as the country is at its early stage of digital economy transformation. E-commerce is everywhere ranging from online shopping and online food delivery to digital payment and others. In 2020, 58% of Cambodian people are active social media users, and Facebook alone shared 58.6% of total online activities. Furthermore, in the context of the COVID-19 pandemic, Cambodian tax revenues are declining while public expenditures on healthcare and government subsidies rise. Therefore, adopting a DST will be an additional source of tax incomes that helps the Cambodian government cope with current and future economic hardship.

Nevertheless, levying and collecting DST require a comprehensive feasibility study, strict compliance with the international tax system and well-rounded expertise to draft and implement this new tax law. Hence, Cambodia should keep track of DST regulations, especially those proposed and developed by the OECD, and learn from the success stories of other countries in implementing this new tax.

The views expressed are the author's own and do not reflect the views of the Asian Vision Institute.

AVI POLICY BRIEF

ISSUE 2021, No. 01

Cambodia | 21st January 2021

Techno-Nationalism and Techno Sovereignty

GILBERG Trond[a], PhD
CHHEM Rethy[b], MD, PhD (Edu), PhD (His)

Executive Summary

❖ The technological revolution of our time has several important ramifications for international relations and diplomacy. An early tendency in this process is for states to emphasise their technological development to meet the challenges of the revolution. This is *techno-nationalism*. But the major powers such as the United States and China also seek to persuade others to adopt their versions of the new technology, a policy that is called *techno-imperialism*. Techno-imperialism produces serious problems for small and medium-sized states, which are being pressured to adopt the Chinese or US technologies as part of the world-wide competition by the two superpowers.

❖ The alternative for smaller states is to adopt a policy of te*chno-sovereignty*, in which they seek to maintain national control over technological developments while cooperating with others for mutual benefit. In Cambodia, the policy of techno-sovereignty will be challenged by the relatively low level of the current technological infrastructure as well as financial constraints in infrastructural development. Human resources inadequacies represent another challenge.

❖ At the same time, there are bright spots and prospects in the development of institutions with a focus on science and technology, and the emergence of new leadership in the public and private sector, which will lead the way in confronting the challenges represented by the new technological revolution.

[a] **GILBERG Trond** is an Advisor to the Centre for Inclusive Digital Economy (CIDE) at the Asian Vision Institute (AVI).
[b] **CHHEM Rethy** is an Honourary Distinguished Fellow at AVI.

- Policy options for Cambodia:
  - Cooperation with all states based on mutual advantage but with full respect for national sovereignty and the implementation of a plan of international technology and information management;
  - Development of Cambodia's own technology base in a focused priority plan, in cooperation with relevant international stakeholders;
  - Intensification of human resource development in relevant fields, as exemplified by the young experts at the Asian Vision Institute (AVI);
  - Establishment of appropriate research, training and educational institutions in Cambodia that can serve as national and regional centres of excellence; and
  - Further development of existing programmes focusing on the use of advanced technology for peaceful purposes, including regional and international peacebuilding.

សេចក្តីសង្ខេបអត្ថបទ

- បដិវត្តន៍បច្ចេកវិទ្យាបានបង្កឱ្យមានផលវិបាកស្មុគស្មាញសំខាន់ៗមួយចំនួនទៅលើទំនាក់ទំនងអន្តរជាតិ និងវិស័យការទូត។ ដំណាក់កាលដំបូងនៃដំណើរបដិវត្តន៍នេះ តម្រូវឱ្យរដ្ឋនានាបង្កើនការអភិវឌ្ឍបច្ចេកវិទ្យារបស់ខ្លួនដើម្បីឆ្លើយតបទៅនឹងបញ្ហាប្រឈមដែលបង្កឡើងដោយបដិវត្តន៍នេះ។ នេះហៅថា «Techno-nationalism»។ ប៉ុន្តែ ប្រទេសមហាអំណាចដូចជាសហរដ្ឋអាមេរិក និងចិនក៏បានព្យាយាមបញ្ចុះបញ្ចូលប្រទេសដទៃឱ្យទទួលយកបច្ចេកវិទ្យាថ្មីរបស់ខ្លួន ដែលគោលនយោបាយនេះហៅថា «Techno-imperialism»។ Techno-imperialism បង្កជាបញ្ហាធ្ងន់ធ្ងរសម្រាប់រដ្ឋតូចៗ និងមធ្យមដែលកំពុងរងសម្ពាធឱ្យទទួលយកបច្ចេកវិទ្យារបស់ចិន ឬអាមេរិក ដែលជាការប្រណាំងប្រជែងរវាងមហាអំណាចទាំងពីរ។
- ជាជម្រើស រដ្ឋតូចៗអាចប្រកាន់យកគោលនយោបាយ «Techno-sovereignty» ដែលជាគោលនយោបាយគ្រប់គ្រងការអភិវឌ្ឍបច្ចេកវិទ្យារបស់ជាតិ ស្របពេលជាមួយនឹងការសហការជាមួយប្រទេសដទៃទៀតដើម្បីផលប្រយោជន៍ទៅវិញទៅមក។ នៅប្រទេសកម្ពុជា គោលនយោបាយ «Techno-sovereignty» ត្រូវប្រឈមនឹងបញ្ហាហេដ្ឋារចនាសម្ព័ន្ធបច្ចេកវិទ្យាទន់ខ្សោយ ក៏ដូចជាបញ្ហាកង្វះហិរញ្ញវត្ថុក្នុងការអភិវឌ្ឍហេដ្ឋារចនាសម្ព័ន្ធ។ កង្វះធនធានមនុស្ស ក៏ជាកត្តាប្រឈមមួយផ្សេងទៀតផងដែរ។

❖ ទន្ទឹមនឹងបញ្ហាប្រឈម កម្ពុជាក៏មានកាលានុវត្តភាពផងដែរ ដូចជាការកសាងស្ថាប័នដោយផ្ដោតទៅលើវិទ្យាសាស្ត្រ និងបច្ចេកវិទ្យា និងការលេចចេញនូវភាពជាអ្នកដឹកនាំថ្មីក្នុងវិស័យសាធារណៈ និងឯកជន ដែលនឹងត្រួសត្រាយផ្លូវក្នុងការដោះស្រាយបញ្ហាប្រឈមដែលបង្កដោយបដិវត្តន៍បច្ចេកវិទ្យាថ្មី។

❖ ជម្រើសគោលនយោបាយសម្រាប់ប្រទេសកម្ពុជា៖

- ○ ការធ្វើកិច្ចសហប្រតិបត្តិការជាមួយប្រទេសទាំងអស់ ដោយផ្អែកលើផលប្រយោជន៍ទៅវិញទៅមក ប៉ុន្តែដោយគោរពយ៉ាងម៉ឺងម៉ាត់ចំពោះអធិបតេយ្យភាពជាតិ និងការអនុវត្តផែនការគ្រប់គ្រងព័ត៌មាន និងបច្ចេកវិទ្យាអន្តរជាតិ។
- ○ ការអភិវឌ្ឍមូលដ្ឋានបច្ចេកវិទ្យាទៅវិស័យអាទិភាព ដោយសហការជាមួយភាគីពាក់ព័ន្ធអន្តរជាតិនានា។
- ○ ការពង្រឹងការអភិវឌ្ឍធនធានមនុស្សក្នុងវិស័យពាក់ព័ន្ធ។ ឧទាហរណ៍៖ អ្នកជំនាញវ័យក្មេងនៅវិទ្យាស្ថានចក្ខុវិស័យអាស៊ី (AVI) ជាដើម។
- ○ ការបង្កើតស្ថាប័នស្រាវជ្រាវ បណ្តុះបណ្តាល និងអប់រំ ដែលអាចដើរតួនាទីជាមជ្ឈមណ្ឌល «Centres of Excellence» ថ្នាក់ជាតិ និងតំបន់។
- ○ ការបន្តអភិវឌ្ឍកម្មវិធីដែលមានស្រាប់ ដោយផ្តោតលើការប្រើប្រាស់បច្ចេកវិទ្យាជឿនលឿនសម្រាប់កសាងសន្តិភាពទាំងក្នុងតំបន់ និងអន្តរជាតិ។

Introduction

For a quarter of a century, globalism and globalisation were the buzz words of international relations and diplomacy. A seemingly unstoppable process of technological innovation produced a near revolution in communications and the way increasing numbers of people worked. Computerisation and robotisation changed both the workplace and the conditions of everyday life. International relations increasingly were based on the soft power of knowledge and information transmission. A gap developed between the high-tech states and firms, on the one hand, and low tech, labour-intensive economies, on the other hand. Internally in virtually every state, a so-called digital divide developed between those who had the required skills in the new economy and society and those who did not. An underclass of marginalised people developed in every country and every society, while a new class of technology entrepreneurs and specialists emerged. Since power was now increasingly soft rather than hard, new constellations emerged in international relations, where smaller states with a highly developed technological base play more vital roles even if they had relatively small populations and small territories (Stiglitz 2002).

Globalisation predictably led to countermoves, even in the heyday of its process. Many people began to feel alienated, controlled by technological forces and manipulators that were beyond control. Large corporations with technological expertise were perceived to be out of control, and individuals and groups, particularly those who were left behind and marginalised, turned their alienation into political movements focusing on nationalism, patriotism and pride in traditional values. A good example of this countertrend was in states such as Hungary and Poland in the alleged poster boy of integration and globalism, the European Union (EU) (Bonciu 2017). Globalism did not beget nationalism but produced a confrontation between the two processes and conditions. Once again, it became clear that global performance was plagued with its own severe problems; those analysts who had predicted the demise of the state got a rough awakening in the global financial crisis of 2007-2008, where the state had to intervene in many places to save the very system that was supposed to make this institution wither away. This contradiction between globalism and statism often expressed as nationalism continues today (Gellner 1983).

For a more detailed understanding of the concepts utilised here, brief definitions are in order. Globalism has been defined as a condition in which events and processes in one country are directly related to developments elsewhere and influenced by events elsewhere so that global processes become more important than those in any single country. This condition is driven by a process of globalisation. One of the drivers of globalisation is the process of digitalisation, namely the increasing amount and importance of communication driven by the development and expansion of computers and computer-based information and communication. The role of the state (statism) has presumably been reduced in international relations. During the last decade or so, criticism has been voiced of the process of globalisation, and in several countries, politics have swung back towards an emphasis on the state and its role in political and socio-economic life. This trend is, predictably, called statism. As will be seen below, this trend has been strengthened by the world's response to the COVID-19 pandemic. And computerisation has increased soft power, the power of information and digital communication, at the expense of hard power (military and industrial power).

The Big Powers and Techno-Nationalism

After the end of the 1990s, the American decade of hegemony, there emerged an international system, first bipolar, where the United States was confronted with the rapidly rising power of China, and then, to a lesser but still important degree, a modified multipolar system, with re-emerging Russia as a third player. Eventually, other powers such as Japan also became a key player in this complicated relationship, while the EU, once thought to be the new major power in international relations and diplomacy, began to feel the process of internal tensions between the "federalists" and "autonomists". As the technological revolution, exemplified by AI, 5G and other aspects of cyber competition accelerated during the last few years, the major powers increasingly competed in technological advancement, in a form of techno-nationalism.

Techno-nationalism describes a situation where each state emphasises its own technical and scientific development and seeks to protect this development from others. This was increasingly the case in the steadily intensifying competition between the United States and China. The United States, having enjoyed a clear advantage in various forms of high tech, was now confronted by a serious challenge from rampant Chinese technological developments (Hoyama 2020). As is often the case in big power competition, the first tendency is for each contender to turn to nationalism and an attempt to increase national power. But the nature of the technological revolution is, by its very nature, global; all states will have to respond to it or suffer the fate of being left behind, marginalised and reduced to labour-intensive industry and eventually, economic irrelevance. But since the United States and China were competing in global technologies, it soon became necessary for both competitors to take the fight to others in the form of persuading or bullying other states to accept and implement the US version or the Chinese alternative. We can call this process one of turning techno-nationalism into techno-imperialism conducted by the two global powers. Techno-imperialism is the attempt by major powers to entice or force other states to accept a particular version of the technology (MIT Technology Review 2020).

The Two Versions of Techno-Imperialism

Today, there are two distinct versions of techno-imperialism, as evidenced by the approach of China vs the United States. The Chinese are emphasising the alleged win-win aspect of adopting Chinese-based technology, a form of a common quest for prosperity and a common future moving towards a brighter society for all. Recently, China produced a programme for the shared use of technology that emphasises these points. In adopting this line, the Chinese leadership emphasises its respect for national sovereignty, multilateralism and shared gains. This was discussed in the Chinese state news agency Xinhua on 8th September 2020, entitled "Global Initiative on Data Security" (Xinhua 2020). The United States, on the other hand, is taking a more aggressive stance, attempting to hinder or eliminate Chinese competition and threatening punishment in various forms for those who do not go along with Washington' wishes (Hoyama 2020). This was vividly demonstrated by the US response to a global pandemic, in which the United States became an outlier that refused to support the World Health Organization, thereby exhibiting an extreme form of techno-nationalism, whereas China became a strong backer of global efforts to fight a global problem. The defensive tone is evidenced in the US programme of information and technology control. This may be an artefact of the approach to foreign relations exhibited by the Trump administration, but more likely it is a natural reaction to a hegemon being challenged seriously by an upstart. To be prudent, smaller states should assume that the competition between the US and China will not go away even with a potential new administration in Washington after the 2020 election (MIT 2020).

Small State Alternative: Techno-Sovereignty

Small states like Cambodia, with a relatively weak national technological base, at first glance seem compelled to be subordinated by one or the other of the versions of techno-imperialism. But this would be a negative outcome of the present situation. It is therefore proposed that Cambodia should adopt techno-sovereignty, which has been advocated by some commentators. Essentially, it states that a state will cooperate with others for the mutual benefit of the use of technology, but each state will retain sovereign control of the use of technological processes and development. This condition would have several major aspects to it, as follows:

- Cooperation with all states based on mutual advantage but with full respect for national sovereignty and the implementation of a plan of international technology and information management;
- Development of Cambodia's own technology base in a focused priority plan, in cooperation with relevant international stakeholders;
- Intensification of human resource development in relevant fields, as exemplified by the young experts at the Asian Vision Institute (AVI);
- Establishment of appropriate research, training and educational institutions in Cambodia that can serve as national and regional centres of excellence; and
- Further development of existing programmes focusing on the use of advanced technology for peaceful purposes, including regional and international peacebuilding.

If we can begin the process of achieving these goals and objectives, it would be a win-win situation for Cambodia and ultimately the world.

Obstacles, Challenges and Prospects

The policy recommendations listed above will meet with major obstacles and challenges in Cambodia's foreign policy on this crucial issue. Cooperation with other states is challenged by the very aspect of techno-imperialism discussed above. The United States and other Western powers, while competing among themselves in various areas, are beginning to express increased dissatisfaction with Chinese policies in a variety of areas, and this scepticism is matched by apprehension about the Chinese foreign policy offensive in parts of the world and the increasing power of the eastern giant in the global economy, despite the need to cooperate with Beijing in economic matters. China is also increasingly viewed negatively, both institutionally and in terms of the characteristics of the personalities of the leadership, including President Xi Jinping. This negative perception is also fuelled by alleged Chinese human rights violations in regions populated by ethnic minorities.

While perceptions of China are increasingly turning negative in the West, there is a certain optimism expressed in terms of the change to a new administration in the United States, which will certainly seek to improve its relations with traditional allies, thereby hoping to increase the likelihood that Washington's techno-imperialism will become more acceptable (Silver 2020). Whether this is a realistic assumption will soon be put to the test. But it should be noted that the present chaos in the United States, with serious challenges to the very political order itself, is putting major obstacles in the way of Washington's efforts to reclaim its position in the world. For small states, the pressures produced by techno-imperialism in the past will most likely continue.

The improvement of Cambodia's technology base and the further development of the human resources of the country will also meet with problems and obstacles. The infrastructure of the new technology is expensive, and the Cambodian economy is suffering from the effects of COVID-19 and the characteristics of the economy itself, primarily based on labour-intensive and low value-added products such as garments, footwear and travel bags, plus some limited exports of rice and a few other agricultural commodities. Human resources development, while impressive at the upper levels of education, such as doctoral and master's degrees suffers from a very weak public education sector, particularly in the countryside. Again, massive investments will be needed to bring the general level of education to a point where techno-literacy needed for the new economy can be reached. By techno-literacy, I mean the ability to understand and use the new technology, at least in a basic way and Cambodia in this has a long way to go.

There are, however, some bright spots as the country struggles to deal with the massive challenges discussed above. One is the development of new educational infrastructure through the establishment of institutions of higher learning focusing on science and technology. Another very encouraging development is the new order among some public institutions and ministries, where key personnel have grasped the need for new ways of thinking and a new focus on the challenges confronting the country. With this kind of new leadership, the challenges discussed will be confronted because they must be confronted. The alternative is the old and outmoded policy focusing on producing t-shirts and shoes. That is the focus of the past. The technological revolution forces us to look ahead and to take appropriate measures to progress into that challenging but exciting future.

The opinions expressed are the author's own and do not reflect the views of the Asian Vision Institute.

References

Bonciu, Florian. "The New Characteristics of Globalization and Their Impact on the Design of a New International Economic Order." *Global Economic Observer* 5 (2017): 8-15.

Gellner, Ernest. 1983. *Nations and Nationalism*. Ithaca, NY: Cornell University Press.

Hoyama, Taisei. 2020. "US Stance on Huawei Wavering as Hawks Push for Crackdown." *Nikkei Asia Review*. Accessed on January 15, 2021. https://asia.nikkei.com/Spotlight/Huawei-crackdown/US-stance-on-Huawei-wavers-as-hawks-push-for-crackdown.

MIT Technology Review. 2020. "The Technonationalism." *MIT Technology Review*, September.

Silver, Laura, Kat Devlin, and Christine Huang. 2020. "Unfavorable Views of China Reach Historic Highs in Many Countries." *Pew Research Center*. Accessed on January 15, 2021. https://www.pewresearch.org/global/2020/10/06/unfavorable-views-of-china-reach-historic-highs-in-many-countries/

Stiglitz, Joseph. 2002. *Globalization and its Discontents.* New York, NY: W. W. Norton & Company.

Xinhua. 2020. "Global Initiative on Data Security." *Xinhua*. Accessed on January 15, 2021. http://www.xinhuanet.com/english/2020-09/08/c_139352274.htm.

AVI POLICY BRIEF

ISSUE 2020, No. 05

Cambodia | 26th March 2020

5G Geopolitics and Implications on Southeast Asia

BONG Angkeara[a], PhD
CHHEM Siriwat[b], MDTM

Executive Summary

- The US and China are in a new form of superpower race, fiercely competing head-to-head in 5G advancements. The significantly higher speed and connectivity of 5G has the potential to boost economies to new heights. However, this amplifying technology also concerns national security; allowing for faster cyberattacks, more vulnerable sites for attack, and the security of critical infrastructure and confidential data.
- The technological rivalry between the US and China creates a divide between all nations, forced into deciding which 5G providers to choose, from the two opposing sides. Southeast Asia is experiencing extremely fast technological adoption, due to their young population, affordable mobile data, and high mobile internet usage rate. These factors contribute to the potential of their digital economies, relative to the globe.
- Policy Options:
  - Promote regional and global cooperation to develop rules and norms for global governance of the cyberspace.
  - Create policies and laws to regulate economic and social development, while protecting national sovereignty and interests.
  - Foster public-private partnership between relevant ministries and telecommunications companies, to implement the suggested policies.
  - Develop a national talent strategy to absorb and implement 5G technology.

[a] **BONG Angkeara** is a Senior Research Fellow at the Centre for Inclusive Digital Economy (CIDE) of the Asian Vision Institute (AVI).
[b] **CHHEM Siriwat** is the Director of the Centre for Inclusive Digital Economy (CIDE) of the Asian Vision Institute (AVI).

សេចក្តីសង្ខេបអត្ថបទ

- សហរដ្ឋអាមេរិកនិងចិនគឺកំពុងតទល់គ្នានៅក្នុងទម្រង់ថ្មីនៃការប្រកួតប្រជែងដ៏ស្វិតស្វាញ ដើម្បីក្លាយខ្លួនជាមហាអំណាចនៃវឌ្ឍនភាពបច្ចេកវិទ្យាជំនាន់ទី៥ (5G)។ ល្បឿន និងការតភ្ជាប់ដ៏ឆាប់រហ័សរបស់បច្ចេកវិទ្យាជំនាន់ទី៥ គឺជាសក្តានុពលដ៏សំខាន់ក្នុងការជម្រុញកំណើនសេដ្ឋកិច្ចឲ្យឈានទៅដល់ចំណុចថ្មីមួយទៀត។ ទោះបីជាយ៉ាងណាក៏ដោយ បច្ចេកវិទ្យាដ៏មានអត្ថប្រយោជន៍នេះក៏បានបង្កជាក្តីកង្វល់ដល់សន្តិសុខជាតិតាមរយៈការអនុញ្ញាតឲ្យមានការវាយប្រហារតាមប្រព័ន្ធបច្ចេកវិទ្យាកាន់តែលឿន ចំនួនករណីវងការវាយប្រហារកាន់តែច្រើន និងសន្តិសុខនៃ ហេដ្ឋារចនាសម្ព័ន្ធសំខាន់ៗ និងទិន្នន័យសំងាត់។
- ការប្រកួតប្រជែងខាងផ្នែកបច្ចេកវិទ្យារវាងសហរដ្ឋអាមេរិក និងចិនបង្កើតឲ្យមានបំណែងចែកនៅគ្រប់ប្រទេស ដោយបង្ខំឲ្យពួកគេសម្រេចចិត្តថាត្រូវជ្រើសយកអ្នកផ្តល់បច្ចេកវិទ្យាជំនាន់ទី៥មួយណា ក្នុងចំណោមគូប្រជែងទាំងពីរនេះ។ ប្រទេសនៅអាស៊ីអាគ្នេយ៍គឺកំពុងស្រូបយកបច្ចេកវិទ្យាក្នុងកម្រិតមួយដ៏លឿនខ្លាំង ដោយសារតែរបាយប្រជាសាស្រ្តវ័យក្មេង តម្លៃអ៊ីនធឺណែតសមរម្យ និងអត្រាអ្នកប្រើប្រាស់អ៊ីនធឺណែតខ្ពស់របស់ពួកគេ។ កត្តាទាំងនេះរួមចំណែកទៅក្នុងសក្តានុពលដ៏ធំសម្បើមនៃសេដ្ឋកិច្ចឌីជីថលរបស់ពួកគេ ធៀបនឹងប្រទេសនានានៅលើពិភពលោក។
- ជម្រើសគោលនយោបាយ៖
  - លើកកម្ពស់កិច្ចសហប្រតិបត្តិការតំបន់និងពិភពលោកដើម្បីបង្កើតបទបញ្ញត្តិ និងបទដ្ឋានសម្រាប់អភិបាលកិច្ចបច្ចេកវិទ្យាសកល។
  - បង្កើតគោលនយោបាយ និងច្បាប់ដើម្បីធ្វើនិយ័តកម្មការអភិវឌ្ឍសេដ្ឋកិច្ច និងសង្គម ស្របពេលនឹងការការពារអធិបតេយ្យភាពនិងផលប្រយោជន៍ជាតិ។
  - ជម្រុញភាពជាដៃគូរវាងវិស័យសាធារណៈ និងឯកជនរវាងក្រសួងពាក់ព័ន្ធនិងក្រុមហ៊ុនទូរគមនាគមន៍នានា ដើម្បីអនុវត្តគោលនយោបាយទាំងនោះ។
  - អភិវឌ្ឍយុទ្ធសាស្រ្តទេពកោសល្យជាតិដើម្បីស្រូបយកនិងអនុវត្តបច្ចេកវិទ្យាជំនាន់ទី៥។

US and China

The fifth generation (5G) of wireless technology has become one of the key areas of technological competition between the United States (US) and China. 5G is designed to handle massive numbers of devices and high rates of data transmission, further increasing the interconnectivity between devices and people around the world. The speed of 5G promises to be 100 times faster than the fourth generation (4G) and will be essential to a future world of smart cities filled with endless devices connected to the Internet of Things (IoT)[a]. The tremendous impact of this technological advancement will be felt across the global economy and national security of each individual state[b].

The trade and technological rivalries between the US and China have escalated over the past few years. Economic and national security concerns of the US have grown, as China's industrial, technological, and economic development strategies have become more robust[c]. The major issues associated with 5G networks have become politicised. Both countries increasingly view the control of 5G, which is the next wave of advanced technologies and applications, as an urgent matter of economic and national security[d]. Although several nations are coming forward and claiming that they are ready to utilize 5G technology, with the commercialization of new generation devices, the surrounding infrastructure to support this network is not ready. Huawei (China), Verizon (US), Nokia (Finland), Ericsson (Sweden), and Samsung (Korea), are all in fierce competition to fully implement 5G at their respective national levels.

Implications on Southeast Asia

In this context, Southeast Asia remains one of the most dynamic markets estimated at USD50 billion in 2017 and expected to increase to USD200 billion by 2025. Huawei estimated that Southeast Asia provides opportunities worth USD1.2 trillion, with a potential of USD80 million for 5G service subscribers[e]. These capabilities will dramatically enhance the performance of mobile data networks by enabling new types of machine-to-machine communication, paving the way for the next generation of digital applications that require highly reliable access to massive amounts of data.

However, 5G networks create security concerns through the countless number of connected devices, due to the exponential increase in data volume that challenges the detection of malicious traffic. The advent of 5G will impact the way society is interconnected, extending the usage of mobile data from simple phones to many devices including cars, drones, roads, bridges, and buildings that either provide or utilize data[f]. In 2019, the US accused Huawei of stealing US intellectual property and lobbied their allies to keep Huawei out of their 5G networks, due to national security concerns. Yet, Huawei has denied the allegations. In response, Huawei filed a lawsuit against the US government, for restricting their federal agencies to use Huawei products. Huawei claimed that the US had no solid evidence to support that the former was linked to the Chinese government. On February 6th 2020, Huawei sued Verizon for allegedly using 12 of their patents without authorization, infringing their intellectual property rights. Although the aforementioned patents were not directly related to 5G, they were all key components of network communications technology. Whether or not these two companies are linked to their respective governments, they act as proxies in this tense international rivalry. One must remember that this technological battle is not only taking place in the commercial arena, but its potential extends into military issues. The utilization of 5G would enhance new forms of cyberwarfare, creating a new superpower race to lead the world, based on technological capabilities. Beyond the political fight over 5G, the US and China are competing to develop innovative applications that will run on top of deployed 5G networks. Applications such as driverless cars, advanced factory automation, and smart cities will likely be the largest sources for long-term economic and political leverage from 5G.

