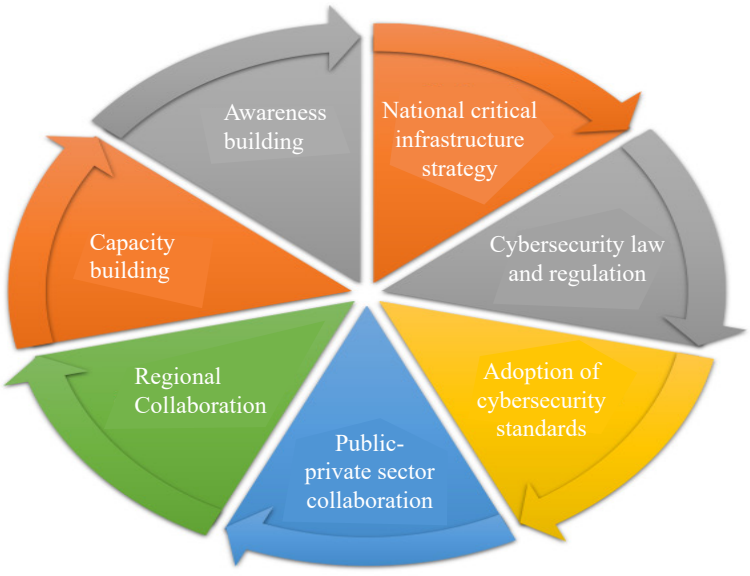
CDRI
Cambodia Development Resource Institute

30th ANNIVERSARY
CDRI 1990 - 2020

Cybergovernance in Cambodia: A Risk-Based Approach to Cybersecurity

Building Cambodia's cybergovernance program



A CDRI Publication

Special Report No. 18

January 2020

Special Report No. 18

Cybergovernance in Cambodia: A Risk-Based Approach to Cybersecurity

A CDRI Publication

CDRI
Cambodia Development Resource Institute

Phnom Penh, January 2020

ISBN-13: 9789924500186

Citation:

CDRI Publication. 2020. *Cybergovernance in Cambodia: A Risk-Based Approach to Cybersecurity.* CDRI Special Report No. 18. Phnom Penh: CDRI.

CDRI
☞ 56 Street 315, Tuol Kork
✉ PO Box 622, Phnom Penh, Cambodia
☎ +855 23 881 384/881 701/881 916/883 603
@ cdri@cdri.org.kh
🌐 www.cdri.org.kh

Layout and cover design: Oum Chantha
Edited by: Susan E. Watkins
Printed and bound in Cambodia by Go Invent Media (GIM), Phnom Penh

Table of Contents

List of figures and tables

Acknowledgements

This background paper was researched and drafted by Joseph A. Pidala, Universita di Bologna, Bologna Business School, who was commissioned by CDRI to provide capacity building to staff and to conduct a preliminary assessment of the state of Cambodia's cybergovernance. The draft paper benefited immensely from feedback and contributions from Mr Ou Phannarith, Director of the Department of Information and Communications Technology Security, Ministry of Posts and Telecommunications.

Abstract

To understand cyber risk in Cambodia and equip policy leaders to oversee it, this paper assesses the successes and challenges of current cyber risk management efforts in Cambodia and throughout the Association of Southeast Asian Nations (ASEAN) region. The findings suggest that there is a large gap between the rapid implementation of new technologies in Cambodia and the capacity to govern consequent cyber threats. Further, current efforts in Cambodia lag behind those in other ASEAN member states, and there have been multiple cyberattacks in the past five years. Policy action must be taken to protect the people and critical information infrastructure of Cambodia.[1] An effective cybergovernance framework requires four key elements: transparent governance systems, adequate human and technical resources, regional collaboration, and clearly defined metrics. Transparent government systems provide means for subject matter experts to help develop and express their views on cybersecurity policy as well as promote a democratic process whereby citizens can share their input freely. It is the government's obligation to use cyber policy to protect its people from cyberattacks while also keeping civil liberties intact. The protection of Cambodia's critical information infrastructure cannot be left to one person or organisation alone as any cyberattack directly threatens Cambodia's vision for becoming a fully developed country by 2050, an ambitious goal Prime Minister Hun Sen has emboldened the country's policymakers, business leaders, academics and citizens to achieve. Thus, strengthening collaboration and developing cyber capacity across the ASEAN region are necessary to develop baseline skills and knowledge to implement cyber systems and processes. Currently, Cambodia does not have enough resources to tackle cybersecurity alone. Cambodia must not only train internal resources but also engage in collaborative efforts with other ASEAN member states and use regional and international frameworks, including ISO27001, the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), which have already been proved effective at enhancing, strengthening and improving cybersecurity framework.