Southeast Asia is readily integrating emerging technologies, including blockchain, Artificial Intelligence (AI), robotics, cloud computing, and financial technology (FinTech)[g]. However, for such technologies to truly reach their fullest potential, the pace of 5G deployment will depend on carrier preferences, government regulatory policies, strategies, and infrastructure, to capture value in a complex technology ecosystem. Thus, the ‘Power Transition Theory’ highlights the importance of innovation imperative, in which technological progress either drives or imposes constraints on global powers. So far, several countries in Southeast Asia have begun testing 5G. Singapore and Thailand are at the forefront of the 5G revolution and intend to implement by 2020. In the Philippines, Globe Telecom confirmed a partnership with Huawei to develop 5G by supporting the Philippines’ controversial public safety campaign, related to the drug war associated to approximately USD383 million[h]. In Cambodia, the Prime Minister welcomed the 5G network as a major step for Cambodia’s economic and technological development[i]. In Myanmar, ZTE signed an agreement with the country’s launch of the 5G network. Vietnam is the only country in the region that has avoided Huawei technology, due to security concerns. Instead, Vietnam plans to be among the very first in the world to develop its own 5G technology. Paying close attention to the aforementioned cases, it is important to distinguish between the nations where 5G is being deployed, and which specific 5G company is being deployed. Geopolitical issues will have a large influence on which 5G companies are deployed in specific countries, due to issues of national security. Technology has become so crucial to a nation that advanced products are becoming key drivers in the dynamics of international relations.

Although, the US ban has created a rift with other allies and partners, countries in Southeast Asia can seemingly be divided into two categories, either linked with the US, or linked with China. Therefore, these countries will face difficult choices concerning whose 5G networks and applications to adopt. The respective governments are likely to come under pressure from the US to avoid dependence on China for 5G. In this context, Beijing has made the development of 5G networks as a national priority, including 'Made in China 2025'. If China successfully capitalises on this technology, it will be able to spread its 5G systems through the Belt and Road Initiative (BRI). One could argue that Huawei has risen to global leadership in 5G development. In contrast, the efforts by the US and its ties to exclude Chinese 5G networks will continue, with the US-China trade and technology rivalries showing little signs of slowing down. For this reason, the US has an advantage in terms of innovation capacity, but China will benefit from its head-start in implementing 5G applications within a structured ecosystem, penetrating the global market.

Finally, one should not underestimate the Chinese drive to reduce its country's dependency on US technology, through accelerated research and development in leading semiconductor technologies. Strategically, China will likely gain first-mover advantage in 5G as it moves towards commercial-scale deployment of its 5G network by 2020. The implications of how Southeast Asia responds is beyond merely 5G technology. The main issue at hand is about global technological dominance and the success of China's Digital Silk Road. 5G will revolutionise the global digital landscape via IoT, big data analytics, and AI. Until now, no country in the region including US treaty allies, is willing to support the ban for political reasons. After all, the security risks incurred from the use of 5G is not only related to this technology alone, but in context of both national policy and technical resources, designed to protect national critical infrastructures from cyberthreats. Narratives about 5G are not always based on scientific evidence resulting from rigorous technical assessment, but from the perspective of national interest and desire for global dominance.

Policy Options

For Southeast Asia to truly thrive in the Fourth Industrial Revolution, governments should work together to consider these challenges and develop collaborative solutions, to ensure that the benefits of new networks can be securely and effectively harnessed. Specifically, in the case of Cambodia, the decision to choose 5G technology should be based on the cost-benefit analysis of quality and productivity, while still cautiously considering the risks to national security. Public-private partnership is key - Smart Axiata and Cellcard are pushing the rollout for their 5G networks with support from local Huawei and ZTE vendors, and approval from the Ministry of Posts and Telecommunications to carry out commercial services in Cambodia. These local initiatives embody Cambodia's hunger for new technology adoption, a result to the nation's young population, affordable mobile data, and high mobile internet usage rate. 5G is after all, only a form technology. The implications of 5G are ubiquitous in the cyberspace. This cyberspace must be governed with proper laws and regulations to enable economic and social prosperity, while rigorously protecting Cambodia's sovereignty and its national interests.

The opinions expressed are the author's own and do not reflect the views of the Asian Vision Institute.

[a] Eurasia Group. 2018. *White Paper: The Geopolitics of 5G,* Eurasia Group Politics First, New York, United States.

[b] Sharun, Turton. 2019. *Huawei extends Asia dominance with Cambodia 5G rollout,* Nikkei Asian Review, Japan.

[c] "The Huawei Dilemma: Washington Still Stuck Trying to Balance National Security Against US Tech Supremacy", *South China Morning Post*, 1 November 2019, Accessed: 10 February 2020.

[d] Digital Watch. 2019. *5G Geopolitics: A Game of E-thrones,* Geneva Internet Platform, Geneva, 39: 1-12.

[e] "Cybersecurity and Geopolitics: Why Southeast Asia is Wary of a Huawei Ban", *The Strategist*, 5 October 2019, Accessed: 3 February 2020.

[f] Rajah and Tann. 2019. *5G in Southeast Asia: Legal and Regulatory Implications*, Rajah and Tann Asia, Singapore.

[g] "How 5G Can Transform Southeast Asia", The ASEAN Post, 22 January 2020, Accessed: 22 February 2020.

[h] Huong Thu. 2019. *A Collision of Cybersecurity and Geopolitics: Why Southeast Asia Is Wary of a Huawei Ban,* Global Asia, Seoul, Korea.

[i] "Cambodia's Adoption of Huawei's 5G Brings Risk to Freedom of Speech", *Voice of America,* 8 July 2019*,* Accessed: 15 January 2020.

AVI POLICY BRIEF

ISSUE 2020, No. 10

Cambodia | 14th August 2020

Submarine Cable Geopolitics

CHHEM Rethy[a], PhD

TRIPATHI Geeta[b]

GILBERG Trond[c], PhD

Executive Summary

- This article starts with a brief review of the history of submarine telecommunication cables. The data show that the Western world has dominated this technology for more than a century. This monopoly has recently been challenged by the emergence of new economic powers such as China, India and Brazil.
- Because controlling submarine optical cables technology is essential for both socio-economic and military power, some Western countries and the US still aim at maintaining their historical global leadership and dominance. While those powers still hold a quasi-monopoly of laying and operating those cables, new investments come now from the emerging markets, with Southeast Asia as the region with the highest growth rate. This increasing competition is essential for the strategic control of the cyberspace, where submarine cables are the foundational infrastructure.
- This article looks into the geopolitics of telecommunication technologies including 5G mobile networks and the Internet that underline the global power race to dominate both the submarine space and the cyberspace. Finally, it examines the 5G and cyber

[a] **CHHEM Rethy** is an Honourary Distinguished Fellow at the Asian Vision Institute (AVI).
[b] **TRIPATHI Geeta** is a Research Fellow at the Centre for Inclusive Digital Economy (CIDE) of the Asian Vision Institute (AVI).
[c] **GILBERG Trond** is Dean of the Faculty of Social Sciences and International Relations at the Pannasastra University of Cambodia. He is also an Advisor to the Centre for Inclusive Digital Economy (CIDE) at the Asian Vision Institute (AVI).

technology dimensions in order to enrich our understanding of the current dynamics of China-US nationalistic rivalry and their race to lead telecommunication technologies.

សេចក្តីសង្ខេបអត្ថបទ

- ❖ អត្ថបទនេះរៀបរាប់ត្រួសៗអំពីប្រវត្តិនៃខ្សែកាបទូរគមនាគមន៍ក្រោមទឹក។ ទិន្នន័យបានបង្ហាញថាប្រទេសលោកខាងលិចបានគ្រប់គ្រងបច្ចេកវិទ្យានេះអស់ជាងមួយសតវត្សទៅហើយ។ ភាពផ្តាច់មុខនេះត្រូវបានប្រកួតប្រជែងដោយការលេចឡើងនូវមហាអំណាចសេដ្ឋកិច្ចថ្មីៗដូចជា ចិន ឥណ្ឌា និងប្រេស៊ីល។
- ❖ ដោយសារតែការគ្រប់គ្រងបច្ចេកវិទ្យាខ្សែកាបអុបទិកក្រោមទឹកមានសារៈសំខាន់សម្រាប់សេដ្ឋកិច្ចសង្គម និងអំណាចយោធា ប្រទេសលោកខាងលិចមួយចំនួនរួមទាំងសហរដ្ឋអាមេរិកផងដែរ នៅតែមានបំណងចង់រក្សាតំណែងជាអ្នកដឹកនាំពិភពលោក និងឥទ្ធិពលដ៏យូរលង់របស់ពួកគេ។ ខណៈពេលដែលប្រទេសមហាអំណាចទាំងនោះស្ទើរតែកាន់កាប់ផ្តាច់មុខក្នុងការពង្រាយ និងដំណើរការប្រព័ន្ធខ្សែកាបទាំងនោះ ការវិនិយោគថ្មីៗបានលេចឡើងមកពីទីផ្សារថ្មីនៅអាស៊ាន ដែលជាតំបន់មួយមានអត្រាកំណើនខ្ពស់។ កំណើននៃការប្រកួតប្រជែងនេះ គឺមានសារៈសំខាន់ណាស់សម្រាប់ការគ្រប់គ្រងយុទ្ធសាស្ត្រនៃសន្តិសុខបច្ចេកវិទ្យាគមនាគមន៍ ដែលមានខ្សែកាបក្រោមទឹកជាហេដ្ឋារចនាសម្ព័ន្ធគ្រឹះ។អត្ថបទនេះពិនិត្យមើលទៅលើភូមិសាស្ត្រនយោបាយនៃបច្ចេកវិទ្យាទូរគមនាគមន៍ ដែលរួមមាន 5G បណ្តាញទូរស័ព្ទចល័ត និងអ៊ិនធើណេតដែលគូសបញ្ជាក់អំពីការប្រកួតប្រជែងអំណាចជា សកលដើម្បីគ្រប់គ្រងលំហសមុទ្រ និងលំហបច្ចេកវិទ្យាគមនាគមន៍។ ចុងបញ្ចប់ យើងពិនិត្យមើលអំពីទិដ្ឋភាព 5G និងបច្ចេកវិទ្យាគមនាគមន៍ ដើម្បីបង្កើនការយល់ដឹងរបស់យើងអំពី សក្តានុពលនៃជម្លោះបែបជាតិនិយមរវាងចិន និងអាមេរិក និងការប្រកួតប្រជែងរបស់ពួកគេដើម្បីភាពឈានមុខផ្នែកបច្ចេកវិទ្យាទូរគមនាគមន៍។

Introduction

The cyberspace has become an absolute necessity for mankind to be connected globally. It has become the new 'home of the mind' and has placed an unprecedented demand on communication networks. Cyberspace, in this emerging new world order, has to play a crucial role in both socio-economic situations for sustainable development and military communications. The world economy and security are highly dependent on submarine communication cables because they are the only path for telecom and internet communications. By holding the monopoly (more than 90%) of telecommunication data of the world, maintaining the dominance over the control of submarine optical cables is paramount for established powers of the 20th century. The recent emergence of China and India in the submarine cables and telecommunication industries is perceived as a threat to Western hegemony over the rest of the world because it is causing a shift in global geopolitical balance. The recent China-US trade war, the 5G paranoid narrative and more recently the politicisation of the COVID-19 pandemic are symptoms of this global power shift.

Brief History of Submarine Sea Cables

Designing the transoceanic submarine cables has been a quest for more than 160 years. The redundancies it can offer give it a geo-strategic importance since the submarine cables were born in 1820. The British first used telegraphy technology to consolidate their imperialistic expansion across the globe. Following the two World Wars, the US exerted their hegemony during the telephony era (1950s to 1980s). That period saw the technological transition from copper cables to fiber optic cables. Starting from the late 1980s, the rise of BRIC nations (Brazil, China, Russia and India) changed the dynamics of power struggle for the dominance of submarine cable era. The monopoly of Europe-US in laying submarine cables was fiercely challenged by those emerging technology powers (UNEP 2009).

Western Dominance Over Submarine Telecommunication and the Rise of the Rest

The Internet as we see today grew out of an American military project called DARPAnet or ARPANET (Advanced Research Projects Agency Network), which was founded in the 1960s with the goal to enhance intelligence activities during the Vietnam War. It is the first computer network that was born in the context of military intelligence. The Internet was a tool to collect intelligence abroad and at home, and “so the computer networks, which became the Internet, functioned as sensors in society in order to monitor unrests and demands.” (Jutel and Levine 2018, 3). Hence, the Internet is a surveillance weapon that was used for decades by many countries, whether they are democratic or authoritarian. Jutel and Levine (2018, 6) wrote, “To sell the Internet as a technology of democracy when it’s owned by giant corporations is ridiculous.”

In the last four decades, the Internet has been used increasingly in banking, insurance, e-commerce platforms (Alibaba, Amazon, etc.), socialising (Facebook, WeChat, etc.), and searching for things (Google, Baidu, etc.) creating its own world in cyberspace and accelerating internet economies. The importance of cyberspace does have the global implication of power and gives a new paradigm to the changing dynamics of conflicts among nations. The cyberspace is part of the “Anti Access/Area Denial” or A2/AD strategy (Russell 2017, 3–6).

As we examine the cyberspace, analysing its infrastructure becomes very critical as it makes the internet work, like DNS (Domain Name Service), ISP’s (Internet Service Provider) and ICANN (Internet Corporation for Assigned Names and Numbers) (ICANN 2020).

The physical layer of cyberspace comprises of submarine optical fiber cable, cell towers, satellites, servers and computers for voice and data communication. The submarine cable is carrying more than 99% of the voice and data traffic of the entire world, while satellites carry only 1% of the data with a speed that is 5 times slower. The cable landing station (CLS) is where submarine cable connects with terrestrial networks through a backhaul system. Submarine cable has the capability to meet the demand of the bandwidth hungry technologies like Internet of things (IoT), virtual reality and cloud computing. The cable landing station is a critical component of a submarine cable system contributing towards the geo-strategy and geo-economic influence for competing nations.

The current traffic indicates towards higher network bandwidth demands in the near future. Here various global players are competing for equipment or components inside cable landing stations. As of now in 2020, our ocean floor has 406 active submarine optical cables stretching over 1.2 million km in service globally. Amazon, Facebook, Google, and Microsoft own or lease more than 50% of global submarine cable capacity. These cables allow US$10 trillion in transactions every day while the Internet bandwidths are distributed unevenly globally. It is worth noting that there are around 100 cable breaks per year due to natural disaster. The ever-increasing maritime conflict further adds threats to our cyberspace and can be a disaster to macroeconomic development of emerging nations.

In the past few years, the submarine cable investments have shifted towards emerging markets with ASEAN as the highest growth rate region in the world. There is a strong correlation between bandwidth and GDP per capita, and a weak submarine connectivity is an obstacle to sustainable human development and keeps countries detaching from efficiencies of being part of the global digital economy moving towards Industry 4.0 or Globalisation 4.0 (World Development Report 2016).

In the last decade, the submarine cable has shifted towards emerging markets (Mordor Intelligence 2020). The surge in demands for submarine cables has led countries like the US, China, Russia and a few others to seek to control or wield their influence over the global networks under the ocean delivering the Internet, especially in the Asia Pacific region. According to the British Think Tank Policy Exchange's 2017 Report, the power of submarine cables enabled 15 million financial transactions per day and US$10 trillion financial transfer per day. This think tank raised some essential questions. Why are cables so vital to national and global security? Why are cables essential to the global economy? What are the threats to submarine cables? Is the international law adequate to protect submarine cables?

If we look at the length of the cables from both the users' and suppliers' perspectives, Huawei looks pale compared with American, French and Japanese firms. From the users' side, in 2016, Google owned 112,000 Km, Facebook 91,859 Km, Microsoft 6,605 Km, and Amazon 30,557 km. From the suppliers' side (2015–2020), SubCom laid 100,000 Km of cables, NEC 68,000 Km, ASN 49,000 Km and Huawei 6000 Km (TeleGeography 2020; Submarine Telecoms Forum 2020; Broad Band Now 2020; Huawei Marine 2020).

The race to control the submarine cables and the sea above have further added tension to the current geopolitical crisis of seeking to control the market and governance of submarine cables and subsequently the dominance of the cyberspace. All the considerations mentioned above raised crucial geopolitical questions about these cables that represent the vital infrastructure that fundamentally support not only the Internet economy but all the security challenges that are inevitable in this era of cyberspace (Policy Exchange 2017; United Nations 2020; UNCLOS 2020).

Geopolitics of Submarine Cables

The discussion above has amply demonstrated the essential functions of submarine cables in national and global economies in the era of globalisation of communication that we live in today. But this is not an entirely new phenomenon. As discussed above, even in the 19th century it was understood that socio-economic and commercial development required a communications system that was relatively secure and to a large extent unhindered by national borders. Already then it was clear that improved communication would be essential for development. It would also become an object of rivalry between states, and that those who were strongest in technological and military terms would most likely dominate the field of communications as well, leading to a sharp division between the haves and the have-nots.

Submarine cables became an essential feature of hard power, the capabilities of states to use communications as part of the components of power traditionally understood in international relations and foreign policy, such as military capability, hardware (tanks, planes, artillery) and human assets (the public and private as well as specialists in communications). Communications became increasingly crucial elements in soft power as well, through imaging, transmission of intelligence, entertainment, propaganda, and the escalating contest over how others perceive you and your country's achievements. The importance of both hard and soft power was discussed by major analysts decades ago (Nye Jr. 2009, 160–163). And, given a variety of factors including some discussed above, the US became the dominant player in the soft power competition. One of the reasons for this was the near dominance of the US in the development of the Internet and telephone communications. A crucial aspect of this dominance was the advantage the US and its allies had in the construction and maintenance of submarine cables.

Several factors have combined together to change this landscape of near American dominance. First of all, the explosive development of China as an economic, military and technological superpower has begun to challenge the US hegemony in all areas of power, be they hard or soft. In fact, in some areas China is ahead of the US technologically. Secondly, the Chinese state view power as a composite and drive their development forward through smart policies, which at least at this time appear to have an advantage over the sometimes chaotic and competitive policies found in more open societies.

While it is possible that the creative forces unleashed by such a competition will prove superior to the more directed policies of the Chinese, this is by now by no means certain, a fact that explains the near panic in the US over the Chinese advances in 5G technology, as evidenced by the frantic efforts by Washington to bar others from buying into Huawei and other Chinese developers. This 5G pivotal juncture is another Sputnik moment for the US (Atlantic Council 2019). This multifaceted revolution has enabled the Chinese to go on the offensive campaign in many areas of technology. And in order to compete successfully, the Chinese leadership knows that the control over, or at least more influence in the management of the nexus of communication, namely submarine cables, is necessary.

A final factor in this complex development is the decline of the US as a global power, as discussed by many analysts. This decline may be explained by the cycle of history notion (that states grow and then decline, like the human body) or by, certainly in the last three or four years, a US foreign policy that has focused on isolationism and conflicts with presumptive or real allies and its disastrous approach to China, which has resulted in a trade war and open verbal confrontation, mostly in a cynical display of opportunism rather than of a strategic policy based on the facts of life in international relations. Under these circumstances, there is no incentive for China to cooperate with the US in a crucial field such as telecommunications.

It should be made clear that Beijing has a strategy of its own and that the Chinese actions in the competition for the nexus of communication, especially submarine cables, are part of a long-term and overall quest for China to be a competitor with the US for global influence. Other parts of this strategy are the Belt and Road Initiative (BRI), the increased involvement with less developed countries in economic terms, and as a promoter and protector of major international organisations such as the World Health Organization (WHO) during the COVID-19 pandemic. Against this, the Trump Administration offers a sharp and opposing narrative based on exceptionalism and protectionism while disengaging from many multilateral organisations or international agreements. At least for now, there can be little doubt as to who is winning in this geopolitical competition and the crucial battleground to maintain the current US dominance over the submarine cable system.

The US's near monopoly in cable construction and management is being challenged not only by China, but also by Brazil, Russia, India, and members of ASEAN. Still, it is the challenge from Beijing that worries Washington the most (South China Morning Post 2019). Against this US quasi monopoly over the submarine cables, Huawei together with Unicom, China Telecom, and the China Ministry of Industry & Information Technology have recently submitted a revolutionary standard for network technology to the International Telecommunication Union (ITU). This transformative approach to the "New IP" (Internet Protocol) proposed by China has won the support of Russia. This alliance will certainly create a new geopolitical landscape for the global battle to control the fundamental infrastructure of the Internet. The RIPE/EU have already expressed a clear opposition to China's proposal for a new IP system. The EU is of the opinion that the establishment of Internet standards should be the prerogative of the Internet Engineering Task Force (IETF) rather than of the ITU/UN where political influence prevails over technical evidence (Belt and Road News, 2020).

There is abundant literature on this subject. Malecki and Hu (2009) provided a comprehensive overview of this competition in the Annals of the Association of American Geographers. Rishi Sunir also discusses the essential insecurity of submarine cables in Policy Exchange (Malecki and Hu 2009). Winseck (2017) examined the issue of cables in The Geopolitical Economy of the Global Internet Infrastructure. More articles can also be found in various media publications, such as in (South China Morning Post 2019), Japan Times (The Japan Times 2019) and The Wall Street Journal (The Wall Street Journal 2019). The conclusion of all these pieces of research is that the geopolitics of cyber conflict is increasingly playing out in the case of submarine cables, the life nodes of communication and commerce in the globalised world in which we live. This is an epic struggle that will have to be resolved through compromise and cooperation, not trade wars and confrontation. For now, the Chinese challenge to earlier US dominance is a crucial aspect of submarine cable geopolitics.

The opinions expressed are the author's own and do not reflect the views of the Asian Vision Institute.

References

UN Environment Programme. 2009. "Submarine Cables and the Oceans: Connecting the World."

https://www.unepwcmc.org/system/dataset_file_fields/files/000/000/118/original/ICPC_UNEP_Cables.pdf?1398680911

Jutel, Olivier and Yasha Levine. 2018. "In Surveillance Valley: An Interview with Yasha Levine." *Springerin* 3.

Russell, Alison L. 2017. *Strategic A2A/AD in Cyberspace.* New York: Cambridge University Press.

ICANN. 2020. "The Internet Corporation for Assigned Names and Numbers." https://www.icann.org/

World Development Report. 2016. "Exploring the Relationship Between Broadband and Economic Growth."

http://pubdocs.worldbank.org/en/391452529895999/WDR16-BP-Exploring-the-Relationship-between-Broadband-and-Economic-Growth-Minges.pdf

Mordor Intelligence. 2020. "Submarine Optical Fiber Cable Market - Growth, Trends, and Forecast (2020 –2025)."

https://www.mordorintelligence.com/industry-reports/submarine-optical-fiber-cable-market

TeleGeography. 2020. "Submarine Cable Map." https://www.submarinecablemap.com/

Submarine Telecoms Forum. 2020. "Submarine Cable News Now." https://subtelforum.com

Broad Band Now. 2020. "The Largest Database of Broadband Providers." https://broadbandnow.com/

Huawei Marine. 2020. "Experience." http://www.huaweimarine.com/en/Marine/Home/Experience

Policy Exchange. 2017. "Undersea Cables: Indispensable, insecure."

https://policyexchange.org.uk/publication/undersea-cables-indispensable-insecure/

Sustainable Development Goals: Knowledge Platform, United Nations. 2020. "United Nations

Convention on the Law of the Sea (UNCLOS)." https://sustainabledevelopment.un.org/topics/oceans/UNCLOS

"United Nations Convention on the Law of the Sea."

https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

Nye Jr., Joseph S. 2009. “Get Smart: Combining Hard and Soft Power.” *Foreign Affairs* 88:160–3.

Atlantic Council. 2019. “The Race to Secure 5G Networks: Another Sputnik Moment for the United States?”

https://www.atlanticcouncil.org/blogs/new-atlanticist/the-race-to-secure-5g-networks-another-sputnik-moment-for-the-united-states/

South China Morning Post. 2019. “Undersea US-China Tech War’s New Battleground: Internet Cables.”

https://www.scmp.com/week-asia/politics/article/3042058/us-china-tech-wars-new-battleground-undersea-internet-cables

Belt and Road News. 2020. “China & Huawei Propose Reinvention of the Internet.”

https://www.beltandroad.news/2020/03/29/china-huawei-propose-reinvention-of-the-internet/

Malecki, Edward J., and Wei Hu. 2009. “A Wired World: The Evolving Geography of Submarine Cables and the Shift to Asia.” *Annals of the Association of American Geographers* 99:360–82.

Winseck, DWayne. 2017. “The Geopolitical Economy of the Global Internet Infrastructure.” *Journal of Information Policy* 7:228–67.

The Japan Times. 2019. “China’s Next Naval Target is the Internet’s Underwater Cables.”

https://www.japantimes.co.jp/opinion/2019/04/16/commentary/world-commentary/chinas-next-naval-target-internets-underwater-cables/#.XvwIPUBuLIV

The Wall Street Journal. 2019. “America’s Undersea Battle with China for Control of the Global Internet.”

https://www.wsj.com/articles/u-s-takes-on-chinas-huawei-in-undersea-battle-over-the-global-internet-grid-11552407466

AVI COMMENTARY

ISSUE 2019, No. 15

Cambodia | 14th December 2019

Geopolitics of Rare Earth Elements in the Asia-Pacific Region

HUL Seingheng[a], PhD

CHHEM Siriwat[b], Master in Digital Technology Management

Rare Earth Elements (REEs) are essential ingredients in contemporary electrical products such as smartphones, vehicles, and even military equipment. The quality of these products relies mainly on the concentration, types, and purity of these elements. As a result, the supply and demand for REEs have become increasingly sensitive with the emergence of the US-China trade war. Furthermore, these non-renewable resources have gained even more traction, due to dynamic economic growth in the Asia-Pacific region, namely China, India, and ASEAN nations. Many high-tech industries that are underlying this growth, are driven by the utilization of REEs. The market for REEs, dominated by China, represents a new dynamic in the geopolitics of the Asia-Pacific region, enhanced by the US-China trade war.

The term Rare Earth Elements (REEs), could be considered a misnomer. Located mostly in the bottom second row of the periodic table, these REEs are known as lanthanides. Scandium and Yttrium are exceptions, due to their occurrence in the same ore deposits as the lanthanides, attributing similar chemical properties. They have been prioritized as the "Vitamins of Modern Industries" and are indispensable and irreplaceable in electronic, metallurgic, magnetic, catalytic and technological areas. These 17 elements are classified into three groups: including light REEs (the highest demand in the market), Medium REEs, and High REEs, based on increasing atomic number. Each group has its own chemical and physical properties, with different functions in industrial applications. These metals are not easily purified from their the

[a] **HUL Seingheng** is Director of the Research and Innovation Center (RIC) at the Institute of Technology of Cambodia (ITC) and a Research Fellow at the Centre for Inclusive Digital Economy (CIDE) at the Asian Vision Institute (AVI),
[b] **CHHEM Siriwat** is Director of CIDE, AVI.

naturally-occurring ores, but are more commonly extracted from carbonates, fluorides, phosphates, oxides or silicates. Getting the highest purity of these elements has been a significant challenge for process engineers.

Their unique silver colour, in combination with high lustre and electrical conductivity, make them very useful in the application of modern industries. The global supply chain of high-tech industries requires these elements, in order to improve the efficiency of their final products. Their exceptional functions are found in high-tech applications such as cancer treatment, rechargeable batteries, advanced ceramics, computers, watches, wind turbines, catalysts in cars and oil refineries, televisions, lighting, lasers, precision lenses, fibre optics, superconductors, and glass polishing. Moreover, REEs are in demand for military equipment including jet engines, missile guidance systems, missile defence system, and satellites.

The rising demand of these elements in the global market has caused international trade to become more volatile. The supply chain is susceptible since REEs are small and concentrated around a handful of suppliers, namely China, Australia, Malaysia, Myanmar, and Russia. There are four stages prior to its readiness for use in product development by factories. The stages consist of exploration, mining with legal commercial permission, processing, and production by isolation of elements based on needs.

Competitive pricing and advanced processing technology in China, put them at the forefront on an international scale. Furthermore, China's vast reserve and production capacity increases global dependency on Chinese REEs, further strengthening their presence international trade. The shift in monopoly of the REE market began in 1987 after Deng Xiaoping's statement: "The Middle East has its oil. China has rare earths". The Senkaku-Diaoyu island disputes between Japan and China in 2010, also impacted the REE supply chain, due to both nations' involvement in the same market. Currently, the market share of REEs shows China controlling 90% of global exports and 80% of US REEs imports are from China. While the uncertain impacts from the US-China trade war persists, the tariff by China on REE exports to the US remains an obstacle for high- tech product manufacturing. This tit-for-tat game between the two superpowers could push China to intervene in the supply chain of REEs. If this occurs, the potential consequences could be grave and would be felt by all actors involved.

However, the REE market could be counter-balanced by other nations by increasing local production, developing mine prospects according to price fluctuations, and reusing, recycling, substituting alternative sources of the minerals, all backed by government policies. The impacts on the REE market were evaluated by inter-locked scenario analysis, described in the review paper published in 2018 by the Materials Research Society on “Rare Earths: A Review of the Landscapes”.

The possible change of China’s policy on REE supply could allow other countries to explore substitutes. ASEAN, however, has paid little attention to the discovery, processing technology, and market segmentation of REEs, albeit a minor supply of the materials by Malaysia and Myanmar. Back in 2012, a Chinese company showed interest in building a REE plant in Laos, but was rejected due to environmental reasons. Most of the ASEAN nations are in the emerging stage of their economies, requiring more electrical products that utilise REEs. However, they lack REE policies and specialised human resources. Japan has placed eyes on Kazakhstan, Vietnam, in addition to its own sources, while India has initiated exploration on its sea floors. The possible economic opening of North Korea could be another key factor, due to its abundant source of REEs.

However, studies have shown that the aforementioned nations might face technological challenges in mineral processing, environmental impact, regulation, and pricing. The best option for developed nations, based on these constraints could be the recycling of REEs from waste. Likely, most nations will continue to depend heavily on China for sustaining the supply chain of REEs, unless policy actions are taken from both demand and supply side. Cambodia could potentially source their own REEs, if more focus was emphasized on their mining and future resource management. Consequently, REEs are not just valuable metals used in production, but significant geopolitical drivers in the Asia-Pacific Region. These elements play a crucial role in the US-China trade war, amplified by the increasing global demand for the manufacturing of electrical products.

The views expressed are the author’s own and do not reflect the views of the Asian Vision Institute.

AVI PERSPECTIVE

ISSUE 2020, No. 07

Cambodia | 27th May 2020

Myanmar in the Global Geopolitics of Rare Earth Elements (REEs)

OO Zeyar[a], Master in Public Administration and MA in English

Executive Summary

- ❖ Rare Earth Elements (REEs) are all sources of today's innovation and advanced technology that constitute a range of sophisticated and high-tech products for both civil and military use.
- ❖ Growing demand for REEs by global nations such as the United States, Japan, the EU and some other technologically-advanced nations, has reinforced China's legitimate domination of REEs in the global market and believed to have posed threats to global geopolitics in one way or another.
- ❖ The changing perception of global nations on Chinese REE supply power has shifted to the cooperation with non-Chinese countries for REE production. At the expense of geopolitical conflicts of REEs, the global market gap may open up at any time in the future, providing opportunity for non-Chinese REE countries like Myanmar to fill in the gap.
- ❖ In 2008, Myanmar became a net exporter of Chinese REEs, ranking as the world's fourth highest position among the countries which are extracting REEs. However, Myanmar could not benefit properly from REEs mining and trading as it should have, due to domestic conflicts and inadequate laws, as well as the need for sound policy applicable to REE exploration and trading.

[a] **OO Zeyar** is a Research Fellow at the Centre for Inclusive Digital Economy (CIDE) at the Asian Vision Institute (AVI).

- Thus, this paper studies the global geopolitics of REEs, entailing the market gap, and explores Myanmar REEs in global geopolitics and defines policy options for Myanmar to deal with REEs production in the future.

សេចក្តីសង្ខេបអត្ថបទ

- ធនធានរ៉ែកម្រ គឺជាប្រភពនៃនវានុវត្តន៍និងបច្ចេកវិទ្យាទំនើបទាំងអស់ ដែលបង្កើតទៅជាផលិតផលទំនើបៗជាច្រើនសម្រាប់ការប្រើប្រាស់ទាំងផ្នែកស៊ីវិលនិងយោធា។
- កម្រើនតម្រូវការនៃធនធានរ៉ែកម្ររបស់ប្រទេសនៅជុំវិញពិភពលោកដូចជា សហរដ្ឋអាមេរិក ជប៉ុន សហភាពអឺរ៉ុប និងបណ្តាប្រទេសមានភាពជឿនលឿនខាងផ្នែកបច្ចេកវិទ្យាដទៃទៀត បានពង្រឹងអំណាចគ្រប់ដណ្តប់ទីផ្សារសកលស្របច្បាប់របស់ប្រទេសចិនទៅលើធនធានរ៉ែកម្រ ដែលត្រូវបានគេជឿជាក់ថានឹងបង្កការគំរាមកំហែងដល់ភូមិសាស្ត្រនយោបាយសកលតាមរបៀបមួយឬច្រើនយ៉ាង។
- បំលាស់ប្តូរទស្សនៈរបស់ពិភពលោកទៅលើអំណាចផ្គត់ផ្គង់ធនធានរ៉ែកម្ររបស់ចិន បាននាំទៅរកកិច្ចសហប្រតិបត្តិការជាមួយបណ្តាប្រទេសនានាក្រៅពីចិនសម្រាប់ផលិតកម្មធនធានរ៉ែកម្រ។ ដោយសារជម្លោះភូមិសាស្ត្រនយោបាយនៃធនធានរ៉ែកម្រ គម្លាតទីផ្សារសកលអាចកើតមានឡើងនៅពេលណាមួយនាពេលអនាគត ដែលអាចផ្តល់នូវបុព្វសិទ្ធសម្រាប់បណ្តាប្រទេសនានាក្រៅពីចិនដែលមានធនធានរ៉ែកម្រដូចជា ប្រទេសមីយ៉ាន់ម៉ាជាដើម ដើម្បីបំពេញចន្លោះប្រហោងនេះ។
- នៅក្នុងឆ្នាំ២០០៨ មីយ៉ាន់ម៉ាបានក្លាយជាប្រទេសនាំចេញសុទ្ធលើធនធានរ៉ែកម្ររបស់ចិន ដែលត្រូវបានគេចាត់ទុកជាប្រទេសមួយក្នុងចំណោមប្រទេសទាំងបួនដែលទាញយកធនធានរ៉ែកម្រច្រើនជាងគេនៅលើពិភពលោក។ ទោះបីជាយ៉ាងណាក៏ដោយ មីយ៉ាន់ម៉ាមិនអាចទទួលបានអត្ថប្រយោជន៍ពីការជីកនិងការជួញដូរធនធានរ៉ែកម្រឲ្យបានសមប្រកបតាមដែលខ្លួនគួរទទួលបាននោះទេ ដោយសារតែវិវាទផ្ទៃក្នុងនិងកង្វះច្បាប់ក៏ដូចជាគោលនយោបាយដ៏មានប្រសិទ្ធភាពក្នុងការរុករកនិងធ្វើពាណិជ្ជកម្មធនធានរ៉ែទាំងនេះ។
- ដូច្នេះ អត្ថបទនេះសិក្សាអំពីភូមិសាស្ត្រនយោបាយសកលនៃធនធានរ៉ែកម្រដែលក្នុងនោះរួមមានគម្លាតទីផ្សារ សិក្សាអំពីធនធានរ៉ែកម្ររបស់មីយ៉ាន់ម៉ានៅក្នុងភូមិសាស្ត្រនយោបាយសកល និងរកឲ្យឃើញនូវជម្រើសគោលនយោបាយសម្រាប់ប្រទេសនេះក្នុងការដោះស្រាយផលិតកម្មធនធានរ៉ែកម្រនាថ្ងៃអនាគត។

Introduction

In the era of advanced technology and growing energy transition, the global nations have accepted the usefulness of rare earth elements (REEs) which are very significant to the global innovation of high-tech products ranging from the civil use of smart phones, hybrid cars, and wind turbines to advanced military technology such as guided missile, surveillance equipment and so on. The REEs are a group of seventeen elements that consist of lanthanum, cerium, praseodymium, neodymium, promethium, samarium, europium, europium, gadolinium, terbium, dysprosium, holmium, erbium, thulium, ytterbium, lutetium, and scandium that appear in low concentrations in the ground[a]. There are two types of REEs; heavy rare earth elements (HREEs) and light rare earth elements (LREEs).

However, refining and purifying the REEs ores and concentrates is a technology-intensive process that requires heavy costs of production to meet international standards of environmental protection. Due to the immense consequences generally resulting from the refining process of REEs that severely affects the environment and ecosystem, most REE-consuming countries are quite reluctant to operate REE refineries in their own territory[b]. Such backdrop has exposed China to have become the world's top REE-processor and exporter, and to use its REE supply power as a strategic weapon while pursuing its national interest around the global geopolitics.

The recent trade tensions with the United States in 2019 and the diplomatic tension between China and Japan in 2010 are the best examples to prove that there is a potentiality that China may use the REE card against its rivalries whenever necessary for its strategic interest. In 2014, the World Trade Organization (WTO) ruled out restrictions on Chinese REE activities and forced the latter to remove all quotas and price adjustments, following the official complaint submitted by the United States, Japan and the EU[c]. Subsequently, the high consuming countries have enforced themselves in the pursuit for cooperation with non-Chinese countries to track an alternative REE supplier and to keep a distance from the sphere of the China-dominated global REE market.

There have been precedents that whenever China makes adjustment with its REE import and export quotas in the global supply chain, the market gap for REEs has appeared to be filled by non-Chinese countries which are extracting REEs. Myanmar as one of those countries that export REEs ores the most is also expected to grasp such privilege, and therefore, Myanmar has become a net exporter for China that contributes to the global market.

Overview on the Global Geopolitics of Rare Earth Elements

The occurrences of REEs are generally found in many countries around the world, but the unique issue of REEs is how to process and purify such REE materials that require significant processing methods and extreme cost in production. With that reason, as mentioned above, the high consuming countries of REEs such as the United States, Japan, the European countries and some others have been hesitating for years to possess their own REE processing plants, advocating China to become the world's top REE-exporting country ever since 1962. Currently, China is holding 90 per cent of the REE market portion, in which the United States is the top consumer with 78 per cent of Chinese REEs metals.[d] That has kept the United States in a vulnerable position of heavily relying on China for the former's increasing demand of the latter's REEs. After having several launches of tariffs on Chinese imports conducted by the United States, a high-profile inspection tour of President Xi Jinping to a factory of REEs in Jiangxi Province was considered as a kind of political show-of-force to use REE leverage against the United States amid the trade tension[e]. That has forced the United States to offer a viable alternative source of REEs to reduce its great dependencies on Chinese REEs in the future.

In November 2019, the United States and Australia signed the deal to formalise an ongoing partnership between the two countries to develop new sources of REEs, so as to decrease future reliance on Chinese REEs[f]. Similarly, Japan, Australia, India and the EU also have come up with strong aspirations to balance China's domination of REEs in the global market, compelling them to work with non-Chinese countries[g]. Lynas Corporation, an Australian REE giant, declared in 2018 to expand its processing capacity, and plans to double their output of REEs in order to balance China's domination in the global REEs market. Such attempts have provided a unique space for countries which are enriched with REEs including Myanmar, to jump into the global market gap[h].

Coupled with the aggressive demand of REEs in the global innovation of high-tech products and energy transition, the dominant of Chinese REEs will continue to be very critical to global REEs market. Against this backdrop, the potential conflicts of REEs between China and high-consuming countries which are also powers, might take place in the future for various reasons.

Three causes are considered for the occurrence of potential conflicts of REEs in the future. First, increasing demand of the REEs by technologically-advanced nations. Second, continued dominant position of China in global REE supply chain that can, at any time, shake the global REE market. Third, the increase in geopolitical competition between China and powerful countries such as the United States and Japan.

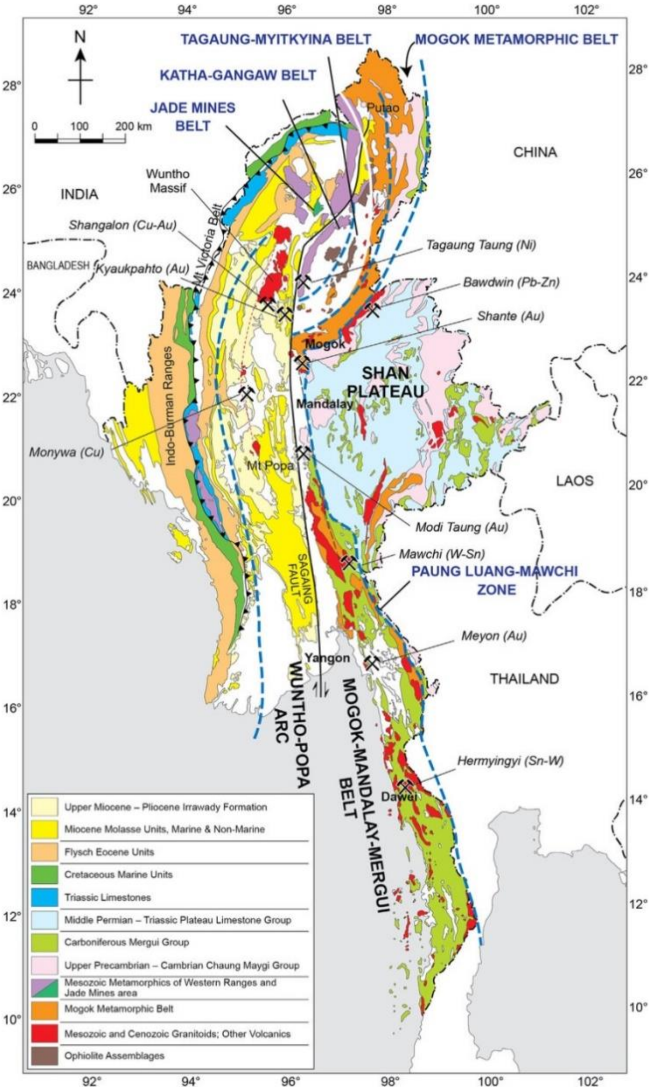
Rare Earth Elements in Myanmar

Myanmar is a well-known resource-rich nation which is famous for its precious stones such as ruby, sapphire, jade and emerald, and its minerals such as copper, gold, silver, zinc, lead and tungsten and tin, and its natural gas such as oil and gas[i]. This is in addition to Myanmar being abundant in heavy rare earth elements (HREEs). Peculiarly, Myanmar expanded the exploration and extraction of REEs in 1963, and reopened in 2013. Most REE deposits occur in northern and north-eastern parts of Myanmar, most of which are dominated by the ethnic armed organisations (EAOs) and share a border with China. Myanmar REEs are very similar in features with the REE clays explored in the southern province of China, and most are composed of three elements such as dysprosium, terbium and gadolinium which are key HREEs. Such HREEs are very useful and essential in global innovations of advanced technology, especially those in producing permanent magnets in the most high-tech products such as smart phone, hybrid vehicles, wind turbines and so on.

Considered as a home to natural resources, Myanmar has developed a series of mining laws which should be abided by the government-owned enterprises (GOE), mining companies, firms and operators. Myanmar is also keen on rectifying and amending those mining laws to be consistent with the current developments, mining systems and environmental protection. Currently, there are fourteen laws which are governing all sorts of mineral mining activities in Myanmar that include: four documents related to mining; two on state-owned economic investments, another two for gemstone exploration, two for pearl exploration, and four for environmental conservation[j]. Those rules, regulations and laws are intended to govern and regulate mining-related activities, ranging from application and registration to exploration, extraction and environmental conservation. Practically, those laws are deemed to miss certain aspects of the governance of REE mining, due to its distinctive features that need complex technical processing methods and heavy costs of environmental protection.

Compared to other mineral mining, the exploration and extraction of Myanmar REEs have not been very popular and are unknown, as it should have been since the reintroduction of REEs production in 2013. Little knowledge of the REE production is earned for the people in Myanmar. The dominance of China in the global market and the accumulation of illegal activities of Myanmar REEs in border areas, has resulted in Myanmar's heavy reliance on China.

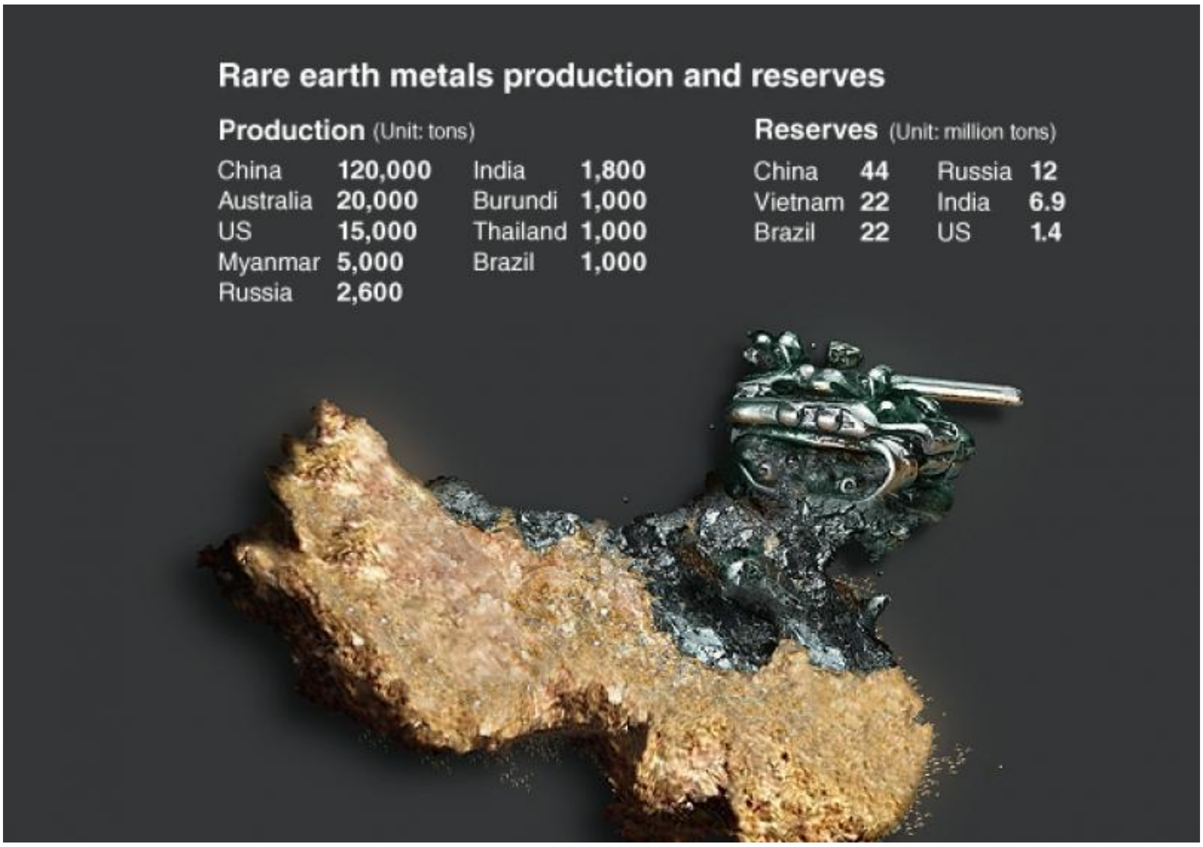
Source: The Myanmar Geosciences Geographical Map of Myanmar (MGS, 2012)



Myanmar Rare Earth Elements in Global Geopolitics

According to the United States Geological Survey (USGS), Myanmar ranked fourth in REE-extracting countries with 5,000 tons of REEs after Australia and the United States in 2018[k]. Following China's adjustment of Japanese import quotas in the wake of diplomatic tension, Japanese Parliamentary Vice Foreign Minister Makiko Kikuta launched a cordial visit to Myanmar in 2011. During her visit, Japan eyed possible cooperation for REE production in the future[l]. As a globally-responsible country and with its own growing demand, China may need to adjust its REE export quotas for global nations and keep REE reserves for its high domestic demand in the coming years.

Along this line, it is assumed that there would be potential conflicts of REEs in the global arena if Chinese REE export quotas do not meet the demand of the global nations. On the other hand, China as the dominant country in the global REE market would also continue to maintain its position that would lessen its REE reserves and therefore need to import from other countries, especially resource-enriched countries like Myanmar. Therefore, Myanmar has become China's net exporter accounting for one third of domestic consumption of REEs that has given Myanmar a market space in the global REEs market[m]. Thus, it can be said that by exporting REE materials to China, Myanmar is sharing a role of responsibility in the global REE market. But the effect of its political condition and lack of government policies on exploring, extracting and exporting REEs, Myanmar is still limited for direct access to the global market, and expected to continue its reliance on China for REE exports.



Rare earth metals production and reserves

Production (Unit: tons)

China	120,000	India	1,800
Australia	20,000	Burundi	1,000
US	15,000	Thailand	1,000
Myanmar	5,000	Brazil	1,000
Russia	2,600		

Reserves (Unit: million tons)

China	44	Russia	12
Vietnam	22	India	6.9
Brazil	22	US	1.4

Source: THE KOREA HEARLD published on 2nd June 2019

Dilemma in the Production of the Myanmar Rare Earth Elements

However, the occurrences of REEs are unpopular and less beneficial for Myanmar due to some particular reasons. First, most of Myanmar mining areas are generally located in ethnic inhabitant areas where the prevailed rules and regulations are merely regarded and practised by the local people upon un-arrival of the government's bureaucratic power at the expense of EAO's domination. That has led to an increase in illegal activities of REE production, in which most involved parties are Chinese who come to hunt Myanmar REEs. Last December, there was a report released by the Mining Department of Kachin State (MDKS), mentioning that the mining officials had spotted Chinese citizen and workers and illegal mining plots with thirty vehicles carrying the REEs in Panwar region in Kachin State[n]. The reckless REEs operators, both Chinese and locals do not fully practise the international standards of environmental protection in REE mining, causing serious environmental erosion. Once China implemented stringent environmental controls in southern Chinese in 2016, approximately 15,000-16,000 Chinese people migrated from Ganzhou, Jiangxi province, to Myanmar to exploit REE resources and supply materials back to the Chinese market[o]. Thus, it can be assumed that the illegal and unregulated exploration, extraction and trading of Myanmar REEs arose due to the absence of rules and regulations emerging from the un-reach of the government's bureaucratic power.

Second, Myanmar is supposed to suffer from the environmental damages amid the REE-related illegal activities which would impact the integrity of the existing legal instruments of Myanmar, related to mining and environmental conservation sectors. It is presumed that Myanmar mining laws are not fully regarded for REE mining and related activities including environmental protection, and therefore Myanmar may need to check with the existing laws, rules and regulations if they are consistent with the present situation. However, the weaker the laws, the more the REE operators will engage in illegal activities, resulting in poor national interest and greater environmental erosion.

Third, it is observed that there is a need for policy coordination between Myanmar and China to address the turbulence in the flow of exports and imports of REEs between the countries that has caused global market uncertainty. China is a net consumer which imports REEs from Myanmar. Since China started combating illegal REE mining in 2018, REE production decreased by 50 per cent, and the consequent market gap was filled by other countries, in which Myanmar has become an important source of HREEs for Chinese magnet and alloy industries[p]. Due to lack of cooperation and coordination at the governmental level, illegal REE activities have become a dilemma for Myanmar to handle that has finally engaged in the issue of environmental erosion.

Looking at other events occurring in 2019, it is clearly seen that the two countries would need a culture of coordination for REE deals at various layers, especially at the governmental level. When China banned the import of Myanmar REE ores in the earlier days, the market presented a shift in price of REEs[q]. Later on, in 2019, Myanmar also blocked REE mining and exporting to China due to unregulated operators and not befitting from the REEs that also caused market uncertainty in the region, through which the global market has become vulnerable[r]. Consequently, that might have forced Myanmar to consider new partners such as the United States, Australia and Japan for REE cooperation in the future.

Conclusion

Observing all those points mentioned above, the strategic importance of REEs will be very crucial in global geopolitics. The growing demand of REEs by the global nations would reinforce China's legitimate domination in the global REE market and that provides China with strategic power in projecting its position in global geopolitics. There might be a possibility for China to use its REE supply power as a strategic weapon in the course of strategic competition with the United States. Thus, the continued domination of Chinese REEs would introduce potential conflicts of REEs with other nations such as the United States, Japan, India, Australia and the EU, forcing them to set up an alternative market for REEs. That has already exposed powerful countries to find cooperation with non-Chinese countries, especially those that are highly producing REE ores and concentrates.

At the expense of geopolitical conflicts of REEs, Myanmar would be privileged to expand its market and accordingly contribute to the global REE market. However, to effectively and efficiently explore, extract and mine the REEs and to contribute to the global REE market, the government of Myanmar should consider the following policy options. First, since most REE mining is located in the ethnic-controlled areas, the government should establish a close contact and proper coordination with the locals in enforcing prevailed rule, regulations and laws. Second, since the REEs are embedded with the peculiar features that relatively affect the environment, the government should review the existing legal instruments and if necessary should consider amendments or separate laws for REE mining. Third, the government should also consider setting up a mechanism that includes actors from different backgrounds such as the representatives from related departments, EAOs, local communities and environmentalists to ensure that the operators are abiding by the laws, rules and regulation, as well as to protect REE mining activities. Fourth, the government should consider to practise active policy in engaging with other countries for REE cooperation, especially with China to protect national interest, the environment and contribution to the global market.

Having gone through the whole picture, there is potentiality for geopolitical conflicts of REEs among the global nations, especially those which will remain or become superpowers in the future. The high pursuit for REE cooperation among those countries such as the United States, Japan, Australia, India and the EU will constitute market gaps that will confer a great opportunity to non-Chinese countries including Myanmar. However, Myanmar is likely to continue to suffer from REE mining and related activities, if proper action is not taken. In the absence of policy review for REE mining, Myanmar may face potential impacts in the future, to some extent, in economic, social, and political sectors.

The opinions expressed are the author's own and do not reflect the views of the Asian Vision Institute.

[a] "Global Cooperation needed on Rare Earths", Julie Klinger, Boston University, 26th September 2019.

[b] "Geopolitics of Rare Earth Elements", 8th April 2019, Stratfor.

[c] "Will China weaponise rare earths in tech-war", The ASEAN Post, 26th May 2019.