1 The Singapore Cybersecurity Bill of 2017 defines critical information infrastructure as "a computer or a computer system that is necessary for the continuous delivery of essential services which Singapore relies on, the loss or compromise of which will lead to a debilitating impact on the national security, defense, foreign relations, economy, public health, public safety or public order of Singapore."

1. Introduction

As the number of cyberattacks continues to rise, governments and businesses will increasingly feel the repercussions on the global economy. By 2020, the lack of cybersecurity readiness could lead to a USD3 trillion loss in global economic value (World Economic Forum 2014). Although the bulk of the breaches have occurred in developed countries, cyber risk in ASEAN member states should not be overlooked as the region further integrates information and communication technology (ICT) systems into global supply chains. Cybercriminals will always target the weakest link, and it is common for large companies to be vulnerable to attack through third-party partners, suppliers and vendors in their supply chain. Large-scale breaches are already a problem in the ASEAN region and will rapidly increase if the deployment of technology outpaces cybersecurity expertise, awareness and resources. By 2020, the region is predicted to have an internet penetration rate of 480 million users, about three-quarters of the population, almost double the rate in 2017 of 260 million users (Google and Temasek 2016). In Malaysia, cybercrimes accounted for 70 percent of reported crimes in the country in 2013 (Majid 2013). Although there are fewer quantitative studies on the financial impacts of cybercrime in ASEAN than in western countries, and this will be a limitation of the study, Norton (2013) reported that cybercrime cost Singapore USD1 billion in 2013. The need for proper governance of cyber security is being increasingly recognised as a key aspect of reducing cyber risk. The Council of Councils, an international initiative that releases a yearly Report Card on International Cooperation to direct high-level attention to the world's most pressing policy challenges, rated managing cybergovernance the sixth of 10 global priorities for 2019, ahead of combating transnational terrorism and promoting global health (Council of Councils 2019).

The objectives of this paper are to understand recent cyber events and current governance processes in a succinct, organised report. To do this, the methodology was to review current policy and governance systems in place in Cambodia and other ASEAN member states, along with strategic goals and plans published by ministries, research centres and large international companies. As a new topic, prior research studies are limited. This paper represents an effort to raise awareness and spark meaningful dialogue about cybergovernance and cybersecurity strategy. The paper starts with a broad overview of regional efforts, then focuses on specific efforts in Cambodia, and lastly offers some recommendations and sets out specific action steps Cambodia can take in the next five years as it tackles the development of its cybergovernance program. The main goal is for policymakers, government officials and business leaders to be able to use this information to develop and improve their policies and governance systems. Additionally, the hope is that fellow researchers can expand on these findings and keep up with emerging technologies and the rapid pace of technological change in Cambodia.

2. Cybergovernance efforts in the ASEAN region

Before diving into an analysis of the actions Cambodia and other ASEAN member states have taken to strengthen cybersecurity framework, it is important to understand the context behind these efforts. Far too often, cybersecurity efforts are reactive and ad hoc, meaning action is only taken when forced by either a breach of security or regulation, so it is important to recognise the cyberattacks that have affected the region. After understanding the impacts of cybersecurity incidents in the ASEAN region, the paper discusses what cybersecurity organisations are doing to prevent future incidents from occurring. Collaboration on cybersecurity between Cambodia and other ASEAN member states is critical for Cambodia to develop and attain the goals of a successful cyber governance strategy. In addition, the paper includes an analysis of ASEAN's

cyber governance efforts as there are far more efforts taking place regionwide than in Cambodia alone from which to draw recommendations and conclusions.

2.1 Notable cyberattacks

To understand the impact cyberattacks can have in the ASEAN region, five incidents from five countries, including Cambodia, from the past 10 years (2010–2019) were selected for brief discussion due to their distinct political effects. The first incident was a denial-of-service attack in 2010 on Myanmar's then main internet provider, the Ministry of Post and Telecommunications, shortly before the 2010 national election. Denial-of-service attacks are very common, easy to execute, and can cause mass disruptions to ICT networks. To execute the attack, hackers overloaded the network of Burma's main internet service provider, the Ministry of Post and Telecommunications, causing countrywide internet communication to slow to a crawl. As a result, the ministry was unable to provide a stable internet connection, and public service broadcasting of crucial information for voters over the election period was restricted (Chang 2017). Second, a cyber incident occurred in Cambodia in 2012 when the co-founder of The Pirate Bay, a website known for sharing software and media via copyright infringement, was arrested by Cambodian authorities and deported. In protest, two international hacking groups executed a cyberattack on the Cambodian government. The first group, NullCrew, attacked several Cambodian businesses, government and armed forces websites and leaked highly confidential information and passwords online. The second group, Anonymous, stole and leaked 5,000 government documents on the dark web from Cambodia's Ministry of Foreign Affairs (Nguon 2017). It is not known whether the passwords or confidential information have been used with malicious intent or whether the hack was simply a threat, but the data will now be forever in the hands of anyone who wants access.