[d] "US Dependence on China Rare Earth: Trade War Vulnerability", Reuters, 28th June 2019.

[e] "Would China really embargo exports of rare earth metals from US manufacturers?", Paul Ausick, 24th May 2019.

[f] "Australia and the US: a rare, rare earth partnership", Heidi Vella, January 2020.

[g] "Global Cooperation needed on Rare Earths", Julie Klinger, Boston University, 26th September 2019.

[h] "Threaten rare earth export restriction, Australia, Estonia and Myanmar it, Minda Zetlin", 30th May 2019.

[i] "Mining in Myanmar", Khin Cho Kyi, July 2019.

[j] "Mine Financing and Myanmar Mines Law", Than Htun, 19th September 2019.

[k] "Top Ten Countries for Rare Earth Metal Production", Charlotte, Mcleod, 23rd May 2019.

[l] "Japan Eyes Rare Earth Deal with Myanmar", the Japan times News, 26th March 2011.

[m] "China rare-earth imports from Myanmar will decline", Global Time, 13th April 2019.

[n] "Rare earth illegally dug in Panwar: Kachin", Mining Department, 11th December 2019.

[o] “Rare Earth: China closes Tengchong Yunnan/Myanmar port and bans imports of rare earth from Myanmar”, Industry News, 24th May 2019.

[p] “Rare Earths Market Regional Data Analysis by Production”, Revenue, Prize and Gross Margin, 26th August 2019.

[q] “Rare earth prices fall to 7-month low as China supply fears ease”, NIKKEI ASIAN REVIEW, 30th November 2019.

[r] “Myanmar banned Rare Earths Exports to China”, SMM News, December 2019.

AVI PERSPECTIVE

ISSUE 2021, No. 05

Cambodia | 27th April 2021

US-China Tech War: Would Huawei Survive?

PONG Pich[a]

BONG Chansambath[b]*, MA in Security Studies*

Executive Summary

- As political and economic tensions have continued to rise between Beijing and Washington, the technological sphere has become part of the strategic competition these two great powers use to counter each other's global influence.
- Based on the allegation that Huawei is a tool used by the Chinese government to spy on foreign citizens, in May 2019, the Trump administration issued executive orders prohibiting all executive agencies of the US Federal Government from using Huawei-made components and restricting US tech companies from supplying critical tech components to the Chinese firm. Furthermore, the United States has banned all Huawei-made products from being sold on the US market.
- The decisions made by the Trump administration have had imminent political implications for US-China bilateral relations and, more importantly, for Huawei's business future. This article examines the origin of the tech war between the United States and China to understand how Huawei has gotten into the situation it is now, what the company has done to address the issue and what that means for its business future.

[a] **PONG Pich** is an intern at the Centre for Inclusive Digital Economy (CIDE) of the Asian Vision Institute (AVI) and a junior student majoring in International Relations at the Royal University of Law and Economics (RULE).

[b] **BONG Chansambath** is Deputy Director of CIDE, AVI.

សេចក្តីសង្ខេបអត្ថបទ

- នៅពេលភាពតានតឹងផ្នែកនយោបាយ និងសេដ្ឋកិច្ចរវាងទីក្រុងប៉េកាំង និងទីក្រុងវ៉ាស៊ីនតោនបានបន្តកើនឡើង វិស័យបច្ចេកវិទ្យាបានក្លាយជាយុទ្ធសាស្ត្រមួយដែលមហាអំណាចទាំងពីរបានប្រើ ដើម្បីប្រកួតប្រជែងឥទ្ធិពលគ្នានៅក្នុងសកលលោក។
- ដោយបានចោទប្រកាន់ថា ក្រុមហ៊ុន Huawei គឺជាឧបករណ៍ស៊ើបការណ៍សម្ងាត់របស់រដ្ឋាភិបាលចិនទៅលើពលរដ្ឋបរទេស នៅខែឧសភា ឆ្នាំ២០១៩ រដ្ឋបាលរបស់លោក Trump បានចេញបទបញ្ជាហាមឃាត់រាល់ទីភ្នាក់ងារប្រតិបត្តិការរបស់រដ្ឋាភិបាលសហព័ន្ធអាមេរិកមិនអោយប្រើប្រាស់គ្រឿងបន្លាស់របស់ក្រុមហ៊ុន Huawei និងរឹតត្បិតក្រុមហ៊ុនបច្ចេកវិទ្យាអាមេរិកមិនឱ្យផ្គត់ផ្គង់សមាសធាតុបច្ចេកវិទ្យាសំខាន់ៗដល់ក្រុមហ៊ុនចិននេះ។ លើសពីនេះទៀត សហរដ្ឋអាមេរិកក៏បានហាមឃាត់រាល់ផលិតផលដែលផលិតដោយក្រុមហ៊ុន Huawei មិនឱ្យលក់នៅលើទីផ្សារអាមេរិកផងដែរ។
- ការសម្រេចចិត្តដែលធ្វើឡើងដោយរដ្ឋបាលរបស់លោក Trump នេះ បានធ្វើឱ្យមានផលប៉ះពាល់ផ្នែកនយោបាយនៃទំនាក់ទំនងទ្វេភាគីរវាងសហរដ្ឋអាមេរិក និងចិន ជាពិសេស ដល់អនាគតអាជីវកម្មរបស់ក្រុមហ៊ុន Huawei តែម្តង។ អត្ថបទនេះ ពិនិត្យមើលអំពីដំណើរដើមទងនៃសង្គ្រាមបច្ចេកវិទ្យារវាងសហរដ្ឋអាមេរិក និងចិន ដើម្បីស្វែងយល់ពីស្ថានភាពបច្ចុប្បន្នរបស់ ក្រុមហ៊ុន Huawei ហើយតើក្រុមហ៊ុនបានធ្វើអ្វីដើម្បីដោះស្រាយបញ្ហា និងតើវាមានន័យយ៉ាងដូចម្តេចចំពោះអនាគតអាជីវកម្មរបស់ក្រុមហ៊ុនមួយនេះ។

Introduction

From 2017 to 2020, the relationship between the United States and the People's Republic of China (PRC) deteriorated significantly. President Donald J. Trump began raising tariffs and other trade barriers to export Chinese-made products to the United States in March 2018 (Council on Foreign Relations n.d.). This decision was justified due to the growing bilateral trade deficit, alleged intellectual property theft and forced transfer of US-made technologies by Chinese firms and the PRC.

This tension has made Huawei the principal target of the Trump administration, which began scrutinising the use and transportation of Chinese-made technologies. Besides, it imposed sanctions prohibiting Huawei from getting access to the US consumer market and critical tech components such as smartphone chips and operating system. The United States has also led an international rally warning other countries about the risks posed by Huawei-made 5G infrastructures. For this reason, the Chinese tech giant has faced perhaps its toughest challenge that would determine its business future.

This article is divided into five parts. The first part examines the nature of the current tech war between the United States and China and its global technological strategy under the umbrella of its Belt and Road Initiative (BRI), whereas the second part explains Washington's campaign against the Chinese tech giant Huawei. The third and fourth sections look at how the tech war has affected Huawei and what it means for its business future. It ends with a conclusion.

A China-Led Global Digital Order?

The US-China technological war is a competition over the development of advanced technological research and innovations, which involve investment control, export control and constraint on the transfer of high-tech products. While the Trump administration used US science and technological prowess to gain the upper hand in its global strategic competition with China, Beijing has responded with a multi-pronged approach that incorporates technological elements of its domestic and foreign policies.

Technological development is a critical factor in the current strategic competition between Washington and Beijing, as the latter has used the Digital Silk Road (DSR) to foster China-backed digital integration outside of its region, increase its geopolitical influence and expand its control over contemporary technology that would help the country become a technological superpower. In 2015, the Chinese government declared that the DSR was part of its foreign and domestic policies, consisting of bolstering the Internet base, expanding space cooperation, creating common "technology standards" and promoting policing systems among the BRI countries (Hao 2019). Since its launch, the DSR has generated new waves of opportunities to develop commercial technologies in Asia. In 2016, the Chinese Academy of Sciences created two local research centres in Hainan and Xinjiang as "part of a Digital Earth Under the Information Silk Road initiative to gather space-based remote sensing data for multiple projects under the BRI, particularly in South and Southeast Asia" (Ibid).

The DSR project consists of four core components. First, China contributes to "digital infrastructure" overseas along with the next-generation cellular networks, fibre optic cables and data centres (Council on Foreign Relations 2019). Second, the initiative contains a residential centre to foster innovations that will serve basic global financial and military control, satellite-navigation frameworks, manufactured insights and quantum computing. Third, since China recognises the significance of financial interdependency in its international strategy, the DSR advances e-commerce through computerised free exchange zones, which increment universal e-commerce by diminishing cross-border exchange boundaries and building up territorial "logistics centres" (Ibid). Fourth, the PRC is working to create an international digital ecosystem through digital diplomacy and a multilateral governance framework of which it is the leader.

Since technology is an area where the PRC can effectively compete with the United States, the DSR has become a top priority for the Chinese government to incorporate telecommunication and technological development facilities across Asia, the Middle East, Europe, Africa and Latin America. To achieve its goal of connecting advanced digital infrastructures with the BRI countries, the DSR uses three technological components of the PRC's foreign policy such as Chinese telecoms gear creators, "Data Centre and Storage Infrastructure along the economic corridors" and export of Chinese-made smart city sensors and information platforms (Wheeler 2020).

Since its launch in 2015, the DSR has gained global tractions. China has signed DSR partnership agreements with at least one-third of the 138 countries participating in the BRI project (Kurlantzick 2020). The partnerships include a wide range of cooperation, in which China would assist partner countries in improving their digital infrastructures, smart cities initiative, surveillance technology, AI, e-commerce, and mobile payment.

To counter the PRC's growing technological influence, the United States has convinced its allies about the harmfulness of Chinese-made technologies and lobbied them to prohibit Chinese tech companies from involving in critical digital infrastructures. These efforts, however, have generated mixed results. While Australia, New Zealand and Japan have banned Chinese tech companies from their 5G networks, the United Kingdom and Germany have been less willing to follow suit.

While the United States continues to rally its allies and partners to reject Chinese technologies, one of the tech companies caught in the crossfire between Beijing and Washington is the Shenzhen-based tech giant Huawei, one of the largest telecommunications companies globally. Aside from the national security concerns, there are three additional reasons why the Trump administration targeted Huawei. First, China has been alleged of not allowing full access of its domestic market to US and European telecom companies, whereas Huawei has enjoyed complete access to the said markets. Second, Huawei has allegedly involved in unfair trade practices such as cheating in a phone benchmark test in 2017 and lying to the US about its ties to the Chinese government (Keane 2021; Reichert 2019). Third, since Huawei symbolises China's rapid technological advancement and a global brand representing the country, targeting this firm is the US's priority.

Washington's Campaign Against Huawei

Huawei is a private Chinese technology company founded in 1987 in the southern province of Shenzhen. According to TrendForce (2021), Huawei was the 3rd largest smartphone vendor in 2020, with 170 million of its devices shipped worldwide, although the number is projected to decrease significantly in 2021. In 2019, it was the largest telecom equipment supplier with approximately US$100 billion annual revenue (Zen and Li 2019). Its business portfolio includes telecommunication networks, consumer electronics, operational and consulting services, and electronic equipment to enterprises inside and outside China. Huawei's founder and current CEO, Ren Zhengfei, was previously an officer in the Chinese People's Liberation Army (PLA). The latter started the business from a small company and transformed it into a global tech giant. Currently, Huawei employs more than 194,000 people and has branches in more than 170 countries and regions, serving more than three billion customers worldwide (Huawei n.d.). "Huawei's vision and mission are to bring digital" to every individual, house and institution for a completely connected, intelligent world (Ibid).

Due to its sheer size and the concern that the company uses its technologies to spy on foreign citizens on behalf of the Chinese government, Huawei has become a security concern for several countries, namely the United States, pointing to Ren Zhengfei's previous connection with the PLA. As tension between the US and the PRC has continued to simmer, and as the COVID-19 pandemic has brought the global economy to a partial halt, Huawei faces difficult situation that could have decisive impacts on its future business operations. To understand how Huawei has gotten into the situation it is now, we need to go back to the beginning of the US campaign against Chinese technologies in late 2018.

On 1st December 2018, the United States requested Canada to arrest and deport Huawei's Chief Financial Officer (CFO), Meng Wenzhou, the daughter of Ren Zhengfei. She was accused by the US Department of Justice of violating trade sanctions placed on Iran and committing fraud. Then on 6th March 2019, during a court procedure against Meng, the US Federal Government moved to ban Huawei's equipment from being used in all executive agencies. In addition to legal procedure against Meng, the Trump administration launched an "aggressive campaign warning other countries" not to allow Huawei equipment into their 5G networks, claiming that the Chinese government could use the company to spy on their citizens and government bureaucracies (Council on Foreign Relations n.d.). Moreover, in May 2019, President Trump signed an executive order to add Huawei to a list of companies permanently restricted from doing business with US enterprises. By doing so, the Trump administration galvanised local and global attention around its technological race against China. Google is among the US companies forced to cut off business ties with Huawei.

The Trump administration's measures, such as the prohibition of the transfer of US techs to China and the idea that American companies should not host Huawei-created applications on their operating system, were unclear, unpredictable and even damaging to some of the strengths of the US innovation system (Segal 2020; Wadhams 2020). In response to the US accusations, Huawei claimed that it was not a Chinese government tool and that it was a private company that sold telecommunication equipment and mobile handsets. Although the accusation about Huawei's connection to the PRC remains largely unsubstantiated, Huawei finds it difficult to completely brush off the allegations because, according to Article 7 of the Chinese National Intelligence Law, "Any organisation or citizen shall support, assist, and cooperate with state intelligence work following the law, and maintain the secrecy of all knowledge of state intelligence work" (Chinese National People's Congress 2017). Basically, the law provides the

Chinese government with the legal authority to order domestic firms to hand over their customers' private information to the state for national security reasons. Some critics claim that this law enables the Chinese intelligence to access every customer's private information stored on Huawei products (The Economist 2019). Nonetheless, Huawei has continued to deny the allegation, claiming that "it has never spied on behalf of any country and would refuse any request to spy for Beijing" (Pancevski 2020).

The US ban on Huawei has had major implications on its domestic and overseas operation because smartphone production relies on a global supply chain of critical components that stretches across many nations. For instance, the iPhone production line requires hardware from more than a dozen international suppliers (Costello 2021). The audio camera is made by Japan-based Sony, whereas the accelerator is made by Bosch Sensortech, a German company with various locations worldwide. Likewise, the Wi-Fi chip is exported from different parts of East and Southeast Asia, while the Touch ID is made by TSMC in Taiwan. Since companies need to import components from foreign sources, the US ban has severely impacted Huawei's operation, which depends on US-based firms such as Google. Although Huawei can continue to produce smart devices by depending on its existing stockpile of essential tech components, the stockpile will run out at some point, which is when the real problem will begin. Once it runs out, any companies planning to ship new components to Huawei will need to obtain an export license from the US Federal Government, which has grown increasingly hostile toward Huawei and China.

While the concern about the Chinese government using Huawei to spy on American citizens is not without merit, the risk can be minimised by limiting the use of Huawei-made equipment to smaller parts of the US' domestic 5G infrastructures. According to James A. Lewis, Senior Vice President at the Washington-based Center for Strategic and International Studies (CSIS), it is a major concern for the United States that a strategic competitor like China is holding significant control over the development and deployment of 5G network globally. That said, it is even more troubling if China uses Huawei as a tool to spy on foreign citizens.

Who Has Stopped Doing Business with Huawei?

Following President Trump's executive order banning Huawei, the Chinese company has been designated as a national security risk by the US Department of Commerce and included in the "entity list" (Hamilton 2019). This means that any US companies wanting to supply manufacturing components or doing business with Huawei need to get permission from the US Federal Government. For instance, Qualcomm Inc. is one of the major companies that sell chips to Huawei. After Trump's executive order was signed, Qualcomm needs to obtain a US Federal Government license before any of its shipments of tech components can be processed. Qualcomm has made the case to US policymakers that the export ban will not stop Huawei from obtaining necessary components and that it will hand over billions of dollars of market share to overseas competitors such as Taiwan-based MediaTek Inc. and South Korea-based Samsung Electronics Co. (Fitch and O'Keeffe 2020).

This indicates that the US global campaign against Huawei not only leads to growing tension with Beijing but also generates drawbacks for domestic tech businesses such as Qualcomm that sees its global market share shrinking. Like Qualcomm, Google has been ordered to stop licensing its Android mobile operating system (OS) to Huawei, making some apps on Huawei smartphones such as Play Store and Gmail apps unavailable. The US ban thus cuts off Huawei from core parts of Android OS such as Google Play and Gmail.

Shortly after the Trump administration announced its ban on Huawei, major American chipmakers such as Intel and Qualcomm have lobbied the US Federal Government to ease sanctions on Huawei, arguing that its smartphones do not present the same national security concerns as grave as its 5G infrastructures. They also argue that they should be allowed to continue to supply components to Huawei's smartphone and smartwatch production (Nellis and Alper 2019). It is worth noticing that US$11 billion out of US$70 billion Huawei spent on buying chips in 2018 went to US companies like Intel and Qualcomm. The Trump administration's sanctions would allow these companies' competitors to take advantage of the situation and slice their share of the global chip supply market.

Could Huawei Survive without Supplies from US Companies?

Despite the tremendous pressure imposed by the Trump administration, Huawei has searched for ways to handle this situation. Since 15th September 2020, no US companies have been permitted to ship their components to Huawei. Meanwhile, without a US Department of Commerce license, other major chip suppliers such as Taiwan-based Semiconductor Manufacturing Co (TSMC) and South Korea-based memory chipmakers, Samsung and SK Hynix, have halted their shipments to Huawei. Other critical smartphone components such as semiconductors, camera lenses and printed circuit boards produced by US companies are also included in the ban. Even though Huawei cannot order chips and US companies' components, it still can make products using existing stockpile, according to Edgar Pere, an independent consultant and an American-Peruvian business author. According to CGTN, "Huawei has been stockpiling all kinds of chips since the end of 2018. In the past three months, the company's last-minute chip orders pushed Taiwan's overall electronic component export growth to the mainland by 30 per cent year-on-year" (Zheng and Zhu 2020).

Even before the ban was proposed and implemented, Huawei appeared to prepare for an eventual crisis. According to Gai Keke, Associate Professor at the School of Computer Science and Technology of the Beijing Institute of Technology, another consequence of the US ban is pushing China to create its semiconductor industry. He said that Huawei smartphones would face problems because of the lack of chips in a short time. Still, he is hopeful in Huawei's technological development, as the company has already revised its trade policy and expanded its hardware production of customer electronics such as laptops (Ibid).

The technological landscape in China remains largely normal without Google because about 1.4 billion Chinese people wake up every morning checking WeChat instead of Gmail, using Baidu instead of Google Maps, and watching videos on Youku instead of YouTube. Nevertheless, the problem is that Huawei consumers outside of China cannot use those apps. Since most of Huawei's consumers overseas rely on Google, it will be an issue for them if there are no Google apps available on their devices. According to Regalado (2019), one of the main reasons people consider Huawei smartphone is the quality of its camera. If people need a smartphone with advanced camera technology, they can think of a Huawei smartphone. Now that the United States is banning Huawei, the question of how Huawei can still satisfy its customers remains to be seen.

Although Google has strictly abided by the Trump administration's executive order and suspended all trade with Huawei, the Chinese company can continue to use the open-source version of Android OS. Google also announced on Twitter that previous Huawei smartphones would retain access to Google Play, but future Huawei smartphones cannot access the Google Play Store and download apps such as Gmail, YouTube and updates to its OS. Aside from the impacts on device productions and access to Android, Huawei will significantly lose access to the US consumer electronic market, as carriers such as AT&T and Verizon do not sell the company's gadgets at their outlets.

In response to the US ban, Huawei has been developing its OS called HarmonyOS, but, according to its representatives, the company still favours Android OS. In case no exemptions to the sanctions are granted, Huawei and other Chinese companies may need to move toward creating "an alternative operating system and ecosystem of apps for their phones sold abroad" (Su 2019). Huawei has invented an operating system called HarmonyOS, which is applicable only for TV sets from Huawei and Honor. However, by 2021, HarmonyOS will be installed on new generation smartphones. According to CGTN, "Huawei's ecosystem is working in the Chinese mainland market. But outside China, where more people prefer Google's software, Huawei is having a hard time promoting its smartphones" (Gong 2020).

Conclusion

The technological competition between the United States and China has been spurred by simmering tension between the two major powers. As Washington has galvanised a global campaign against Chinese technologies, Beijing has used the Digital Silk Road as a tool to expand its geopolitics influence, digital integration and technological prowess. Due to its allegedly close ties to the Chinese government, Huawei has become the primary target of the Trump administration's ban prohibiting the trade of tech components between American companies and Huawei based on the accusation that the Chinese company spies on foreign citizens on Beijing's behalf. In addition to the ban, the United States has rallied its allies and other countries worldwide to cut Huawei off their domestic 5G infrastructures.

From a business perspective, the United States' actions have had strong impacts on Huawei's current and future operations, as Huawei-made devices primarily depend on Android OS owned by Google. Moreover, Huawei would lose access to US consumer markets and that its customers outside of China may consider switching to other brands such as Samsung or Apple. Although Huawei has invented HarmonyOS to replace Android OS and that the company can rely on the existing stockpiles of hardware while the US sanctions remain in place, its future remains uncertain, as US-China relations remain increasingly hostile even after Donald Trump got voted out of office in November 2020.

The opinions expressed are the author's own and do not reflect the views of the Asian Vision Institute.

References

Chinese National People's Congress. 2017. "National Intelligence Law of the People's Republic." *Chinese National People's Congress*, Last Modified June 27, 2017. http://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf.

Council on Foreign Relations. 2019. "China's Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism." *Council on Foreign Relations*, Last Modified September 26, 2019. https://www.cfr.org/blog/chinas-digital-silk-road-strategic-technological-competition-and-exporting-political.

Council on Foreign Relations. n.d. "US Relations with China 1949–2020." *Council on Foreign Relations*. https://www.cfr.org/timeline/us-relations-china.

Fitch, Asa, and Kate O'Keeffe. 2020. "Qualcomm Lobbies US to Sell Chips for Huawei 5G Phones." *The Wall Street Journal*, Last Modified August 8, 2020. https://www.wsj.com/articles/qualcomm-lobbies-u-s-to-sell-chips-for-huawei-5g-phones-11596888001.

Gong, Zhe. 2020. "Huawei's HarmonyOS 2.0 coming to smartphones in 2021." *CGTN*, Last Modified September 10, 2020. https://news.cgtn.com/news/2020-09-10/Huawei-s-HarmonyOS-2-0-coming-to-smartphones-in-2021-TFLqH0vMeQ/index.html.

Hamilton, Isobel Asher. 2019. "Here Are All the Big Companies that Have Cut Ties with Huawei, Dealing the Chinese Tech Giant a Crushing Blow." *Business Insider*, Last Modified June 18, 2019. https://www.businessinsider.com/all-the-companies-that-have-cut-ties-with-huawei-2019-5.

Hao, Chan Jia. 2019. "China's Digital Silk Road: A Game Changer for Asian Economies." *The Diplomat*, Last Modified April 30, 2019. https://thediplomat.com/2019/04/chinas-digital-silk-road-a-game-changer-for-asian-economies/.

Huawei. n.d. "Who is Huawei?" *Huawei.* https://www.huawei.com/us/corporate-information.

Keane, Sean. 2021. "Huawei Ban Timeline: Company Tries to Blame US for Sanctions for Global Chip Shortage. *CNET*, Last Modified April 15, 2021. https://www.cnet.com/news/huawei-ban-full-timeline-us-sanctions-global-ship-shortage-china/.

Kurlantzick, Joshua. 2020. "China's Digital Silk Road Initiative: A Boon for Developing Countries or A Danger to Freedom?" *The Diplomat*, Last Modified December 17, 2020. https://thediplomat.com/2020/12/chinas-digital-silk-road-initiative-a-boon-for-developing-countries-or-a-danger-to-freedom/.

Nellis, Stephen, and Alexandra Alper. 2019. "US Chipmakers Quietly Lobby to East Huawei Ban." *Reuters*, Last Modified June 17, 2019. https://www.reuters.com/article/us-huawei-tech-usa-lobbying-idUSKCN1TH0VA.

Pancevski, Bojan. 2020. "US Officials Say Huawei Can Covertly Access Telecom Networks." *The Wall Street Journal*, Last Modified February 12, 2020.

https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256.

Regalado, Francesca, 2019. "Customers ask: Is a Huawei Phone Without Google Worth $1,000?" *NIKKEI Asia*, Last Modified October 9, 2019. https://asia.nikkei.com/Spotlight/Huawei-crackdown/Customers-ask-Is-a-Huawei-phone-without-Google-worth-1-000.

Reichert, Corinne. 2019. "US Reportedly Accuses Huawei of Lying About Chinese Ties." *CNET*, Last Modified May 23, 2019. https://www.cnet.com/news/us-reportedly-accuses-huawei-of-lying-about-chinese-ties/.

Segal, Adam. 2020. "The Coming Tech Cold War with China." *Foreign Affairs*, Last Modified September 9, 2020. https://www.foreignaffairs.com/articles/north-america/2020-09-09/coming-tech-cold-war-china.

Su, Alice. 2019. "Huawei Will Make Do Without Google, But How Well?" *Phys.org*, Last Modified May 21, 2019. https://phys.org/news/2019-05-huawei-google.html.

The Economist. 2019. "Is America Right to Fear Huawei?" YouTube video. 9:57. Posted by "The Economist" November 13, 2019. https://www.youtube.com/watch?v=1ylleTbizgU&list=LL&index=13.

TrendForce. 2021. "Global Smartphone Production Expected to Reach 1.36 Billion Units in 2021 as Huawei Drops Out of Top-Six Ranking, Says TrendForce." *TrendForce*, Last Modified January 5, 2021. https://www.trendforce.com/presscenter/news/20210105-10630.html.

Wadhams, Nick. 2020. "Pompeo Urges Cutting Ties with Chinese Tech Companies, Apps." *Bloomberg*, Last Modified August 6, 2020. https://www.bloomberg.com/news/articles/2020-08-05/pompeo-urges-cutting-ties-with-chinese-tech-companies-apps.

Wheeler, Andre. 2020. "China's Digital Silk Road (DSR): the new frontier in the Digital Arms Race?" *Silk Road Briefing*, Last Modified February 19, 2020. https://www.silkroadbriefing.com/news/2020/02/19/chinas-digital-silk-road-dsr-new-frontier-digital-arms-race/.

Zen, Soo, and Li Tao. 2019. "How Huawei Went from Small-time Trade in Shenzhen to World's Biggest Telecoms Equipment Supplier." *South China Morning Post*, Last Modified February 18, 2019. https://www.scmp.com/tech/big-tech/article/2186494/how-huawei-went-small-time-trader-shenzhen-worlds-biggest-telecoms.

Zheng, Junfeng, and Zhu Feng. 2020. "Can Huawei Survive the US Chip Ban?" *CGTN*, Last Modified September 16, 2020. https://news.cgtn.com/news/2020-09-16/Can-Huawei-survive-the-U-S-chip-ban--TPVMNJdWq4/index.html.

AVI PERSPECTIVE

ISSUE 2019, No. 12

Cambodia | 22nd December 2019

Cyberconflict: How Should Cambodia Prepare?

CHHEM Siriwat[a], Master in Digital Technology Management

Executive Summary

- ❖ This perspective paper explores the past, present, and future of cyberconflict for Cambodia and on the global scale. The components of cyberconflict will be discussed in terms of resources and actors, tools, and frameworks. Key interactions within the cyberspace include logical, physical, and psychological methods, and the exploitation, attack, and defense of computer networks.
- ❖ Challenges that arise in the field of cyberconflict concern governance and ethics. Cyberconflict laws must be forward-looking and preventative, rather than reactive, as technology moves at a much higher speed than policymaking. Ethics in governing the international cyberspace can be extrapolated from traditional pillars such as the "Laws of Armed Conflict" (LOAC) and "Just War Theory", but adjusted within the context of emerging technologies.
- ❖ The following policy options for Cambodia could potentially help in preparing for cyberconflict in the future:
    - o Raise awareness to policymakers on the consequences of cyberconflict and the need for a national cybergovernance strategy.
    - o Integrate computing and security expertise, through education and training.
    - o Partake in regional dialogue to contribute to an ASEAN cyberconflict treaty.

[a] **CHHEM Siriwat** is Director of the Centre for Inclusive Digital Economy (CIDE) at the Asian Vision Institute (AVI).

សេចក្តីសង្ខេបអត្ថបទ

- អត្ថបទ Perspective នេះ បង្ហាញពី អតីតកាល បច្ចុប្បន្នកាល និងអនាគតកាលនៃជម្លោះពាក់ព័ន្ធនឹងអ៊ិនធើណិត នៅក្នុងប្រទេសកម្ពុជា និងនៅក្នុងពិភពលោក។ ជាតុផ្សំនានានៃជម្លោះពាក់ព័ន្ធនឹងអ៊ិនធើណិតនឹងត្រូវលើកមកពិភាក្សាក្នុងបញ្ហាជាប់ទាក់ទងទៅនឹង ធនធានជាមួយនិងតួអង្គ ឧបករណ៍សម្រាប់ទប់ទល់ និងក្របខ័ណ្ឌអនុវត្ត។ អន្តរកម្មសំខាន់ៗនៅក្នុងលំហអ៊ិនធើណិត រួមមាន វិធីផ្សេងៗតាមបែបតក្កវិជ្ជា រូបសាស្ត្រ និងចិត្តវិទ្យា ព្រមទាំង ការកេងប្រវ័ញ្ច ការវាយប្រហារ និងការការពារបណ្តាញកុំព្យូទ័រ។
- បញ្ហាប្រឈមទាំងឡាយដែលផុសចេញពីជម្លោះពាក់ព័ន្ធនឹងអ៊ិនធើណិត វាជាប់ទាក់ទងនឹងអភិបាលកិច្ច និងក្រមសីលធម៌។ ច្បាប់ស្តីពីជម្លោះពាក់ព័ន្ធនឹងអ៊ិនធើណិតត្រូវមានលក្ខណៈជឿនលឿន មើលឃើញវែងឆ្ងាយ និងបង្ការគ្រោះថ្នាក់ ជាជាងព្យាយាមដោះស្រាយបញ្ហានៅពេលបច្ចេកវិទ្យាវារីកលូតលាស់លភនជាងការកសាងគោលនយោបាយ។ ក្រមសីលធម៌ក្នុងការគ្រប់គ្រងលំហអ៊ិនធើណិតអន្តរជាតិ អាចមានខ្លឹមសារបន្តពី សសរស្តម្ភជាប្រពៃណី ដូចជា ច្បាប់ស្តីពីជម្លោះតាមផ្លូវអាវុធ និងទ្រឹស្តីនៃសង្គ្រាមយុត្តិធម៌ ជាដើម ដោយមានការកែសម្រួលទៅតាមបរិបទនៃបច្ចេកវិទ្យាកំពុងផុសឡើង។
- សម្រាប់ប្រទេសកម្ពុជា ជម្រើសគោលនយោបាយដូចខាងក្រោម អាចជួយសម្រួលដល់ការត្រៀមរៀបចំផ្សេងៗ ដើម្បីទប់ទល់លទ្ធភាពមានជម្លោះពាក់ព័ន្ធនឹងអ៊ិនធើណិតនាពេលអនាគត៖

    1. លើកកម្ពស់ការយល់ដឹងដល់អ្នកធ្វើគោលនយោបាយអំពី ផលវិបាកនៃជម្លោះពាក់ព័ន្ធនឹងអ៊ិនធើណិត និងតម្រូវការឲ្យមានយុទ្ធសាស្ត្រអភិបាលកិច្ចអ៊ិនធើណិតថ្នាក់ជាតិមួយ។
    2. ដាក់បន្ស៊ីចូលគ្នានូវកម្រិតជំនាញខ្ពស់ខាងផ្នែកកុំព្យូទ័រ និងសន្តិសុខ តាមរយៈការអប់រំ និងបណ្តុះបណ្តាល។
    3. ចូលរួមក្នុងកិច្ចពិភាក្សាថ្នាក់តំបន់ ដើម្បីជួយរួមវិភាគទានដល់សន្ធិសញ្ញាអាស៊ានស្តីពីជម្លោះពាក់ព័ន្ធនឹងអ៊ិនធើណិត។

Introduction

The nature of international conflict between nations is rapidly evolving; the players, the field of battle, the tools, and the resources we are fighting for. This paper will explore key interactions and actors involved in the cyberspace, including examples of past incidents of cyberconflict around the world. Although policies that govern these types of interactions in the cyberspace are still new and unrefined, we could use methods from traditional conflict to analyse them to a certain extent. We can prepare for the future of cyberconflict by combining our knowledge of previous fundamental theories of conflict, past incidents of cyberconflict, and contemporary domain knowledge of the cyberspace. The following are definitions that will distinguish key terms:

- **Internet** – Set of computer networks.
- **Cyberspace** – World of information through the internet.
- **Cyberattack** – Attempt by hackers to damage or destroy a computer network or system.
- **Cybersecurity** – Protection of internet-connected systems, including hardware, software and data, from cyberattacks.
- **Cyberwarfare** – Use of technology to launch attacks on nations, governments and citizens, causing comparable harm to actual warfare using weaponry.
- **Cyberconflict –** International conflict in cyberspace.
- **Cybergovernance** – Governance of the cyberspace.

The term "cyberwarfare" could be considered a misnomer, as cyberattacks on the global scale have not yet been treated as official acts of war. Throughout this paper, "cyberconflict" will reflect a more neutral stand of an act of cyberwarfare, which has a more offensive connotation.

Cyberconflict

Cyberconflict involves the use of technology to harm another nation or its digital infrastructure. This new age of conflict can be broken down into: (1) Resources and Actors, (2) Tools, and (3) Frameworks.

(1) Resources and Actors

Today’s most valuable resource is data. Previous conflicts were over tangible resources such as currency, land, and oil, but cyberconflict marks the beginning of conflict over intangible resources. This battle takes place in the cyberspace, where traditional boundaries of combat and operations have completely changed. It no longer matters where we are on land, sea, or air, as long as we have access to digital infrastructure – making strategic moves borderless and instantaneous. Actors involved in cyberconflict are of a new profile, not specifically trained, but with general computing and security backgrounds.[a] We are witnessing the emergence of various types of non-state actors.

(2) Tools

The tools used now are not only of physical and psychological nature, but logical as well. Logical tools are related to understanding Computer Network Operations (CNO) and how they can be used to access or manipulate systems, with malicious intent. Physical tools refer to those that would damage Supervisory Control and Data Acquisition (SCADA) systems that are crucial to all industrial processes. Psychological tools concern social engineering, where individuals or organizations are targeted, in attempt to extract confidential information and access their computer networks.[b]

(3) Frameworks

If we look at the bigger picture, Computer Network Exploitation (CNE) acts as a strategic framework that plans the utilization of the aforementioned logical, physical, and psychological tools from start to finish. This form of reconnaissance or espionage first identifies relevant targets that potentially hold key information, in order to plan a future Computer Network Attack (CNA) or Computer Network Defense (CND). A CNA consists of different phases: reconnaissance, scanning, system access, privilege abuse, data extraction, system assault, and trace removal. CND concerns security awareness and training, with regards to protecting data and information. The key principles of the cybersecurity framework are represented by confidentiality, integrity, and availability (CIA), and authentication, authorization, and auditing (AAA).[c] These components are used to evaluate the security of data and information security within a system.

Given this new hybrid of actors, resources, and interactions, how do we interpret cyberattacks compared to physical attacks? Can states respond to "soft" force in the form of cyberattacks, with the use of kinetic military force? How do we distinguish or measure the magnitude of cyberconflict?

Current Challenges

Legal systems vary from nation to nation, in dealing with matters of cyberconflict. The main challenges that arise from addressing issues of cyberconflict are related to: (1) Governance and (2) Ethics.

(1) Governance

The fundamental challenges in cyberconflict are similar to those in traditional security, just in the context of the cyberspace. How can lawmakers strengthen existing legal frameworks to address issues related to this new age of interactions? Cyberconflict laws that are being newly formed should promote "confidentiality, integrity, and availability of public and private information, systems, and networks." Furthermore, these regulations should incentivise the protection of individual rights and privacy, economic interests, and overall national security.[d] These forward-looking laws should prevent future incidents, which is more sustainable than deciding punishments for past incidents. Technology is advancing at a much faster rate, than laws are being made to govern cyberconflict. Therefore, policymakers should focus on preventive measures, rather than reactive.

(2) Ethics

Aside from adopting a forward-looking approach in governing cyberconflict, ethical issues are of paramount importance. Just as with traditional forms of conflict, ethics govern the justifications of actions carried out during conflict. However, controversy arises as different nations sometimes have contrasting ethical standards. For example, China and Russia believe in national cyber sovereignty, as opposed to the free flow of information promoted mainly by the Western world, led by the US. These opposing paradigms underlie the situational ethical differences that contribute to the tension between these nations. Before discussing the ethics of cyberconflict, it would be helpful to explore the ethics of traditional conflict, as a conceptual framework to assess these situations. This comparison could potentially address the ethical gaps between the physical world and the cyberspace. The two main concepts concerning the ethics of traditional conflict are: A) "Laws of Armed Conflict" and B) "Just War Theory".

A) "Laws of Armed Conflict" (LOAC)

Military decisions can be ethically assessed in accordance to the LOAC, consisting of four core principles: (1) distinction, (2) military necessity, (3) humanity, and (4) proportionality.

(1) Distinction traditionally requires soldiers to distinguish between enemy fighters and civilians, and military objects and civilian objects. This pre-determined distinction guides soldiers to target enemy fighters and military objects, and avoid civilians and civilian objects.

(2) Military necessity limits soldiers to use force only when necessary to complete a specific mission, that will benefit their side by weakening their enemy's defense in some measure. However, attacks must align with all four principles of the LOAC. For example, military necessity should not violate the principle of humanity, concerning unnecessary suffering.

(3) Humanity protects combatants against harm that is not necessary to complete a military mission. All people regardless of sides, should be treated humanely and not have to endure any form of torture or preventable death.

(4) Proportionality concerns the balance between military necessity, against distinction and humanity. The main concern is to reduce collateral damage caused by tools on civilians or their property. An attack would be justified in this context, if the collateral damage is not excessive in comparison to the military advantage gained.[e]

Although highly subjective, it is useful to have an assessment criterion in place, so that all aspects of a military decision are first weighed out before executing the plan.

B) Just War Theory

Furthermore, the contemporary "Just War Theory" discusses the views of revisionists and traditionalists. While traditionalists focus more on moral principles such as the LOAC, revisionists prioritise pragmatism. These contrasting views determine whether starting a war is justified, in addition to the conduct in war. Following the war, the moralist of settlement and reconstruction should also be considered. A certain extent of pragmatism could justify a war, if the practical benefits would outweigh the consequences, despite opposing theoretical views.[f]

Given this structured approach to examining traditional military issues, how can we contextualise this framework to appropriately govern cyberconflict? Now that we are dealing with intangible components, the subjective matter of evaluating conflict becomes ever more complex.

Past Incidents of Cyberconflict

To get a better understanding of the nature and potential consequences of cyberconflicts, it would be useful to explore the implications of a cyberattack, by one nation on another. Although the validity of these accusations may sometimes be controversial depending on the origin of the news source, the threat of cyberattacks are real and should not be neglected. A few examples of significant accusations of cyberconflict are provided below to illustrate these threats, involving: (1) China-Philippines (2) Russia-US, and (3) US-Iran.

(1) China-Philippines

Starting in 2012, at the heat of South China Sea conflict, a chain of cyber retaliations between Chinese and Filipino hackers was triggered through induced corruption of academic websites, use of remote access Trojan malware.[g] These series of attacks demonstrate how traditional conflict in terms of geopolitical tension, during the South China Sea dispute, can lead to a series of cyberconflicts.

(2) Russia-US

During the 2016 US presidential elections, a group of Russians allegedly interfered with the process by means of ‘information warfare’, through social media. They used Virtual Private Networks to link their operations back to computers in the US. These cyberattacks occurred in a context of intense rivalries among candidates to the Presidency. These alleged cyber activities are now under investigation, given recent attempts to impeach President Trump.[h] This past incident highlights the powerful nature of social media on the general public, and how key decisions can be influenced at the national level.

(3) US-Iran

In June 2019, the US allegedly carried out a cyberattack on the database of Iran's Islamic Revolutionary Guards Corps. This attack on Iran's intelligence systems caused them to lose data and their capabilities were taken offline. The purpose of this mission was to temporarily hinder Iran's ability to target commercial vessels and oil tankers travelling through the Persian Gulf.[i] In a way, this cyberconflict could be seen as a case of the "security dilemma", translating into the cyberspace. The physical military assets from Iran created fear and tension, instigating the US to carry out a cyberattack on the Iranian database, as a preventive measure against any physical attack.

Policy Options

Cambodia is experiencing peak development and growth in the digital era and should prepare against potential cyberconflict, by learning from past incidents from around the world. Currently, there is no legal framework or clear specialised leadership to govern and protect Cambodia's cyberspace. Due to the lack of a comprehensive platform connecting the appropriate actors and policies, Cambodia is vulnerable to cyberconflict from all angles. Based on the aforementioned incidents of cyberconflict and the current status of Cambodia's strategy, policy options can be formed to address the future of cyberconflict in Cambodia and in ASEAN. Cambodia should:

> (1) Raise awareness to policymakers on the consequences of cyberconflict and the need of a national cybergovernance strategy,
>
> (2) Integrate computing and security expertise through education and training, and
>
> (3) Partake in regional dialogue to contribute to an ASEAN Cyberconflict Treaty.

1) Raise Awareness

Given the insecurity and paranoia that surround cyberconflict, the first step in addressing this issue of national security is raising awareness to policymakers, about its potential consequences. In November, Cambodia hosted a conference, Cyber Security Asia (CSA) 2019 in Phnom Penh. According to Haji Amirudin Abdul Wahab, CEO of CyberSecurity Malaysia, a guest speaker at CSA, "ASEAN is the world's fastest-growing internet region, with the user base forecasted to reach 480 million by 2020."[j] The Cambodian society is becoming exponentially more connected, improving their productivity through faster communication of data and information. However, this rapid technological adoption comes at a price, translating into higher vulnerability to cyberattacks on individual devices. Local events such as CSA 2019 will raise awareness of cybersecurity and its implications on national security.

Furthermore, A.T. Kearney, a global management consulting firm in the US, stated that "In 2017, ASEAN countries collectively spent only 0.06 percent of their GDP, or $1.9 billion on cybersecurity which was in contrast to the global average 0.13 percent." More specifically, CyberSecurity Malaysia is aiming to produce 10,000 security professionals.[k] These regional initiatives highlight the importance of preparing professionally trained security experts.

If Cambodia is unprepared for cyberconflict in the short term, the nation should not be afraid, but instead stay focused and learn from its regional partners. Cambodia has a young and tech-savvy population, which is ideal for keeping up-to-date with technological trends, along with their consequences. Thus, tailored education and training will be essential to provide conceptual knowledge and practical experience to the upcoming generation of Cambodians.

2) Education and Training

Cambodia needs to assemble a team of specialists with both computing and security expertise. As this hybrid role is now in high demand, selected professionals with computing backgrounds must be trained in the context of national security. These individuals would have computing backgrounds, but are able to lead and strategise on a national scale of security. For those few Cambodians with specific expertise in cybersecurity or cryptography, they must be assembled together as key members of the team to advise on the technical aspects of cyberconflict.

From an educational perspective, in order to strengthen the nation against cyberconflict in the long term, the government should incentivise Cambodian students to pursue an academic path in mathematics, computer science, computer engineering, and security studies. These subject matters are foundational components for technical cybersecurity professionals. Currently, the more popular academic specializations in Cambodia are accounting and civil engineering, due to cultural reasons and the past industrial needs of a developing country. Now that Cambodia is striving for digital transformation in the era of Industry 4.0, education and training must be tailored to match the needs of the future. More importantly, these technical experts should be trained how to communicate effectively with policymakers that might be non-technical individuals. Not only is technical expertise important, but so is understanding security issues in the context of the big picture. When addressing a matter of national security, one must understand the motive behind each individual technical process, which plays a crucial role in the grand scheme of an international cyberconflict.

(3) Regional Dialogue

Finally, Cambodia must engage with international partners to voice its national interests concerning cyberconflict. In order for a regional cyberconflict treaty to be established, the national interests of regional members must be exchanged and taken into consideration. Cambodia must send a diverse group of delegates from the government, private sector, academia, and non-governmental organisations to represent the nation, in order to provide different perspectives. Furthermore, these delegates should attend regional dialogues of varying themes, so as to comprehend the entire situation from all narratives.

As with traditional security issues, communication between nations is key. Rather than focusing on potential cyberattacks stemming from paranoia, Cambodia can proactively interact with regional partners to constructively contribute to regional stability. Cambodia's best way to prepare for future cyberconflict is to develop technical expertise on a national scale within a clear national cyberconflict strategy.

For example, on October 14th 2019, the Ministry of External Affairs of the Government of India and the Observer Research Foundation (ORF) hosted the ASEAN-India Track 1.5 Cyber Dialogue in New Delhi. Cambodian delegates were invited to constructively discuss the digital future of ASEAN. Aside from the high potential growth of the digital economy, even more consideration must be paid to the governance of cyberspace in the global context. Nations at the dialogue had the opportunity to share how they utilise emerging technologies to strengthen their own governance methods and how they wish to deal with issues of norms in the cyberspace and international cyberconflict.

However, the main challenge of these regional dialogues is to reach a consensus amongst all nations present. As a most recent example, the US-ASEAN Cyber Dialogue was held in Singapore on October 3rd 2019. The US and Laos co-chaired the event, discussing the themes of 5G, digital economy, and cyber capacity building. Although views were exchanged on their respective national interests and how to promote regional capacity building and cooperation in the cyberspace, more specific technical details were not expressed.[1] All nations wish to know what their regional partners' strategies are, but they will never disclose their own security methods and strategies, in technical details. As a conclusion, there was no consensus due to the relatively general statements provided by each side. However, as all nations take their first cautious steps into the cyberspace, it is crucial to initiate collaborative efforts internationally, in order to address this highly sensitive issue.

Conclusion

The global fear of cyberconflict stems from its intangibleness and uncertainty, as a new form of interaction in an unfamiliar cyberspace. The more our economies and societies become digitally interconnected, the more vulnerable our privacy and data are. These dynamics create a controversial trade-off for all nations: security of privacy and data, for technological convenience and efficiency.

On an international scale, as states increasingly convert their data into digital format, there are more sites prone to potential cyberattack by another state. Thus, it is of paramount importance for Cambodia to strategise and assemble a national team of experts to prepare for cyberconflict in the future, in line with the rapid growth of its digital economy. On a regional level, although Cambodia is relatively behind in terms of technological advancements and qualified human resources, initiatives can be taken to address this gap. The first step is to acknowledge the lack of national preparedness against the grave consequences of potential cyberconflict. Cambodia as a small state, cannot possibly control what lies ahead in the cyberspace, but can make every effort in preparing to respond to future cyberconflict by educating and training experts and the general public, establishing a national strategy for cybergovernance, building cybersecurity infrastructures, and learning from regional partners.

The opinions expressed are the author's own and do not reflect the views of the Asian Vision Institute.

[a] Andress, J. and Winterfeld, S. "Cyber Warfare" *Techniques, Tactics and Tools for Security Practioners*, No.2 (2014).

[b] Ibid.

[c] Ibid.

[d] Kosseff, J. "Defining Cybersecurity Law" *Iowa Law Review,* Vol. 103 (2018) p.985-1030.

[e] Department of Defence of Australian Government. "Laws of Armed Conflict" (January 11th 2017).

[f] Lazar, S. "Just War Theory: Revisionists Versus Traditionalists" *Annual Review of Political Science*, Vol. 20 (2017) p.37-54.

[g] Manantan, M. “China’s Alleged Cyberattacks Come Amid Rising Sentiments in the Philippines Over the South China Sea Disputes” *The Diplomat* (August 5th 2019).

[h] BBC News. “Russia-Trump Inquiry: Russians Charged Over US 2016 Election Tampering” (February 17th 2018).

[i] Doffman, Z. “Secret U.S. Cyber Mission Devastated Iran’s Attack Capabilities, Officials Say” *Forbes* (August 29th 2019).

[j] Flynn, G. “Cambodia Sorely Lacking Cybersecurity Professionals” *Khmer Times* (September 2nd 2019).

[k] Ibid.

[l] Parameswaran, P. “What’s Behind the New US-ASEAN Cyber Dialogue?” *The Diplomat* (October 4th 2019).

AVI PERSPECTIVE

ISSUE 2020, No. 01

Cambodia | 3rd February 2020

Cyberwarfare and Its Implications for Cambodia

LIM Menghour[a]

SEK Sophal[b]

Executive Summary

- Cybersecurity has become an emerging issue for Southeast Asian countries including Cambodia.
- For Cambodia, cyberattacks have relatively less impact on its military, but they have huge impact on the country's banking system, database of private and public institutions, and the dissemination of false information.
- Though lagging behind other countries when it comes to cybersecurity, Cambodia has been intensifying its efforts in combating cyberattacks in the country through strengthening local and international mechanisms.

[a] **LIM Menghour** is Deputy Director of the Mekong Centre for Strategic Studies (MCSS) at the Asian Vision Institute (AVI).
[b] **SEK Sophal** is Programme Coordinator at MCSS, AVI.

សេចក្តីសង្ខេបអត្ថបទ

- សន្តិសុខលើបណ្តាញអ៊ីនធឺណិតបានក្លាយជាបញ្ហាប្រឈមមួយសម្រាប់ប្រទេសនៅក្នុងតំបន់អាស៊ីអាគ្នេយ៍ដោយរាប់បញ្ចូលទាំងប្រទេសកម្ពុជាផងដែរ។
- នៅប្រទេសកម្ពុជា ការវាយប្រហារតាមប្រព័ន្ធអ៊ីនធឺណិតមិនសូវមានផលប៉ះពាល់ខ្លាំងក្លាទៅលើវិស័យយោធានៅឡើយទេ ក៏ប៉ុន្តែវាមានផលប៉ះពាល់ខ្លាំងទៅលើវិស័យធនាគារ ប្រព័ន្ធគ្រប់គ្រងទិន្នន័យរបស់ស្ថាប័នឯកជន និងសាធារណៈ និងការផ្សព្វផ្សាយព័ត៌មានក្លែងក្លាយ។
- បើទោះបីជាមានការយឺតយ៉ាវជាងប្រទេសផ្សេងទៀតចំពោះវិធានការគ្រប់គ្រងទប់ទល់នឹងការវាយប្រហារដោយប្រព័ន្ធអ៊ីនធឺណិត កម្ពុជាបាន និងកំពុងពង្រឹងកិច្ចខិតខំប្រឹងប្រែងរបស់ខ្លួនក្នុងការប្រយុទ្ធប្រឆាំងនឹងការវាយប្រហារដោយប្រព័ន្ធអ៊ីនធឺណិតតាមរយៈការពង្រឹងយន្តការជាតិ និងអន្តរជាតិ។

Introduction

With the rapid growth and diffusion of Information and Communications Technology (ICT), the world is becoming digitally connected. The digital communication is extremely fast comparable to the speed of light. The prospects of digital economy are real and promising. In 2002, the Royal Government of Cambodia launched an ICT-oriented policy reform when it introduced an ambitious e-Government project, including the Government Administration Information System (GAIS) and several other cyber systems for banking, customs and transportation. The ICT or digital technology has arguably played more critical roles in generating growth and transparency for the kingdom's private and public sectors. Despite its significant roles, the ICT has also brought with it some negative impacts particularly the growing threats from cyberwarfare. While the threats from cyberattacks are universal, cyberwarfare has apparently gained momentum in Cambodia. Although cyberattacks have less impact on the Cambodia's military, they have huge impact on the country's e-banking system, public and private databases and the credibility of media as a reliable public source of information, all of which can potentially affect Cambodia's national security and stability.

What is Cyberwarfare?

Cyberwarfare could be easily understood as the use of computer technology to disrupt the online activities of a state, organisations or individuals, especially the deliberate attacking of information systems for strategic or military purposes. The cyber-attackers use various methods to alter computer codes, logic or data, resulting in a data breach or system failure. This is an emerging threat that transcends borders and has the potential to cause untold damage, both financially and socially with more than 90 percent of Asia-Pacific businesses having been the victims of cyberattacks.[a]

General Situation of Cyberwarfare in Cambodia

Today, Southeast Asian countries including Cambodia are lagging behind other more developed countries when it comes to cybersecurity – the protection of computers, servers, mobile devices, electronic systems, networks and data from malicious attacks or cyberattacks. Cyberwarfare has been recognised as an emerging issue in Cambodia. Therefore, the country needs to do more to enhance its cybersecurity capability to protect its citizens and national interests against the threat.

Cambodia has not yet had in place a strong protection mechanism or institution to protect users and companies against cyberwarfare, leading to an increase in cyberattacks in the country. According to Kaspersky Lab, in 2018 alone, Cambodia witnessed 4,590,076 online cyberattacks that affected 30.5 percent of internet users, an increase of 2,835,938 compared with the attacks in 2017. Even the Facebook Page of Cambodian Prime Minister Hun Sen was also hacked in February 2019. Arguably, cyberwarfare has already taken root in the kingdom although its existence is not yet widely known among the public. As a result, experts fear that government institutions, businesses and individuals are not well prepared to deal with the impact of cyberwarfare because their awareness of it is still limited. Besides, despite its rapid growth, Cambodia's Information Technology (IT) sector has not yet ready to embrace this new challenge, as the country has not developed sufficient human resources to support its IT businesses. The kingdom is still lacking resourceful ICT experts in cybersecurity, resulting in an increase in cyberattacks in the country.