Third, in another incident intended to disrupt a national election, shortly before the 2016 Philippine general election, the hacking group Anonymous Philippines hacked the Philippine Commission on Elections website calling for tighter security on vote counting machines. One day later, the hacking group LulzSec Philipinas hacked and posted the entire database of the Commission on Elections online, including voter data containing 1.3 million passport numbers and 15.8 million fingerprints (Trend Micro 2016). Such attacks not only expose sensitive information, but also weaken the people's trust in the government. The fourth incident, also in 2016, took place after Thai authorities arrested and sentenced two Myanmar workers for murdering two British tourists on the island of Koh Tao. In protest to the controversial case, Myanmar vigilantes took down 300 Thai government websites demanding justice and that tourists boycott Thailand until Thai authorities change the way they handle investigations involving foreigners (Bangkok Post 2016). Lastly, during the 2016 South China Sea dispute, hackers suspected to be from China launched an extensive hacking campaign against Vietnam. In one instance, Vietnam Airlines was hacked and the personal information of over 400,000 frequent flyers posted online (Chang 2017). Additionally, flight monitors at Hanoi and Ho Chi Minh airports were defaced and public announcement systems were hijacked to broadcast offensive messages about the dispute (Clark 2017).

In July 2018, in Singapore's worst cyberattack, hackers stole the personal particulars of 1.5 million patients (Ministry of Health, Singapore 2018). Of these, 160,000 people, including Prime Minister Lee Hsien Loong and a few ministers, had their outpatient prescriptions stolen as well. The hackers infiltrated the computers of SingHealth, Singapore's largest group of healthcare institutions with four hospitals, five national specialty centres and eight polyclinics. Two other polyclinics used to be under SingHealth.

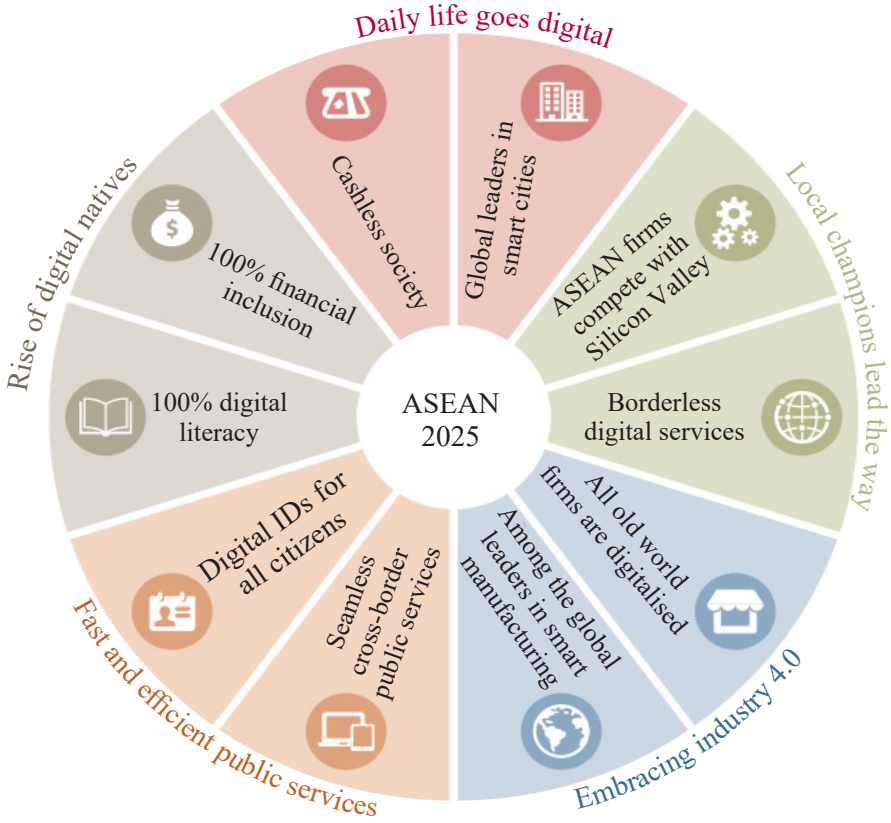
In November 2018, several of Cambodia's biggest internet service providers (ISPs) were hit by large-scale distributed denial-of-service (DDoS) attacks over several days (Cimpanu 2018). Users of EZECOM, SINET, Telcotech and Digi had difficulty accessing online services for an entire week, with the biggest problems reported in the first few days. Local news outlets called the DDoS attacks some of the biggest in the country's history. According to anecdotal reports from sources familiar with the matter, DDoS attacks totaling nearly 150 Gbps hit Cambodian ISPs.[2] With such glaring issues affecting internet connectivity all over the country, several ISPs issued a press release apologising for the technical problems. The irony, however, was not lost on some users, who were quick to point out that some ISPs that provide DDoS mitigation services were unable to safeguard their own infrastructure and needed to bring in outside specialists.