It is also worth mentioning that the increase in cyberattacks in Cambodia has occurred at a time when cyberattacks in Southeast Asian region has also increased. Countries in the region have been trying to catch up with the Western world in the area of IT industry. Countries like Singapore, Malaysia, Indonesia and Thailand have hugely invested in this sector with an emphasis on digital infrastructure expected to play a major role in promoting economic growth in the countries. Therefore, the region's increase in IT makes it more prone to cyberattacks than ever before. Hence, Cambodia is no exception. It is exposed to more cyber threats as an increasing number of its citizens spend more time online than ever before shopping, banking, communicating, working, managing finance and socialising. This can be a major issue for the region in general and for Cambodia in particular, as they have not had good preparation and effective governance to handle the issue.

Impacts of Cyberwarfare on Cambodia

Cyberwarfare has relatively less impact on the Cambodia's military. Experts in the military tend to discuss cyberwarfare by referring to the capabilities of the digitalised information system operated to block or destroy Military Command and Control (C2). Cyberwarfare is practical only if C2 system is computer-based. However, the Cambodia's military still use conventional military hardware or old equipment from the Cold War era. Because Cambodia's C2 system is not computer-based, cyberwarfare is less harmful to the Cambodia's military. The threats from cyberwarfare; however, are not simply confined to the military. They affect other sectors such as banking system, database and the dissemination of false information, all of which directly affect Cambodia's national security.

1. Banking system

Raiding accounts of bank customers and stealing money in their credit cards have long been the common threats posed by cybercriminals. However, those threats to financial and banking sector are becoming more dangerous and evolving from targeting individuals to national and global banking system. As Symantec Corporation, a US-based software company with its headquarter in California, wrote in its 2018 Internet Security Threats, "With each passing year, not only has the sheer volume of threats increased, but the threat landscape has become more diverse, with attackers working harder to discover new avenues of attack and cover their tracks while doing so." Financial sector has become one of the most vulnerable targets of attacks. According to IBM X-Force Research in 2017, the financial service sector accounted for 65 per cent of the total cyberattacks across all industries for which it provided security services.[b] Cybercriminals become more ambitious and target banks rather than their customers.

2016 marked a year of 'extraordinary attacks' vindicating that the threats of cyberwarfare against financial and banking sector at national and global level are real. On February 4, 2016, a group of hackers successfully hacked the computer system of Bangladesh's Central Bank and stole no less than $81 million.[c] The hackers could have used malwares to deliver infected e-mails to collect passwords and usernames. According to the investigation report released on May 24, 2018 by Al Jazeera, there is "considerable evidence the hackers used the bank's credentials to access 'SWIFT', the international messaging system used to send money around the world". The hackers generated 35 fund transfer requests from Bangladesh's account with the Federal Reserve Bank in New York.[d] Four out of the 35 were successful. The money was transferred to RCBC, a bank in the Philippines, and continued to casinos before its disappearing.

The case of Bangladesh marks the biggest bank robbery by cyber criminals in modern time and may have an implication for Cambodia's banking system. Even though there has not been any reported cyberattack against the National Bank of Cambodia (NBC), it does not necessarily mean the NBC is free from any future attack. Like other developing countries in the region, the trend of e-banking in Cambodia is on the rise. Payment, fund transfer and other financial transactions are becoming internet based. Yet, how secure its e-banking system is remains questionable.

Cyber threats are sophisticated and more dangerous. Today best security mechanisms might become outdated tomorrow. As the World Bank warned in its 2018 Report of Financial Sector's Cybersecurity: Regulation and Supervision, "Attacks on cyberspace, that is, the space between interconnected computers, are increasing in sophistication, frequency, and persistence, [and] cyber risks are growing more dangerous and diverse, threatening to disrupt our interconnected global financial systems and the institutions that operate and support those systems."[e] With this regard, what happened to Bangladesh's Central Bank might also happen to Cambodia.

2. Database of private and public institutions

In addition to the banking system, Cambodia's private and public database systems are also in imminent danger to cyberattacks. Cybercriminals currently use a technique called Distributed-Denial of Service (DDoS) attacks to steal or destroy all the information or take down the government websites.[f] On February 13, 2017, for instance, the National Election Committee (NEC) reported a group of hackers tried in vain to hack the NEC's voter lists on its website. The main objective of the hackers, according to the NEC's press release, was "to change the data of the voter lists, which [the] NEC posted on its website for the information to voters."[g]

Cybercriminals target not only state institutions, but also key pubic figures, whose messages are influential to the public and society. Politicians and senior government officials, of course, are the key targets of cyberattacks. The high-profiled case of cyberattack against government officials in Cambodia was clearly seen when the Facebook Page of Prime Minister Hun Sen was hacked in late February 2019. The hackers started spreading false information about political issues on the Prime Minister's Facebook Page causing confusion to the public. Even though the Cambodian government managed to re-gain access of the Facebook page from the hackers and reported no loss of data, the incident manifests the potential risks of cyberattacks to national security, which should not be underestimated.

Cambodia is one of the most vulnerable countries in the Asia-Pacific region to cyberattacks. The majority of its private and public sectors store their database in computers with unsecured protection software. According to Keshav Dhakad, Assistant General Counsel and Regional Director of Digital Crimes Unit of Microsoft Asia, "Eight out of ten computers [in Cambodia] do not have any protection whatsoever because they are on non-genuine systems."[h] Without protection software, the database system is vulnerable to malicious software (malware) threats. Cambodia, according to Microsoft Asia's Malware Infection Index 2016,[i] ranked number seven on a list of top markets in the Asia Pacific under threats from malware. The Cambodian government has made some efforts to deal with the issues. More, however, need to be done.

3. Dissemination of false information

False information dissemination is by no means a new phenomenon to society. In fact, false information has existed since the ancient time. Deception, according to Sun Tzu's Art of War, is one of the key principles to fight and win wars. Spreading false information is, of course, central to victory. Even in modern societies, lie, leak, rumour, and fabricated news including corruption scandal circulations are quite common. Politicians lie during election campaign by offering unfulfilled promises; International corporations lure customers into buying products they do not necessarily need by running attractive commercial advertisements. Not all of these are necessarily true.

However, in the digital age, these forms of polluted information are becoming critically dangerous, triggering a climate of uncertainty and posing long-term negative impacts on national security and social stability. On July 22, 2019, for instance, the Wall Street Journal reported that the Cambodian government singed a secret agreement with China that would allow China to establish a naval base at Ream Naval Base for 30 years. Cambodia's Ministry of National Defence called the news report 'fake' and allowed journalists to access Ream Naval Base to prove that the alleged agreement is groundless.[j] While nothing was found at the site related to the alleged base agreement, the news report has generated strategic uncertainty and misperception affecting Cambodia's diplomatic relations with the U.S. and other countries in the region particularly Vietnam and Thailand. The issue of dis-information has obviously posed an imminent threat to Cambodia's national security and stability.

Cambodia's Prevention of Cyberwarfare

Though Cambodia lags behind other countries in tackling cybersecurity threats, it has initiatives and has developed action plans to respond to the threats. Over the years, the Working Group of the Council of Ministers has drafted a cybercrime legislation aimed at establishing a national Anti-Cybercrime Committee to investigate cybersecurity-related risks. In addition, local agencies like IdeaLink Consulting, a consulting firm in Cambodia, has partnered up with Molla Technology from Malaysia to provide digital banking security solutions to several banks such as ACLEDA Bank, Vattanac Bank, Hattha Kaksekar Limited Microfinance Institution and Phillip Bank, as those banks are becoming more aware of the issues and trying to find solutions to adverse the threat.[k]

A plethora of cybersecurity conferences have been organised in Cambodia in recent years in an effort to raise Cambodian people's awareness of cyber threats. Cambodia hosted the Cyber Security Asia Conference in November 2019 to provide insights into local and regional trends in cyberwarfare and cybersecurity. Such activities demonstrate the full commitment of the Royal Government of Cambodia in strengthening national cybersecurity as well as in safeguarding the kingdom from cyberattacks. The government has also issued the ICT Master Plan 2020 in order to enhance the kingdom's capacity to deal with cybercrime and to develop cybersecurity measures across the board. The implementation of the Master Plan is pretty a daunting task that requires businesses, institutions and governmental agencies in Cambodia to work together to address the common threats.

More Local and Regional Efforts to Tackle the Threats

Arguably, Cambodia should and could do more to intensify her efforts in combatting cyberattacks in the country. The Royal Government of Cambodia needs to invest more in fundamental security solutions that could provide cybersecurity framework and standards to prevent cyberattacks in the future. These include the provision of training and capacity building to Cambodian people with a focus on upgrading high quality ICT infrastructure and enhancing skilled talents that can combat cyber intrusions. In doing so, Cambodia will be able to enhance its cybersecurity defence against future cyberattacks.

Furthermore, Cambodia should seek to deepen cooperation with other countries at regional and international levels in order to combat cyber threats. For instance, the ASEAN cybersecurity capacity building efforts announced during the Singapore Cybersecurity Week 2016 may serve not only as a platform for dialogues on confidence building measures, but also as a forum to contribute to international cybersecurity norms that could enhance local, regional and global security.[l] Superpowers like the US, Russia and China respectively have vowed to assist Cambodia and ASEAN as a whole in promoting security cooperation and combating cybercrime. In this case, Cambodia should consolidate and push for such great opportunities in order to enhance her capacity, coordination and capabilities to deal with this new challenge of cyberwarfare.

It is also worth mentioning that cybersecurity is not just the sole responsibility of a government. All individuals particularly internet users should also do more to respond to the threats. Indeed, they could protect themselves through several ways such as enabling stronger authentication and passwords for their major email addresses, social media and financial accounts. Also, the users should ensure that the security software, operating system, and web browsers are clean and up to date in order to prevent any possible intrusion by unknown attackers. The passwords of their social media accounts as well as of the Wi-Fi networks should also be updated regularly, especially when the users suspect that their security is compromised. In addition, when sharing their online information, internet users should limit the amount of personal information that they share online and use privacy settings to avoid sharing information widely. These measures should be taken into due consideration by internet users in Cambodia, where online activities and connectivity have been considerably on the rise. Cybercriminals often target careless individuals and businesses who have contacted each other through various networks and exchanged critical information via digital platforms.

Conclusion

In summary, as Cambodia's economy continues to grow at a fast pace and more financial institutions are expanding their business activities on the digital platforms, it is time for the kingdom to strengthen the country's IT security in order to protect valuable data from being stolen by hackers. In other words, the growth of the information and internet-based technologies is not going to slowdown in the future. Hence, it is critical for Cambodia to take a holistic, concerted and multi-stakeholder approach to combat cybercrime and threats in order to transform Cambodia into a strong digital country by 2030. That is to say, to combat the cyberwarfare, the Royal Government of Cambodia needs to develop policies that can effectively enforce the national legal system on cybersecurity and that can push for other potential regional and global cooperation, particularly within ASEAN, so as to promote cybersecurity in the country and in the region. Companies need to rethink their long-entrenched approaches to cybersecurity. Individuals should also play more important roles than ever before in contributing to the tackling of cyberthreats by developing rigorous cyber habits as mentioned above. In short, all actors in Cambodia have to work together to minimise the risks posed by cyberwarfare.

The opinions expressed are the author's own and do not reflect the views of the Asian Vision Institute.

[a] Gerald, F. 2019. "Cambodia to host international cybersecurity conference," *Khmer Times,* August 26, 2019. Accessed: August 26, 2019.

[b] IBM. 2016. *IBM X-Force: Financial Services Most Targeted by Cybercriminals in 2016*. https://www-03.ibm.com/press/us/en/pressrelease/52210.wss

[c] Raju, G., and Manuel M. 2016. "Bangladesh Bank official's computer was hacked to carry out $81 million heist: diplomat," *Reuters,* May 19, 2016. Accessed: November 15, 2019.

[d] Steve, C. 2018. "Hacked: The Bangladesh Bank Heist," *Al Jazeera Television's 101 East*. May 24, 2018.

[e] World Bank. 2018. *Financial Sector's Cybersecurity: Regulation and Supervision*. United States of America: World Bank.

[f] "Call to improve network and IT security amid cybercrime threats," *The Phnom Penh Post,* December 07, 2018. Accessed: November 15, 2019.

[g] NEC. 2017. *Press Release of April 13, 2017*. Phnom Penh: National Election Committee.

[h] Lauren, B. 2016. "Cybersecurity more than just an IT issue, it's a business issue," *The Phnom Penh Post*, December 16, 2016. Accessed: November 15, 2019.

[i] Microsoft Report. 2016. "Malware Infection Index 2016 highlights key threats undermining cybersecurity in Asia Pacific." Microsoft Asia News Center.

[j] Dara, M. 2019. "Journalists invited to tour Ream Naval Base," The Phnom Penh Post, July 29, 2019. Accessed: November 15, 2019.

[k] Lauren, B. 2016. "Cybersecurity more than just an IT issue, it's a business issue," *The Phnom Penh Post*, December 16, 2016. Accessed: November 15, 2019.

[l] Paul, N. 2017. "Working to preserve the stability of cyberspace," *The Diplomat.* September 20, 2017. Accessed: November 15, 2019.

AVI POLICY BRIEF

ISSUE 2021, No. 04

Cambodia | 25th February 2021

Cyber Diplomacy: An International Cooperation Instrument for Cambodia in the Digital Age

TEAN Samnang[a]

PHON Sokpanya[b]

Executive Summary

- The advancement in Information Communications and Technologies (ICTs) has brought changes in how information is disseminated and how the diplomatic mode of communications is conducted. Cyber diplomacy has been recently recognised as an international cooperation instrument to deter the proliferation of cyber-attacks and sustain the peaceful use of digital technology in the digital age.
- Due to differences in interests and the application of internet norms, cyber governance has been divided between nations that support the multilateral model or cyber sovereignty and those that believe in the multi-stakeholder model or simply the internet freedom. Although several United Nations-led initiatives like the Governmental Group of Experts (GGE) and the Internet Governance Forum (IGF) have been established to address internet governance and cybersecurity issues, they fail to generate any significant outcomes.
- As a small state with limited human and financial resources, it is critically vital for Cambodia to have a clearer vision and a strong political will to develop its cyber diplomacy policy to (1) address its relatively low level of digital talent and infrastructure resources; and (2) adapt to the unpredictable future of cyberspace.

[a] **TEAN Samnang** is President of the National Institute of Diplomacy and International Relations (NIDIR), Cambodia's Ministry of Foreign Affairs and International Cooperation (MFAIC).

[b] **PHON Sokpanya** is an Advisor to NIDIR, MFAIC.

Upholding the multilateral approach by adhering to the significant role of the UN agencies in internet governance sovereignty is key to helping promote Cambodia’s self-reliance and self-development in terms of bolstering cooperation, obtaining technical assistance, strengthening confidence-building measures and building its cyber capacity.

សេចក្តីសង្ខេបអត្ថបទ

- ភាពរីកចម្រើននៃបច្ចេកវិទ្យាគមនាគមន៍ និងព័ត៌មាន (ICTs) បានធ្វើឱ្យមានបម្រែបម្រួលនៃទម្រង់ផ្សព្វផ្សាយព័ត៌មាន ដែលនាំឱ្យមានការផ្លាស់ប្តូរយ៉ាងខ្លាំង និងគួរឱ្យកត់សម្គាល់ ក្នុងដំណើរការទំនាក់ទំនងការទូតផង។ នាពេលថ្មីៗនេះ ការទូតតាមប្រព័ន្ធអ៊ីនធឺណែតត្រូវបានគេចាត់ទុកជាឧបករណ៍នៃកិច្ចសហប្រតិបត្តិការអន្តរជាតិ ដើម្បីទប់ស្កាត់ការរីកសាយនៃការវាយប្រហារតាមប្រព័ន្ធអ៊ីនធឺណែត និងជម្រុញឱ្យមានការប្រើប្រាស់បច្ចេកវិទ្យាឌីជីថលប្រកបដោយសន្តិភាព។
- ដោយសារភាពខុសគ្នានៃផលប្រយោជន៍ និងការអនុវត្តបទដ្ឋាននៃប្រព័ន្ធអ៊ីនធឺណែត អភិបាលកិច្ចប្រព័ន្ធអ៊ីនធឺណែតត្រូវបានបែងចែករវាងប្រទេសដែលប្រកាន់យក multilateral model ឬអធិបតេយ្យភាពអ៊ីនធឺណែត និងប្រទេសដែលគាំទ្រ multistakeholder model ឬសេរីភាពអ៊ីនធឺណែត ។ បើទោះបីជាមានគំនិតផ្តួចផ្តើមមួយចំនួនដែលដឹកនាំដោយអង្គការសហប្រជាជាតិ មានដូចជា ក្រុមជំនាញតំណាងឱ្យរដ្ឋាភិបាលនីមួយៗ (GGE) និងវេទិកាអភិបាលកិច្ចប្រព័ន្ធអ៊ីនធឺណែត (IGF) បានបង្កើតឡើងក្នុងគោលបំណងដោះស្រាយបញ្ហាទាក់ទងនឹងអភិបាលកិច្ច និងសន្តិសុខតាមប្រព័ន្ធអ៊ីនធឺណែតក៏ដោយ គំនិតផ្តួចផ្តើមទាំងនោះនៅមិនទាន់អាចដោះស្រាយបញ្ហាអភិបាលកិច្ចប្រព័ន្ធអ៊ីនធឺណែតបានគួរឱ្យកត់សម្គាល់នៅឡើយទេ។
- ក្នុងនាមជារដ្ឋតូចមួយ ដែលមានធនធានមនុស្ស និងហិរញ្ញវត្ថុមានកម្រិត វាមានសារៈសំខាន់ណាស់សម្រាប់ប្រទេសកម្ពុជាក្នុងការកំណត់ចក្ខុវិស័យច្បាស់លាស់ និងមានឆន្ទៈនយោបាយរឹងមាំក្នុងការអភិវឌ្ឍគោលនយោបាយការទូតតាមប្រព័ន្ធអ៊ីនធឺណែតដើម្បី ទី(១) ដោះស្រាយ កង្វះខាតធនធាន និងហេដ្ឋារចនាសម្ព័នឌីជីថល និងទី(២) សម្របទៅនឹងបម្រែបម្រួលដែលពិបាកប៉ាន់ស្មានបាន នៃប្រព័ន្ធអីនធឺរណែតក្នុងពេលអនាគត។ លើសពីនេះទៅទៀត ការប្រកាន់យកនូវ multilateral approach ដោយគោរពលើតួនាទីសំខាន់របស់អង្គការសហប្រជាជាតិក្នុងអធិបតេយ្យភាពអភិបាលកិច្ចប្រព័ន្ធអ៊ីនធឺណែត គឺជាគន្លឹះក្នុងការជួយកម្ពុជាឱ្យមានលទ្ធភាពពឹងផ្អែកលើខ្លួនឯង និងអភិវឌ្ឍប្រទេសតាមរយៈការជម្រុញកិច្ចសហប្រតិបត្តិការ ការទទួលបានជំនួយបច្ចេកទេស ការពង្រឹងវិធានការកសាងទំនុកចិត្ត និងការកសាងសមត្ថភាព វិស័យអ៊ីនធឺណែតក្នុងប្រទេស។

Introduction

The advancement in Information and Communications Technology (ICT) has made the world more interconnected and provided multifaceted benefits for economic and social development across societies (United Nations 2018). The fast-paced technological development has changed how information is disseminated and how the diplomatic mode of communications is conducted. However, amid these benefits, technological innovations are associated with risks, uncertainties and threats, including cyber espionage, cyber-attacks, identity theft, among others, posed by both state and non-state actors. These emerging cyber issues have become unconventional threats that endanger international peace, stability and security. Due to frequent cyberattacks targeting Europe, the European Union (EU) has been very active in preventing and mitigating cyber threats. For instance, all EU member states have introduced their national cybersecurity strategies to address cyber threats at the country level (Ziolkowski 2013). The EU has also upheld the principle of cyber diplomacy, emphasising cyber capacity and trust-building with partners to develop institutional capacity to respond to and recover from cyberattacks and promote inclusive and sustainable growth in the region (Latici 2020).

Cyber diplomacy can be defined as "the use of diplomatic resources and the performance of diplomatic functions to secure national interests concerning cyberspace" (Barrinha and Renard 2017). It serves as a mechanism to promote dialogues, facilitate communication and negotiate agreements to enhance global cyber governance, reduce cyber confrontations and resolve cyber-related issues peacefully by creating cybersecurity and confidence-building measures between states based on agreed international norms. Cyber diplomacy includes, but not limited to, cyber dialogues, internet freedom, human rights in cyberspace and other cyber-related issues (Ziolkowski 2013).

Given that cyber diplomacy is a relatively new discipline, the field itself remains underexplored from the perspectives of International Relations. The reason is that cyber issues were initially considered technical matters to be predominantly addressed by experts. It has later received recognition as a key topic for countries' foreign policies and become a necessity for governments to formulate national cyber strategies to deter the proliferation of cyber-attacks and sustain the peaceful use of digital technology. To further complicate the matters, cyber governance, one of the main components of cyber diplomacy, has yet to have a universal body and law to govern this domain (Kanuck 2010). The ongoing issue concerning 'freedom of the internet' and 'sovereignty of the internet' has divided the international community. The United

Nations (UN) has yet to find a way to mend the gap (Kanuck 2010). Due to the differences in interests and application of internet norms, there remains a politically contentious issue of how cyberspace should be regulated and governed.

This article examines how global Internet governance has been split into two major camps and current international and regional efforts in bridging this global digital divide. It concludes with some policy options for Cambodia to enhance its cyber diplomacy strategies in response to its relatively low level of digital talent and infrastructure resources to promote global peace in the digital age.

Global Divide in Cybersecurity

From the beginning, the United States has been at the centre of cyberspace. Over four billion people are virtually connected through the Internet, making life easier (UN News 2018). Despite the exponential growth of Internet users, there is no internationally agreed framework to govern internet usage (Henriksen 2019). There are currently two major camps with different approaches towards how governments should control cyberspace, one of which is held by the United States and its allies, and another is backed by China and Russia.

The first camp, known as the multi-stakeholder model, believes in Internet freedom and that no one should be restricted from expressing themselves online. They also argue that non-state actors, such as private cooperates, non-profit organisations and individuals, should be involved in cyber governance to create norms and spread civilising missions, although the state still has the power to regulate it (Carr 2015). Powerful non-state actors include the Internet Corporation for Assigned Names and Numbers (ICANN), an American non-profit multi-stakeholder group, giant tech companies such as Google, Apple, Facebook and Amazon (aka GAFA) and Internet Service Providers (ISPs). Internet freedom can be found in the convention on cybercrime or the Budapest Convention, which is drafted by the West with almost no involvement from developing countries (Chang and Grabosky 2017). Cyberspace is still dominated by US tech giants. Therefore, Russia, China and other developing countries do not consider the multi-stakeholder approach fair enough, as they have little voice in the process.

Upholding the multilateral approach, China prioritises state sovereignty, emphasising the central role of the government with full power to regulate cyber activities of its citizens and businesses within their territories. Allowing other actors such as giant tech companies like

GAFA to dictate the sphere would endanger the state's sovereignty (Barrinha and Renard 2020). However, China's four tech giants BATX (Baidu, Alibaba, Tencent, Xiaomi), are now playing major roles in Chinese cyberspace and beyond. Recently, Huawei and ByteDance, the parent company of TikTok, were banned in the United States for national security reasons. In short, the United States and European countries want to push for policies that prioritise individual freedom and rights, while China and Russia want to put state's security as their top priority. Unlike the United States and its allies, China and Russia prefer the multilateral approach. The latter bloc has also established a multilateral organisation called the Shanghai Cooperation Organization (SCO), which has eight member states: India, Kazakhstan, China, Kyrgyzstan, Pakistan, Russia, Tajikistan, and Uzbekistan, four observer states and six dialogue partners (Yuan 2010).

The split between the two opposing blocs became even more divergent when the former US Secretary of State Mike Pompeo announced the "Clean Network" program in August 2020 to protect US citizens and companies from China's cyber intrusions. As a counter-strategy, one month later, in September, China's Foreign Minister Wang Yi proposed the Global Initiative on Data Security as a global standard on data security. The United States remains dominant in cyberspace, although China and Russia are catching up quickly.

Cyber Diplomacy in the Digital Age

Cyber diplomacy can be traced back to as early as the late 1990s when ICANN was established as an international body to administer global Internet domains. Backed by the US and Western countries, ICANN continues to be one of the most important actors in global Internet governance, although it has been the subject of controversy since its inception. International cooperation is predominantly considered a conventional instrument to jointly address global challenges such as global climate change, poverty reduction, marine pollution and nuclear wars. However, international cooperation over cybersecurity is much more complex and challenging as there has been little progress on collaboration and agreements in the last decades.

Although several UN-led initiatives like the Governmental Group of Experts (GGE) and the Internet Governance Forum (IGF) have been established to address issues related to Internet governance and cybersecurity, they fail to accomplish any significant outcomes. The GGE's second consensus report agrees that international order and law are essential for maintaining peace and stability in addressing the existing and potential threats arising from the use of ICTs (Grigsby 2017). However, since the GGE allowed only 25 countries to participate in its in-depth discussion on cyber issues, it resulted in the creation of a parallel process called Open-Ended Working Group (OEWG) proposed by Russia in 2018 (Maurer 2020), which aims to extend the discussion to all UN member states.

In 2006, the Internet Governance Forum (IGF), a global multi-stakeholder group consisting of governments, private sector and civil society groups, was established to address issues arising from the use and misuse of the Internet and facilitate Internet-related policy discussions. Through these platforms, a wide array of cybersecurity issues and confidence-building measures are brought forward for discussions. Nevertheless, none of them delineates responsible behaviours for states and international law obligations, which are tied to states' different interests and priorities (van Eeten and Mueller 2013). There have been several international and regional efforts by Russia and China to shift authority away from ICANN and to advocate for a more significant role for the International Telecommunication Union (ITU), a UN agency, in Internet governance.

The only international legally binding instrument put in force is the Budapest Convention on Cybercrime adopted by the Council of Europe in 2001. It seeks to address cybercrimes and regulate cyber governance by engaging cooperation and harmonising law enforcement against cybercrimes between nations (Renard 2018). However, because the cyber domain has been used to exhibit power by the United States and its allies, the Budapest Convention shows a lack of trust and concerted effort in collectively establishing multilateral rules against cybercrimes (Chaturvedi et al. 2014). Major countries, including China, Russia, and India, neither recognise nor ratify this convention. For the ASEAN region, although some of its member countries are moderately aligned with the Budapest Convention, other countries like Myanmar, Indonesia, and Cambodia have incomplete cybercrime laws required by the convention (Chhang 2020).

At the regional level, there are several intergovernmental or multilateral organisations such as the Organization for Security and Cooperation in Europe (OSCE), Shanghai Cooperation Organisation (SCO) in the Eurasian region, BRICS's working group of cyber experts created in 2014, and ASEAN Regional Forum's work plan on security and the use of ICTs established in 2017. Besides international and regional initiatives, there are also other noticeable bilateral initiatives between countries trying to address cybersecurity or internet governance issues using diplomatic instruments. These agreements include the US-Russia dialogue in 2013, the agreement between the United States and China in 2015 to stop conducting or supporting cyber theft of intellectual property of each other, the US-Japan cooperation in cybersecurity in the same year, and the Sino-Russia agreement on not to conduct cyberattacks against one another.

Cambodian Cybersecurity and Cyber Diplomacy

With its high proportion of the young population, Cambodia is one of the most competitive mobile markets in the region, with 116 mobile-cellular subscriptions per 100 people, and almost half of its population has access to the Internet mainly through mobile phones (ITU 2018). According to the United Nations' E-Government survey in 2020, Cambodia's E-Government Development Index (EGDI) had markedly improved in recent years, thanks to improved telecommunication infrastructures and engagement of citizens in decision-making through social media platforms (United Nations 2020). Being cognizant of the importance of this digital technology, Cambodia fully supports the development of digital connectivity and digital-led society and economy to achieve the country's resilience and sustainable development.[a]

Although ICTs provide opportunities for the country to accelerate social and economic growth, it comes at a price. Due to a relatively poor protection management system and the lack of adequate legal and regulatory framework, and limited human and financial resources, these cybercrime-related issues are challenging for Cambodia to coordinate and respond to (Beschorner et al. 2018). A study conducted by the Cambodian Development Research Institute (CDRI) in 2020 on the cyber government suggests a large gap between the rapid implementation of new technologies and the capacity to take measures against consequent cyber threats. There is a shortage of cybersecurity professionals in Cambodia, as even Prime Minister Hun Sen's Facebook account was hacked in February 2019 (although he could get it back a few days later with help from Facebook (Chheng 2019). During the COVID-19 pandemic, preventing fake news and misinformation from circulating throughout social media is another challenge the government has addressed.

To tackle the growing threats of cyberattacks, Cambodia has established the Anti-Cybercrime Department, a specialised unit under the National Police of Cambodia, and Cambodia's

[a] During the 17th ASEAN-China Expo, Cambodia's Prime Minister Hun Sen emphasised the necessity to increase digital connection development with a particular attention to rejuvenating the country's economy in the post-COVID-19 pandemic.

National Computer Emergency Response Team (CamCERT). Nevertheless, there is no law to regulate cyberspace in Cambodia, although the draft of cybercrime law is now being reviewed by the Ministry of Interior (MoI). However, this law seems to mainly focus on user protection from cybercrimes rather than on national security (Nguon and Srun 2020). There is a law on telecommunications promulgated in 2015, but again it is to regulate the telecom sector rather than protect users and the country from cyberattacks. Furthermore, due to the lack of policy and vision, there are a few joint efforts between private organisations and government ministries in Cambodia in managing and responding to cyber risks (CDRI 2020). Despite ASEAN's declaration to prevent and combat cybercrime in 2017, Cambodia has no clear cybersecurity strategies and no commonly shared legal framework in the region based on which it can adopt to combat cybercrimes and securities (ASEAN 2017).

Considering the geopolitical and economic reasons, Cambodia has to balance the global and regional powers by strengthening its diplomatic relations with China. In terms of cyber diplomacy, Cambodia has also indicated its support towards China by officially seeking the dialogue partner status of the Shanghai Cooperation Organisation (SCO) since 2015 and endorsing the Global Initiative on Data Security soon after China launched it in 2020 (Ministry of Foreign Affairs of the People's Republic of China 2020). However, it is worth mentioning that Cambodia's foreign policy that prioritises national sovereignty and non-interference in other countries' internal affairs is more or less aligned with China's approach emphasising state sovereignty in cyberspace.

Conclusion

The incompatible ideologies of freedom of expression and state-controlled information and different cyberspace governance approaches have decelerated international agreement on cybersecurity cooperation. Although countries have tackled cybersecurity issues by upholding cyber diplomacy through expanded UN initiatives and regional and bilateral cooperation frameworks, cyber diplomacy without regard for agreed international legal binding is pointless in global cyber governance. The mounting challenges of cybersecurity and cyberspace governance issues have led to geopolitical rivalries among major powers.

As a relatively small state with limited human and financial resources, Cambodia has been increasingly influenced by China, which indicates its commitment to supporting Cambodia in safeguarding national sovereignty, dignity and economic development. However, Cambodia also needs to have a clearer vision and a strong political will to develop its cyber diplomacy policy to address its relatively low level of digital talent and infrastructure resources and adapt to the unpredictable future of cyberspace. Multilateral cooperation adhering to sovereignty and international law is key to projecting Cambodia’s foreign policy positions to domestic and foreign audiences, promoting Cambodia’s self-reliance in obtaining technical assistance, strengthening confidence-building measures and building its cyber capacity.

The opinions expressed are the author’s own and do not reflect the views of the Asian Vision Institute.

References

ASEAN. 2017. "ASEAN Declaration to Prevent and Combat Cybercrime." https://asean.org/wp-content/uploads/2017/11/ASEAN-Declaration-to-Combat-Cybercrime.pdf

Barrinha, André, and Thomas Renard. 2017. "Cyber-Diplomacy: The Making of an International Society in the Digital Age." *Global Affairs* 3 (4–5): 353–64.

Carr, Madeline. 2015. "Power Plays in Global Internet Governance." *Millennium: Journal of International Studies* 43 (2): 640–59. https://doi.org/10.1177/0305829814562655.

CDRI. 2020. "Cybergovernance in Cambodia: A Risk-Based Approach to Cybersecurity." Phnom Penh: Cambodia Development Resource Institute. https://cdri.org.kh/publication/cybergovernance-in-cambodia-a-risk-based-approach-to-cybersecurity/

Chaturvedi, Manmohan, Aynur Unal, Preeti Aggarwal, Shilpa Bahl, and Sapna Malik. 2014. "International Cooperation in Cyber Space to Combat Cyber Crime and Terrorism." In *2014 IEEE Conference on Norbert Wiener in the 21st Century (21CW)*, 1–4.

Chhang, Lennon YC. 2020. "Legislative Frameworks against Cybercrime: The Budapest Convention and Asia." In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, edited Thomas J. Holt and Adam M. Bossler. Springer Nature Switzerland: Palgrave Macmillan.

Chheng, Niem. 2019. "Prime Minister Hun Sen Thanks Facebook for Restoring Account after Being Hacked." *Phnom Penh Post*. https://www.phnompenhpost.com/national/prime-minister-hun-sen-thanks-facebook-restoring-account-after-being-hacked.

Grigsby, Alex. 2017. "Overview of Cyber Diplomatic Initiatives." In *GCSC Issue Brief No 1*, 6–38. The Hague, The Netherlands: The Hague Centre for Strategic Studies (GCSC).

Henriksen, Anders. 2019. "The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace." *Journal of Cybersecurity* 5 (1), 1–9.

ITU. 2018. "Measuring the Information Society Report: ICT Country Profile." Geneva: Switzerland: International Telecommunication Union. https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR-2018-Vol-2-E.pdf

Kanuck, Sean. 2010. "Sovereign Discourse on Cyber Conflict under International Law." *Texas Law Review* 88 (7): 1571–1597.

Latici, Tania. 2020. "Briefing: Understanding the EU's Approach to Cyber Diplomacy and Cyber Defence." *European Parliamentary Research Service*. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651937/EPRS_BRI(2020)651937_EN.pdf.

Maurer, Tim. 2020. "A Dose of Realism: The Contestation and Politics of Cyber Norms." *Hague Journal on the Rule of Law* 12 (2): 283–305. https://doi.org/10.1007/s40803-019-00129-8.

Ministry of Foreign Affairs of the People's Republic of China. 2020. "Wang Yi Holds Talks with Cambodian Deputy Prime Minister and Foreign Minister Prak Sokhon." *Ministry of Foreign Affairs of the People's Republic of China* https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1823796.shtml.

Nguon, Somaly, and Sopheak Srun. 2020. "Cambodia vs Hackers: Balancing Security and Liberty in Cybercrime Law." *Konrad-Adenauer-Stiftung*. https://www.kas.de/en/web/kambodscha/single-title/-/content/cambodia-v-hackers-balancing-security-and-liberty-in-cybercrime-law.

Renard, Thomas. 2018. "EU Cyber Partnerships: Assessing the EU Strategic Partnerships with Third Countries in the Cyber Domain."*European Politics and Society* 19 (3): 321–337.

United Nations. 2020. *E-Government Survey 2020: Digital Government in the Decade of Action for Sustainable Development*. New York, NY: United Nations.

UN News. 2018. "Internet milestone reached, as more than 50 per cent go online: UN telecoms agency." https://news.un.org/en/story/2018/12/1027991

Van Eeten, Michel JG, and Milton Mueller. 2013. "Where is the governance in Internet governance?." *New Media & Society* 15 (5): 720–736.

Yuan, Jing-Dong. 2010. "China's Role in Establishing and Building the Shanghai Cooperation Organization (SCO)." *Journal of Contemporary China* 19 (67): 855–869.

Ziolkowski, Katharina. 2013. "Peacetime Cyber Espionage: New Tendencies in Public International Law." In *Peacetime Regime for State Activities in Cyberspace*, edited Katharina Ziolkowski, 425–464. Tallinn, Estonia: NATO CCD COE.

AVI POLICY BRIEF

ISSUE 2020, No. 07

Cambodia | 31st March 2020

Fighting the COVID-19 Pandemic with AI

CHHEM Sirika[a], PharmD

CHHEM Rethy[b], MD, PhD (Edu), PhD (His)

Executive Summary

❖ Although AI is not used widespread in Cambodia yet, the purpose of this article is to review its potential role in countries with advanced science and technology capabilities, in order to reflect on strategically establishing the future ecosystem for AI to develop in Cambodia.

❖ AI was used to detect and cure COVID-19 infections, and prevent further expansion of the pandemic. AI accelerates the identification of the genome sequence of the virus, hence enables the design of early test kits. AI pinpoints potential antiviral drugs and molecules that can be candidates for vaccine production. AI also helps in epidemiological studies including the prediction of outbreaks, spread and mortalities during pandemics. AI plays key roles in addressing the consequences of the pandemic: debunking fake news on social media platforms, enabling home online learning or telework.

❖ From these early experiences of AI in mitigating the COVID-19 pandemic, Cambodia may aim at establishing a proper strategy for preparedness and response to future viral outbreaks, while taking advantage of the emerging digital government and the economy.

❖ Policy Options:

[a] **CHHEM Sirika** is a Research Fellow at the Mekong Centre for Strategic Studies (MCSS) of the Asian Vision Institute (AVI).

[b] **CHHEM Rethy** is an Honorary Senior Fellow at the Cambodia Development Resource Institute (CDRI).

- Prepare various laws to guide and regulate the practices of digitalisation of governance and economy.
- Establish an ecosystem and legal framework to regulate the cyberspace and general data protection.
- Invest in digital infrastructures.
- Build digital talent in all sectors including medicine, public health and global health.

សេចក្ដីសង្ខេបអត្ថបទ

- បើទោះបីជាប្រាជ្ញាសិប្បនិម្មិត (AI) មិនទាន់ត្រូវបានប្រើប្រាស់ទូលំទូលាយនៅកម្ពុជាយ៉ាងណាក៏ដោយ គោលដៅចម្បងរបស់អត្ថបទនេះ គឺធ្វើការសិក្សាអំពីតួនាទីដ៏សំខាន់របស់ AI នៅតាមបណ្ដាប្រទេសដែលមានភាពជឿនលឿនខាងផ្នែកវិទ្យាសាស្ត្រនិងបច្ចេកវិទ្យា ដើម្បីឆ្លុះបញ្ចាំងពីយុទ្ធសាស្ត្រក្នុងការកសាងប្រព័ន្ធ AI ដើម្បីអភិវឌ្ឍកម្ពុជាទៅថ្ងៃអនាគត។
- AI ត្រូវបានប្រើដើម្បីតាមដាននិងព្យាបាលការចម្លងជម្ងឺ COVID-19 និងដើម្បីបង្ការការរីករាលដាលសកល។ AI ជម្រុញការកំណត់អត្តសញ្ញាណនៃបណ្ដុំសេនេទិករបស់វីរុស ដែលជម្រុញឲ្យមានការធ្វើតេស្ដពិសោធន៍បានឆាប់រហ័ស។ AI ចង្អុលបង្ហាញអំពីម៉ូលេគុលនិងថ្នាំប្រឆាំង វីរុសដ៏មានប្រសិទ្ធភាព ដែលអាចនាំទៅរកការផលិតថ្នាំវ៉ាក់សាំង។ AI ក៏បានជួយផងដែរនៅក្នុងការសិក្សាពីជម្ងឺឆ្លង ដែលរួមមានការព្យាករណ៍ពីការផ្ទុះ ការរីករាលដាល និងការស្លាប់ដែលបណ្ដាលមកពីជម្ងឺឆ្លង។ AI ដើរតួនាទីយ៉ាងសំខាន់ក្នុងការដោះស្រាយវិបត្តិបង្កឡើងដោយជម្ងឺឆ្លង ដូចជាការរែកមុខរកប្រភពព័ត៌មានក្លែងក្លាយនៅលើបណ្ដាញសង្គម ការអនុញ្ញាតឲ្យមានការរៀនអនឡាញ ឬការបំពេញការងារពីចម្ងាយដោយប្រើប្រព័ន្ធបច្ចេកវិទ្យា។
- យោងតាមបទពិសោធន៍ថ្មីៗកន្លងមកនេះក្នុងការកាត់បន្ថយការរីករាលដាលសកលនៃជម្ងឺ COVID-19 ដោយប្រើ AI កម្ពុជាអាចបង្កើតយុទ្ធសាស្ត្រដ៏ត្រឹមត្រូវមួយក្នុងការរៀបចំខ្លួនរួចជាស្រេចក្នុងការឆ្លើយតបទៅនឹងការផ្ទុះជម្ងឺឆ្លងនាពេលអនាគត ដោយទាញយកនូវគុណប្រយោជន៍ពីការលេចឡើងនូវសេដ្ឋកិច្ចនិងអភិបាលកិច្ចឌីជីថល។
- ជម្រើសគោលនយោបាយ៖
  - បង្កើតច្បាប់នានា ដើម្បីណែនាំ និងធ្វើនិយ័តកម្មដល់ការអនុវត្តសេដ្ឋកិច្ច និងអភិបាលកិច្ចឌីជីថល។
  - បង្កើតប្រព័ន្ធនិងក្របខ័ណ្ឌគតិយុត្តិ ដើម្បីធ្វើនិយ័តកម្មប្រព័ន្ធបច្ចេកវិទ្យានិងការការពារទិន្នន័យទូទៅ។
  - វិនិយោគលើរចនាសម្ព័ន្ធឌីជីថល។
  - បង្កើតធនធានទេពកោសល្យឌីជីថលនៅគ្រប់វិស័យ ដែលរួមមានឱសថសាស្ត្រ សុខភាពសាធារណៈ និងសុខភាពសកល។

History of AI[a,b]

Diseases have existed in human history from the dawn of time and epidemics have shaped civilisations along the way. Epidemics started when humankind shifted from the hunter-gatherer to agrarian lifestyle in which clusters of settlements permitted the outbreaks of infectious diseases through human-to-human transmission of germs. The discovery of germ theory gave rise to modern hygiene practices, which soon became the early foundation of public health. Currently, as the coronavirus (COVID-19) rapidly spreads globally and public fear becomes uncontrollable, governments and international organisations race against time trying to contain the spread, while efforts are being made to design vaccines and antivirals to protect public health. While fighting the virus, all stakeholders are also addressing the social and economic impact of this epidemic. In this multi-front global fight against the outbreak of a new virus, Artificial Intelligence (AI) technologies seem to occupy a key position in enabling this global battle. Hence, the innovative and ubiquitous role that AI plays in the current epidemic is worth exploring.

As we learn from myths and stories of ancient civilisations, AI is a concept that dates back to the Ancient Greeks, Chinese, Indians and Egyptians. “Thinking machines” were imagined in ancient Egypt 4500 years ago, while in ancient India, automated guardians had been used to protect the relics of Buddha. Around 900 BCE, in China, Yen Shi showed King Mu an automaton that could sing and act. From the 9th to the 13th century, Arab innovators and engineers created several automata that could play music or serve drinks. During the Renaissance, Leonardo da Vinci designed automata in the form of a mechanical knight, a lion, and an auto-propelled cart.

Fast forwarding to modern times, AI has now emerged as a technology that offers many practical solutions to social and economic challenges. Yet, many applications have yet to be validated. The Corona virus outbreak opens unlimited opportunities for scientists and engineers to test their innovative prototypes, both hardware and software. New approaches popularised in the West by Deep Blue’s mastery of chess and Watson’s knowledge in “Jeopardy!” have since evolved to play a part in many other fields, including the healthcare system. AI-powered tools and models have been helping in the detection and management of diseases such as breast cancer detection, determination of the Chagas vector and the improvement in communication between healthcare professionals and patients.

AI to Detect, Cure and Prevent[c,d]

AI technology is currently developing at a breakneck speed in various places across the globe. Complex algorithms and software have enabled the extraction of useful medical information from huge amounts of data that are provided by hospitals and relevant institutions. Such evidence permitted the emergence of predictive medicine and telehealth where scientists, medical and health professionals can now make their decisions to prevent and treat diseases.

In the context of COVID-19, AI technology helps in screening, thus the triage of a large population for fever in order to test them for COVID-19 virus. Thermal sensors placed at airports, train stations or other high traffic public places had not been proven effective, but this policy is in place at almost all airports. AI-temperature screening has been tested to increase the effectiveness of detecting people with fevers. In China's public areas, staff are using handheld temperature-measuring devices to screen clients. More advanced AI tools are used in the capital's train stations: Megvii installed remote fever detection structures that can measure in a crowd through masks and hats, sending alerts with an accuracy of 0.3 degrees Celsius. They only require one staff on-scene and have a range of 5 meters. Baidu's thermal sensors have a smaller margin of error (0.05 degrees Celsius) and can also screen people in motion. Sensetime serves the same purpose, with an additional face recognition functionality, which proves to be useful in the case of people wearing masks. Another interesting tool used in Chengdu is the smart helmet worn by officials in the city, allowing them to scan passers-by at a range of 5 meters for fever. An alarm rings when a high temperature has been detected in a person. One concern in a large country like China is that the epidemic itself is slowing down efforts to distribute such devices, as cities' transport systems are shutting down, which will dampen the efforts aforementioned.

Beyond the triage stage, AI, the Internet of Things (IOT) and their clinical sensors help in guiding remote patient monitoring and data analytics. Besides fever screening, AI analysis of computerised tomography (CT) scans developed by Alibaba allow for distinction between COVID-19-associated pneumonia and other lung infections. AI algorithms that combine clinical data with laboratory and imaging tests provide physicians with unprecedented evidence for a decisive clinical judgment that guarantees the best care for all patients. From the treatment perspective, machine learning (ML) examines correlation between current treatments and patient outcomes by sifting through big data in the search for the optimal treatment options. The possibility of devising treatments by using AI algorithms to identify both the virus' structure and the human genome opens opportunity for personalised cures. Beijing Genomics Institute and Baidu have been supplying researchers with such tools. BenevolentAI, a company specialised in "using AI for scientific innovation" offers tools to detect the Janus kinase inhibitor Baricitinib, as a potential new COVID-19 treatment.

AI algorithms, data science and cloud computing can accelerate the production of new vaccines. Their combined computational power helps in identifying relevant data patterns and even drug prospects to design new vaccine molecules that will be tested through animal models and initiate clinical trials processes. Giant Chinese tech companies like Alibaba, Baidu, Tencent, Huawei and DiDi invested heavily in the development of treatment and vaccines against COVID-19.

AI to Predict Patterns and Mortality Rates[e,f]

AI is a powerful tool for epidemiologists and virologists, as it helps predict the spread and mortality of a disease, thus permitting an early warning of its incidence. Data provided by computation complements the work of those experts, but do not substitute for their expertise. A Canadian AI startup company BlueDot predicted the outbreak of a SARS-like epidemic in Wuhan on 31st December 2019. The US Center for Disease Control recognised the infection on 6th January 2020 and the WHO notified the public on 9th January 2020. A young doctor from the Wuhan Central Hospital, Dr. Lee Wenliang had warned the authorities about an unusual viral infection on 30th December 2019, but did not to prevail. He later died from this this viral infection. What happened next, is now history.

Metabiota predicts and tracks early epidemics by analysing flight traveler data. These disease tracker systems use Natural Language Processing (NLP) and Machine Learning (ML) to crunch flight data, news reports, social media, climate, local livestock and various other sources of information to obtain their results. Mortality rates are estimated using a Recurrent Neural Network (RNN). Chatbots are helpful assistants to inform the public about the clinical symptoms and various patterns of the epidemics, thus freeing scarce health professionals with special expertise to attend to actual patients.

AI to Debunk Fake News[g]

AI can read a very large volume (billions) of web pages in almost 30 languages. NLP, voice recognition and tailored algorithms may help in selecting relevant topics and patterns of interest for users. How would AI be able to distinguish real news from fake news is indeed challenging as the definition of fake news is highly debatable, especially from the propaganda perspective. After all, AI is a just a technological tool.

During this epidemic, fake news triggered the panic buying of medicines, toilet paper, and even garlic. Detection of discriminative language related to the stigmatisation of racial minorities can help maintain social order through the removal of harmful content, while this regulation may lead to excessive censoring. Facebook and Snopes terminated their partnership, due to a disagreement about their fact-checking process.

AI to Manage Schools and Work Disruption[h]

Hundreds of millions of students are now out of school during the outbreak of COVID-19. Online learning is becoming the solution to adapt to this massive disruption. AI distance-learning and home-based working systems are gradually becoming the norm as both governments and industries take precautions in this epidemic by telling their employees and citizens to remain at home. In East Asia, children have been staying home since the Lunar New Year, yet classes have been ongoing thanks to the help of online tools, as well as television broadcasting classes across the affected regions. Video-conferencing and other tools from companies such as Bytedance and Wechat have facilitated working away from the office. Ironically, the Millennials may have been finally offered their “preferred” classrooms. This forced learning experience may trigger a much-needed reform of the traditional school centred on teachers. COVID-19 may become the best online education reformer of the 21st century!

Similarly, some of the millions of workers currently confined at home may have the unique opportunity to create new types of jobs or innovative business models, while others have to adapt old habits to meet the automation process of Industry 4.0. Indeed, while the bulk of those workers will return to their routine once the epidemic is over, the most creative and risk-taking individuals will build a new generation workforce that will sustain the incoming fourth industrial revolution.

Policy Options

AI technology may seem premature in Cambodia now, but the government is pushing to enable the digital economy in Industry 4.0 and will provide a conducive ecosystem for AI to play a major role in the Cambodian healthcare system. Therefore, Cambodia should strengthen her readiness to fight future pandemics using AI through the establishment of innovative forward-looking policies:

1. Prepare various laws to guide and regulate the practices of digital government and economy.
2. Establish the ecosystem and legal framework to regulate the cyberspace and general data protection.
3. Invest in digital infrastructures.
4. Build digital talent in all sectors including medicine, public health and global health.

The opinions expressed are the author's own and do not reflect the views of the Asian Vision Institute.

[a] Department of Classics,"Gods and Robots: Myths, Machines, and Ancient Dreams of Technology," Stanford University, https://classics.stanford.edu/publications/gods-and-robots-myths-machines-and-ancient-dreams-technology (accessed 24th March 2020)

[b] Futurity, "Greek myths have some scary ideas about robots and A.I.," https://www.futurity.org/artificial-intelligence-greek-myths-1999792/ (accessed 24th March 2020)

[c] "COVID-19 and artificial intelligence: protecting health-care workers and curbing the spread," *The Lancet*, Vol. 2 (2020), https://www.thelancet.com/action/showPdf?pii=S2589-7500%2820%2930054-6

[d] Justin Stebbing, Anne Phelan, Ivan Griffin. et al., "COVID-19: combining antiviral and anti-inflammatory treatments," *The Lancet, Infectious Diseases (2020),* https://www.thelancet.com/journals/laninf/article/PIIS1473-3099(20)30132-8/fulltext

[e] Steve Mollman, *How artificial intelligence provided early warnings of the Wuhan virus* (Quartz, 2020), https://qz.com/1791222/how-artificial-intelligence-provided-early-warning-of-wuhan-virus/ (accessed 24th March 2020)

[f] Zixin Hu1,2, Qiyang Ge3, Shudi Li4. et. al., "Artificial Intelligence Forecasting of Covid-19 in China," https://arxiv.org/ftp/arxiv/papers/2002/2002.07112.pdf

[g] Clea Skopeliti, *Coronavirus: How are the social media platforms responding to the 'infodemic'?* (First Draft, 2020), https://firstdraftnews.org/latest/how-social-media-platforms-are-responding-to-the-coronavirus-infodemic/ (accessed 24th March 2020)

[h] Sarah Dai, *China's AI champion SenseTime latest to offer online learning after students told to stay home amid coronavirus outbreak* (China: South China Morning Post, 2020), https://www.scmp.com/tech/enterprises/article/3051183/chinas-ai-champion-sensetime-latest-offer-online-learning-after (accessed 24th March 2020)

AVI COMMENTARY

ISSUE 2020, No. 20

Cambodia | 17th May 2020

Contact Tracing Technology in the Fight Against COVID-19

STIGMER-KUKIC Kristoffer Goran[a], Master of Advanced International Studies

The spread of COVID-19 has forced governments worldwide to adopt a range of different policies to combat this unprecedented phenomenon, with the main arguments of coronavirus policies being; complete lockdown versus herd immunity. Many countries have also declared a state of emergency, as a result of the pandemic declaration by the World Health Organization (WHO) on 11th March, empowering governments to impose policies or laws that would usually not be permitted. The effectiveness and success of government-implemented policies will only be shown with time.

Technology has and will be a crucial tool for governments in the fight against COVID-19, especially in countries such as China, Singapore or South Korea, by assisting public authorities in their containment policies and helping healthcare organisations to: disseminate information to citizens related to the virus (self-diagnosis questionnaires or prevention methods), send warnings to individuals that could have potentially been exposed to the virus and the monitoring and enforcement of quarantine measures. Mobile applications, CCTV cameras, drones, location tracking, smart imaging and Artificial Intelligence (AI) have all been utilised to combat the disease. Although mass surveillance may have been decried in some societies, others have accepted it for the collective benefit of their society and community. Given the increasing accessibility to smart-phones, mobile phone applications have been a popular tool in the fight against the virus, to the extent that states have coordinated with the private sector in developing tracing mechanisms, through syndromic surveillance and contact tracing – that utilise technology to track the spread of the disease and interactions amongst individuals.

[a] **STIGMER-KUKIC Kristoffer Goran** is a Research Fellow at the Centre for Inclusive Digital Economy (CIDE) of the Asian Vision Institute (AVI).

Companies and platforms such as Google, Alipay, Apple and WeChat have all developed tools to assist governments in tracking the virus and allow users and citizens to practice more effective and directed social distancing measures. However, these tools require governments and companies to track citizens using cellular signal – predominantly Bluetooth. Using Bluetooth technology allows for the applications to measure and determine the distance between smartphones and subsequently conclude whether the users were close enough to one another to transmit the virus, ultimately informing them whether they should quarantine themselves or seek testing. This method of "contact tracing" can therefore reduce the stress on public healthcare systems by preventing citizens from straining available medical resources that they may not require. Additionally, this kind of technology is more efficient and far less labour intensive than traditional methods of contact tracing, which require public health workers to interact with people infected with the virus, to learn about their movements and interactions, in order to trace the chain of interactions and contact these individuals.

Contact tracing in the form of technological applications, could be very effective if designed well, in the context of the local epidemic situation. All nations have different economic, demographic, and cultural characteristics, which influence their adoption of new technologies and how the applications should be catered to them. There are several advantages of a contact tracing application such as: relatively fast deployment, automatic and manual position tracing, efficient symptom surveys for employees, and 2nd and 3rd degree tracing. The aforementioned features will allow for the visualisation of the location of self-isolating employees and high-risk areas. Furthermore, this interactive application makes responding to the safety of employees and customers in real-time, possible.

There is additional pressure on governments that have imposed lockdown measures due to the economic impact of these policies, as in many countries non-essential businesses had to close for the duration of the imposed lockdown. Continuing development of contact tracing methods and applications could play a crucial role once lockdown measures are relaxed, by helping governments monitor activities of people as they go back to work, which could help contain a potential resurgence of the virus and impose effective de-escalation strategies. Additionally, providing authorities with location data could be crucial in adopting more targeted lockdown strategies and avoiding complete lockdown, thereby allowing citizens to access more businesses or public places, by making informed decisions based on the likelihood of transmission if access to these was provided. Consequentially, it would allow authorities to determine which establishments or public places need more stringent social-distancing measures and which ones are not risk prone.

Because these applications may raise some data privacy issues, the advantages of contact tracing digital technology should be properly explained to the public. Public health policies should cautiously keep a balance between the right to data privacy and the necessity for establishing a clear public safety policy in case of a deadly pandemic. Additionally, policy makers need to address issues related to cybersecurity, in order to prevent the leakage of personal data on the Internet, to avoid the spread of misinformation and fake news that can disrupt government efforts to control the pandemic. Providing information to other citizens about patients can be hugely problematic as it not only breaches medical confidentiality but also has the potential to fuel stigma towards diagnosed patients. For this reason, coordination between the private sector and government is paramount in order to bolster cybersecurity measures. In states of emergency, governments have a duty and obligation towards their citizens in guaranteeing public health using necessary means to combat the pandemic. However, governments need to ensure that measures taken are necessary, proportionate, transparent and limited to a certain time-period, in order to avoid the misuse of surveillance technologies that could potentially affect the contemporary narrative on data privacy rights.

With the potential risks of data privacy discussed, the utilisation of emerging surveillance technologies in the form on contact tracing could still be largely beneficial. However, balancing these risks and benefits based on sound evidence, is essential. Many of our technological applications and social media platforms already monitor our live locations and keep track of our private information. Technology will always have two sides; perhaps extreme circumstances such as a pandemic will push us to take these risks. If we do not try, we will never move forward!

The views expressed are the author's own and do not reflect the views of the Asian Vision Institute.

AVI COMMENTARY

ISSUE 2020, No. 19

Cambodia | 17th May 2020

Instigation of Science Technology and Innovation by COVID-19 Pandemic

KUOK Fidero[a], PhD

Momentum of the COVID-19 outbreak has been building up, disrupting both the global economy and socialisation by preventing and limiting the mobilisation of individuals domestically and across the world. The evolution of COVID-19 has drastically taken its course, since its first case reported in late December and expanded to over 213 countries with 2,810,325 confirmed cases, including 193,825 deaths as of 26th April 2020, according to the World Health Organization. Despite the negative consequences of this pandemic, the disruptive COVID-19 has catalysed the development of Science, Technology and Innovation (STI).

Historically, the primary impetus of STI development in the case of Cambodia, is evidenced by the massive construction of the Angkor complex using not only hydro-technological advancements, but also precision engineering – as early as the 9th century. Whilst the rise of Western science emerged only during the 16th century expanding from Italy, France, England, Netherlands, and to Germany, to name a few. This spread of Western science was seemingly observed at later stage, through the period of colonial science and the process of science transplantation, with the struggle to instill an independent scientific culture. One astonishing example of this science transplantation was the rapid progress of Japanese science, acknowledged by Charles Darwin in 1879.

Perhaps unsurprisingly, the development pace of STI highly depends on social mobilisation and political will based on which, the status of scientists must be well-recognised and pursued as personal endeavors without any inhibition of the growth of science – only so the expansion

[a] **KUOK Fidero** is Dean of the Faculty of Chemical and Food Engineering at the Institute of Technology of Cambodia (ITC).

of the scientist community could be made possible. One cannot deny nor ignore the fact that STI has drastically and unimaginably changed the world over the past two decades contributing to high economic development and human welfare.

Economically, the rapid rise of global tech start-up ecosystems – the replication of silicon valleys across the world – exhibits the dynamic creativity and innovation. Yet, the activation of technological innovation requires the harmony of various conditions and individual virtue to bring about ambidexterity of divergent and convergent thinking. What could possibly be a stimulant for technological creativity and innovation, amidst the COVID-19 pandemic? One could learn from the flight of Apollo 13 to the moon, during which as explosion on board damaged its air filtration system and put three astronauts' lives at stake. Upon receiving notification back on the ground; engineers, scientists and technicians worked around the clock virtually assisting astronauts to build a replacement of damaged system and saving astronauts' lives.

Unquestionably, the relationship between time-pressure and creativity has great impact on productivity – i.e., saving lives from COVID-19 outbreak. One could argue that an individual's sense of contribution to humanity, during a mission under extreme time-pressure, could potentially unleash powerful creative thinking and problem-solving abilities. Conversely, without a purposeful mission, one would feel unmotivated and uninspired, resulting in less energy and ability to think creatively. This time-pressure and creativity dynamic justifies the call for "One Health, One Planet" Response, where doctors, with inputs from veterinarians and environmental scientists, are working tirelessly to fight against COVID-19.

Recent surveying of more than 100 technology experts on COVID-19's potential impact on global technology and data innovation by Atlantic Council's GeoTech Center on 13th April 2020, affirmed beliefs that the COVID-19 outbreak will accelerate innovation significantly in four main fields: medical and bio-engineering sciences, the future of work, trust and supply chains, and data and Artificial Intelligence (AI), in that particular order. In the next two to five years, it is expected that the most impactful innovation attributed to COVID-19 will be seen in medical and bio-engineering sciences, whilst data and AI the will highly depend on the degree of preparedness and readiness of each country to jump-start innovation, in terms of science and technology research and development.

Less than two decades ago, the SARS epidemic gave birth to two giant e-commerce platforms: Taobao – an online shopping site which later helped Alibaba defeat eBay-backed EachNet, and JD.com – an offline operation selling disc drives and CD burners in Beijing. Seeing the landscape of COVID-19 as impact across all sectors, it is quite prominent that the coronavirus pandemic will bring about innovation and the expansion of online education, delivery services, remote working platforms, and 5G, for instance. Early testimony of this online service expansion is the openness of COVID-19-related scientific journals, such as the Lancet, SAGE, JSTOR, and ResearchGate – free-of-charge across the Web of Science.

Vis-à-vis, resonance of COVID-19 challenges has been witnessed across the globe: Alibaba GET Global Challenge, MIT COVID-19 Challenge, Smart Axiata COVID-19 Relief Fund, HacKHthecrisis Cambodia. All these challenges aim to convene the most inspired minds, to foster creativity and innovation, in addressing the pandemic. In desperate times, solidarity and collaboration are key. Simultaneously, numerous funds have been initiated including the UN COVID-19 Response and Recovery Fund, EU Joint COVID-19 Recovery Fund and COVID-19 ASEAN Response Fund, to support research and development of medicines and vaccines, as well as the utilisation of the ASEAN+3 Emergency Rice Reserve for food security. Organisations across all private, public, and non-governmental sectors are pooling their resources together in acts of philanthropy.

Will history repeat itself, as Sir Isaac Newton described his self-quarantine during the Great Plague of London, as the most intellectually productive period of his life? By working concertedly with all societal actors, with a purposeful mission of national and global importance, the COVID-19 pandemic will surely trigger impactful STI development.

The views expressed are the author's own and do not reflect the views of the Asian Vision Institute.

AVI COMMENTARY

ISSUE 2020, No. 18

Cambodia | 09th May 2020

Digitalizing Cambodia's Education System: Transforming the Learning Experience for the Future

TOUCH Darren[a], Master of Public Policy and Global Affairs

Amidst the spread of the novel coronavirus (COVID-19), students throughout the country began their unprecedented shift towards online classes. Out of necessity, Cambodia's education system is undergoing a digital transformation for the better. Although Cambodia's education system had to embrace digital technologies quickly, it has done so with resilience, innovation, and adaptability. Taking a strategic approach to digital transformation will not only democratise access to education but will also contribute to the development of human capital, further advancing the country's industrialisation.

No educational experience can match the ones offered in a classroom setting; however, in a pandemic, it is the only option to ensure students are educated in a safe and healthy environment. The closure of educational institutions throughout the world has been a measure adopted by governments to limit the spread of the COVID-19. Within a few weeks of shutting down public and private educational institutions, the Ministry of Education, Youth, and Sports (MoEYS) quickly launched an eLearning portal (elearning.moeys.gov.kh), which offers pre-recorded videos in mathematics, Khmer literature, biology, chemistry, physics, history and English. Pioneered by the government, the eLearning portal is the first time for many Cambodian students to utilise an online learning platform to access their studies. Moreover, the MoEYS in cooperation with the Japan International Cooperation Agency (JICA) recently launched 'Think! Think!' to provide free online classes to students.

[a] **TOUCH Darren** is a Research Fellow at the Centre for Inclusive Digital Economy (CIDE) of the Asian Vision Institute (AVI) and a Schwarzman Scholar at Tsinghua University.

The private sector has been a reliable partner in offering and supporting home-based learning opportunities. In addition to the MoEYS' eLearning portal, KOOMPI, a domestic laptop manufacturer, launched "KOOMPI Academy," a platform that not only has online classes for students to continue their studies, but also offers educational institutions a platform to develop their courses and upload their content online. Moreover, to ensure students have internet access, a massive barrier to eLearning for low-income students, Metfone is providing free data to all students accessing the MoEYS' eLearning portals in addition to offering Internet access at a discounted rate. Recently, Metfone, a telecommunication company with 42-percent of the country's mobile market share, has been selected as the MoEYS's official partner in providing telecommunication solutions to the ministry and schools from 2020 – 2025.

With approximately two-thirds of the population under the age of thirty, Cambodia can no longer be complacent in investing in the next generation; instead, we need to tap into the country's unlocked potentials. Both access and quality pose critical challenges to the education system, illustrating a need for improved school curricula, sufficiently trained educators, and more resources for school improvements. Digitalisation is not a silver-bullet to issues plaguing the education system. However, it has the potential to complement the much-needed educational reforms.

With the ambition to transform the country from a lower-middle-income country to upper-middle-income country by 2030 and to be a developed country by 2050, digitalising the education system should be a critical component of Cambodia's grand industrialisation strategy. So far, in light of these unprecedented and disruptive times, the government has been adaptive and agile. However, there are a few considerations we must take in a strategic approach, to a post-COVID-19 education system.

First, we need to acknowledge the digital divide between high inequalities across gender, location and socio-economic groups. In particular, students from low-income families living in rural communities face significant challenges in accessing eLearning platforms, ranging from internet affordability to owning and accessing an electronic device. Policymakers will need to ensure digitalisation does not exacerbate the inequalities within the education system or risk worsening the education gap. Second, the increasing number of partners and actors creating new digital educational resources could lead to fragmentation and overlap in the MoEYS' efforts. Although increases in educational resources are highly beneficial in expanding access to learning, the MoEYS' eLearning platform must be the primary provider of educational instruction. As a ‘public good’, education lies within the purview of the government as the benefits are spread across society in terms of employment, health and social cohesion, and economic prosperity. The emergence of educational partners and actors should not encroach on the MoEYS’ mandate. Instead, other educational resources and platforms, such as KOOMPI Academy and JICA’s ‘Think! Think!’ should complement the MoEYS’ eLearning platform. As more educational resources are developed, all material and content produced should meet the MoEYS’ standards of quality.

Third, continuous improvements to the eLearning platform will be essential to enhancing a student’s learning experience. Although the MoEYS developed the platform to meet Cambodia’s short-term educational challenges during COVID-19, the eLearning platform should be a permanent fixture within the education system. The eLearning portal has the potential to transition from a platform hosting pre-recorded lessons, to an interactive virtual classroom enabling more in-depth learning. Fourth, the success of an interactive virtual classroom will be dependent on delivery. As the eLearning portal evolves, substantial investments will be needed in equipping educators with enhanced communication skills, but more importantly, technological literacy in the ability to use and evaluate internet resources, design and implement online lessons plans, evaluate student performance, and troubleshoot minor technical issues. Fifth, affordable Internet is fundamental to the digital educational experience. Although the MoEYS has partnered with Metfone, who has been a corporate leader in ensuring students have access to affordable Internet, all telecommunication companies should adopt the same practice of waiving internet costs associated with accessing resources offered by the MoEYS.

To re-emphasize, eLearning cannot ever replicate or replace the learning experience in a traditional classroom. It is not a one-size-fits-all solution. However, when harnessed effectively and done right, it can complement the efforts of educators in teaching the next generation for the 21st century. The rapid progress made by the government should be applauded in being able to deliver a solution for the short-term. Whether intentional or unintentional, it has also sparked a new way of learning that could be the solution to not only reducing the barriers to education, but also create a more equitable system in building the talent we need to be a competitive and innovative nation – regionally and globally.

The views expressed are the author’s own and do not reflect the views of the Asian Vision Institute.

AVI COMMENTARY

ISSUE 2020, No. 09

Cambodia | 31st March 2020

COVID-19-Forced Digitalisation of Cambodia's Workforce

LA Victor[a], BComm

The current health crisis being faced by nations across the globe, has placed most of its worldwide population on edge. Facing this unprecedented situation, governments and all stakeholders race against time to save lives of the people infected by COVID-19, which has now escalated into a pandemic. Cambodia is not exempted from this phenomenal occurrence and has started to feel the economic impact of this crisis.

More companies are implementing the remote working concept or "working from home" (WFH), and the government is implementing policies to flatten the growth curve of the virus outbreak and settle in for the "New Normal". The "New Normal" is a term used in business and economics, which refers to the conditions following the recent financial crisis and global recession – a negative scenario for economies that was once abnormal, is now normal. This remote working concept has been a common practice mostly by progressive companies in developed countries, long before this pandemic arrived. Perhaps this practice will be here to stay, since it has proven to positively impact businesses through their employees delivering and even exceeding expectations, despite not working traditionally at their physical offices or workplaces.

We need to harness and empower the workforce of 10 million young Cambodians to build a sustainable and prosperous future, now. Otherwise, we would have missed out on vital national building process, by not developing the potential of these promising young people - at an average age of 25 years. Many countries in the world are envious of this young workforce, but they must first be developed and properly guided. This is where business leaders and

[a] **LA Victor** is a Digital Entrepreneur in the ASEAN region, QuickHR Solutions.

government agencies in the form of Public-Private Partnership (PPP), must work together to help identify potential, then develop and mobilise them. Technology such as AI-based work motivation systems can predict up to 98% accuracy in identifying potential to build team dynamics to increase productivity, create analytics for us to improve recruitment, and mentor and understand what drives our young workforce today. We are in a very unique position to clearly lay down the groundwork and foundation for us to utilise technology to build human resources and the ecosystem. These pillars are essential to start working together cohesively to catalyse the growth of Cambodia. History will look back on this time and the significant transformation, remembering this opportunity to build a better nation and equip ourselves for Industry 4.0.

As our nation moves towards 5G, this will enable us to connect devices to the Internet, store and process in virtual clouds, automate mundane tasks and empower new technologies – hence the call for digitalisation of the country. This shift in mentality could allow us to leapfrog the traditional stages of development. Cambodia has 8.5 million 4G subscribers, already consuming digital content at a high rate, just needing the right push to design and integrate ways to incentivise and engage users, to adopt new technologies. It is pertinent to make this part of their everyday life by raising public awareness of the benefits of digitalising education, commerce and finance, creating a usage pattern that will simplify the transition into the digital economy. This endeavor, of course, needs the whole community to work together. The government's support will play a significant role towards this initiative. Hence, the business community along with all stakeholders, need to work in tandem with the government to drive this digital transformation initiative successfully.

Another economic aspect that will be positively influenced with this digitalisation is moving towards a cashless society – establishing a new collaborative digital finance landscape. This advancement should focus on consumer experience by seamlessly integrating the digital payment, digital banking, digital payroll, and digital government services (NSSF, Taxation Filings). Mass adoption will be achieved when SMEs can operate efficiently and increase their productivity and earnings through this integrated ecosystem. Especially the younger generation, the transition to the national currency will be easier if we make the customer journey user-friendly and personalised. Overall, it should exhibit features that enhance their digital lifestyle and commercial innovations, in line with their on-demand needs.

Digitalisation is going to affect our daily lives, however, what will define us is if we are going to actively drive change or continue to wait for external assistance. The time is now, to enable technology, localise services to increase productivity and commerce through digital infrastructures. Further empowerments of our young workforce to drive the businesses in Industry 4.0 are critical factors in achieving this goal, for the benefit of the country and its people. Young Cambodians that are technology-savvy, open-minded, and forward-looking will boost their nation's workforce to a new level of productivity and efficiency, by taking advantage of digital technologies. These technologies do not necessarily have to be the most advanced or cutting-edge like AI or Blockchain, it can be as simple as moving away from paper, by using your phone or computer. The most crucial factor is the mindset and willingness to change.

The views expressed are the author's own and do not reflect the views of the Asian Vision Institute.

AVI COMMENTARY

ISSUE 2020, No. 11

Cambodia | 16th April 2020

Working from Home in the Time of COVID-19

CHHEM Siriwat[a], Master in Digital Technology Management

Telework allows an employee to perform their job, at an approved alternative worksite (e.g. home, café, co-working space). This entails remote work, during any part of regular paid hours, but does not include work while on official travel or mobile work. However, telework does not fit most workers in the manufacturing, transportation, construction, food and beverage, and retail sectors. White-collar staff naturally benefit most from the digital shift. Telework requires transformative leaders that can promote a shift in mindset towards the utilisation of digital platforms and applications, based on inclusiveness and training in digital literacy.

Although telework is an effective alternative to on-site work, it carries some risks associated with cybersecurity issues that need to be addressed properly. Studies also show that telework results in improving branding capacity for employers, less spillover effects of commuting, decreasing office maintenance costs, and minimising constant supervision of employees – focusing on deliverables. This transition from micro-management to results-based allows leaders to instill confidence in their employees, giving them more autonomy and flexibility, in hope of performing at a higher level. This major shift in work style calls for adjustments to the legal framework of labour and capital investment in terms of digital infrastructure for connectivity.

Telework should be part of the contingency plan of every organisation to cope with unpredictable events. During the COVID-19 pandemic, the World Health Organization (WHO) recommends companies to implement remote work in order to maintain business continuity, while protecting the health of employees through social distancing. This digital shift varies

[a] **CHHEM Siriwat** is Director of the Centre for Inclusive Digital Economy (CIDE) of the Asian Vision Institute (AVI).

from country to country, due to different local mindsets. Cambodia's response to the pandemic is quite remarkable in terms of shifting to telework. Combining the high penetration of smartphones, affordable mobile data and almost-addictive social media usage, Cambodia's young population is certainly an early adopter of advanced telecommunication technologies. During their self-confinement; food, drinks, and groceries are all ordered and paid for seamlessly, via numerous delivery services and financial mobile applications. Jumping from COVID-triggered food delivery to multilateral diplomacy; even regional state leaders used teleconference to exchange policy options during the online "Special ASEAN Summit on COVID-19", on 14th April 2020.

While telework is the concept of working remotely, being a digital nomad portrays the actual lifestyle that is associated with the latter. The two main characteristics of a digital nomad are to be location-independent and to utilise technology in performing their job. A digital nomad requires sustainable access to affordable and reliable internet connection, to use supporting software for content management and communication. Such software includes Zoom, Skype, Google Hangouts/Drive/Documents, Slack, Ding Talk, etc. This work-oriented software can be used to complement everyday social media applications such as WhatsApp, Telegram, WeChat, and the list goes on. The key factor is that all these software and applications can be used to transfer documents, share computer screens in real-time, and act as a platform to substitute face-to-face interaction.

Furthermore, we are able to utilise and manage these tools from the palm of our hands with smartphones – at any time or location. Thanks to these advancements in processing speed, digital storage space, and connectivity, we are able to create our personalised mobile offices, wherever we go. This new reality of flexible working has significantly impacted the way we live our lives. Instead of rushing to the office to retrieve an urgent file, we can instantly find these documents via filtered searches on our mobile devices. Whether it be at home, in the back of taxi, on the beach, or even in another country.

The workforce has become increasingly efficient in producing results remotely and this continues to grow, as our work culture progresses. However, it is not possible for all sectors to take advantage of telework, due to their need for physical presence. At the end of the day, humans also need face-to-face interaction to grow relations effectively within a team or foster leadership. With arguments from both sides presented, each organisation is unique and should strive to find the optimal balance between working remotely and at the physical workplace.

Workers that are not required in physical presence should not be forced to check-in to the workplace, but be given more flexibility to produce results efficiently at their own time and location.

The success factor is open-minded leadership focusing on results rather than office working hours, shifting from a traditional mentality – starting immediately. Moreover, disciplined communication between team members will ensure sustainable telework. With this innovative model, instead of making people work for each other, we will make technology work for us!

The views expressed are the author's own and do not reflect the views of the Asian Vision Institute.

AVI COMMENTARY

ISSUE 2020, No. 23

Cambodia | 29th June 2020

COVID-19 and Cybersecurity: Digital Exercises for Micro, Small, and Medium Enterprise in Cambodia

OU Phannarith[a]*, MBA*

The COVID-19 pandemic has created many unexpected challenges for businesses in Cambodia. We usually say that we need to unite in order to overcome a challenge, but this time, we needed to isolate in order to survive. Besides the social and economic impacts, COVID-19 has created a new environment for Micro, Small, and Medium Enterprises (MSMEs) in Cambodia to operate during the crisis – via the Internet. Internet connectivity has suddenly become overwhelming, as a primary source of communication. We must transform both our mindsets and work culture, in order to adapt during this current downturn and be economically sustainable and resilient in the long-term.

The more we are connected online, the more vulnerable we are. We have to remember that bad actors are always out there and have not taken their hands off of the keyboard. In the ASEAN region, the data breach of Tokopedia, Indonesia's largest online store, with 15 million records of users, had been leaked by an unknown hacker. Health institutions are not an exception during this pandemic. Not only do they have to deal with life and death while fighting against the virus, but they have to worry about the increase in cyber-attacks associated with COVID-19 as well. Medical agencies in the UK have been hit by ransomware attacks, while in Mongolia, they were hit by digital coronavirus malware.

Manipulating the psychology of an individual has become one of the top attack vectors so far and it has been made possible through social engineering. According to KnownBe4, a

[a] **OU Phannarith** is a Research Fellow at the Centre for Inclusive Digital Economy (CIDE) of the Asian Vision Institute (AVI) and an Assistant Professor at the Build Bright University of Cambodia.

prominent security awareness training company, cyber-attacks associated with COVID-19 have raised up to 60 per cent worldwide, targeting individuals and businesses in the first quarter of this year with 45 per cent of them asking users to either check or type their passwords on a malicious website that had spoofed the legitimate ones. The attackers leverage the COVID-19 situation through anxiety, using scare tactics and urgent calls to action including relief packages, help desk impersonations, safety measures, outbreak cases, and more.

Working from home is a new norm, bringing MSMEs to the attention of the endpoint (computer) security. When employees work from home, a new vector for cyber-attacks is opened on cooperation credentials, sensitive data, and intellectual property. Home network security is a large concern, as there is an average of ten Internet-connected devices per each home and most do not update their home routers for not just months, but years. Additionally, we rarely carry out security checks for PCs, laptops, and smart-phones, that can potentially be used as a stepping stone to attack our neighbours and others, even a thousand miles away.

Video-conferencing apps are currently becoming a new playground for bad actors. Due to the urgent change of working environments, most of the MSMEs choose communication platforms based on ease, convenience, and cost, but not on security and privacy. Naturally, every software and application has vulnerabilities, and some of those vulnerabilities could be exploited by attackers. Starting from Zoom to Microsoft Team vulnerability, most of these incidents fall into the hands of individuals who are using the technology themselves. Often, users are not equipped with basic cybersecurity hygiene and especially, up-to-date information on the events occurring in the cyber-world during this crisis.

The challenges do not only affect employees alone, but also the MSMEs that need to ensure their company systems and data are securely protected during the sudden spike of remote connections. The lack of cybersecurity policies such as remote access, back-up, access control, etc., in addition to technical measures including software licenses, antiviruses, firewalls, and patching will open doors for attackers to penetrate systems easier than ever before. In order for MSMEs to strengthen cybersecurity practices and digital exercises, they can adopt the following solutions:

Firstly, the telecommunication operators especially Internet Service Providers (ISPs), should ensure the stability and quality of their services to subscribers during this unexpected period. ISPs should exercise their business continuity process (BCP) playbook, if available, or risk losing their customers to other competitors. Secondly, cybersecurity awareness and education are crucial for every single individual at an organisation, as they play equally important roles in defending against cyber threats. These programs should be categorised as Executive-level, IT-level and User-level. Furthermore, they should be done periodically, rather than waiting for a pandemic to trigger urgency, in responding to cyber-attacks. Thirdly, organisations must stay updated and be aware of the vulnerability of video-conferencing software and patch their systems appropriately, in order to minimise the risk of cyber-attacks on critical digital assets. Subscribing to online cybersecurity content could help significantly.

Fourthly, home networks should be secured by updating all internet-connected devices to their latest versions and upgrading routers to their newest models. Home networks could unintentionally become safe-houses for cyber-criminals, to use as a stepping stone towards confidential data of a linked organisation, or even launching an international attack. Fifthly, IT security policies should be implemented at the workplace concerning e-mail and Internet usage, back-up, etc. Internet access should be restricted and not available for everyone. A Virtual Private Network (VPN) should be used when there is a need to access internal resources. By having the capacity to monitor all connections in and out of an organisation's network to better understand who is accessing what, it will allow for more time to stop malicious connections at an early stage.

Lastly, properly licensed software and applications should be used and updated whenever possible. This will help organisations to protect themselves from malicious activities targeting both people and data.

The COVID-19 pandemic is playing a crucial role in accelerating Cambodia's digital transformation in both the government and private sector. Overcoming these unprecedented challenges can act as a digital exercise for all of us to be resilient in these types of extreme situations. Cybersecurity should be one of the top priorities for all MSMEs during this forced shift towards digital platforms. Transitioning out of this pandemic, a new normal for both work and life will continue to evolve, based on the utilisation of digital technologies.

The views expressed are the author's own and do not reflect the views of the Asian Vision Institute.