These five cyber incidents, meant to instil fear within governments and among the people, have compelled ASEAN to take action to protect the region from cyberattacks. Given the region's rapid digital development, it has become more of an imperative than ever for governments and businesses to develop cyber governance strategies.

2.2 Implications for the digital economy

As ASEAN member states continue to deepen their integration into global cyber supply chains, the cyber threat landscape grows in parallel. When organisations connect their computer systems and networks, they increase the cyber risk to the overall system. ASEAN has an aggressive agenda for advancing regional digital growth and transformation, as shown in Figure 1.

Figure 1: ASEAN digital transformation 2025



Source: Menon 2015

2 Gbps stands for billions of bits per second and is a measure of bandwidth on a digital data transmission such as optical fibre (https://whatis.techtarget.com/definition/Gbps-billions-of-bits-per-second).

If the goals of the ASEAN digital revolution are realised, such as cashless societies, 5G telecommunication networks and borderless services, the cyber risk to ASEAN countries will increase significantly, and they will become just as much a target as highly developed countries in East Asia and the West. The challenge begins with the lack of IT and cybersecurity expertise in the region, apart from Singapore, though cybersecurity is much more than a technology issue. Cybersecurity expertise and resources are crucial, but policy, regional alignment and information sharing are just as important. The lack of unifying ASEAN technology governance framework makes it difficult for governments and organisations to organise collaboration and intelligence efforts. This leads to further unmanaged cyber supply chain relationships and increased cyber incident response times. The average time it takes an organisation to identify and contain a breach is 279 days, which is 4.9 percent longer than the average of 266 days in 2018, and it takes an average of 314 days to identify and contain (Ponemon Institute 2017, 2019). These are staggering numbers given the amount of damage that can be done in such a large timeframe. Another aspect of cyber risk mitigation relates to differing national priorities and capabilities, and lack of trust, among ASEAN member states. Given that ASEAN countries are at drastically different levels of development, some governments are unable to commit to cybersecurity efforts and investments due to more pressing domestic concerns demanding their attention. There is also an innate lack of trust when it comes to national security of any kind, especially cybersecurity. Governments and organisations fear reputational harm if they admit to being hit by a cyberattack. This attitude must be replaced with one of common interest as crisis management is an integral part of the plans, programs and projects to encourage collaboration throughout the region (Dobberstein 2018).

2.3 International collaboration

ASEAN has adopted four key declarations to promote international collaboration on cybergovernance. The first is the Declaration to Prevent and Combat Cybercrime, adopted in 2017. This Declaration aims to "acknowledge the importance of the harmonization of laws related to cybercrime", "enhance cooperation and coordination among ASEAN bodies … in dealing with cybercrime to reinforce efforts through exchanges of information, experiences, and good practices", and most importantly, to "monitor and review the implementation of this Declaration …to be facilitated by the ASEAN Secretariat" (ASEAN 2017). The element to ensure that a single authority monitors, evaluates and reviews a program's progress is very important to its success. Without a single sponsor in place, programs often fail due to lack of accountability. In 2018, ASEAN adopted the ASEAN Leaders' Statement on Cybersecurity Cooperation and the ASEAN-United States Leaders' Statement on Cybersecurity Cooperation. These Statements, the first on a regional level and the second on an international level, promote the cross-border coordination of cybersecurity policy development and capacity building. Lastly, in 2019, ASEAN finalised the ASEAN-EU Statement on Cybersecurity Cooperation, which focuses on the exchange of best practices and responsible behaviour in cyberspace to enable economic progress and improve living standards across the ASEAN region. It is too soon to say whether these statements will generate tangible results. Even so, the discussions are a vital step in the right direction.

The ASEAN-JAPAN Cybersecurity Capacity Building Centre is currently under ASEAN (part of the TELSOM/TELMIN platform), and the ASEAN-Singapore Cybersecurity Centre of Excellence (Singaporean initiative to support ASEAN member states to build human capacity) is outside ASEAN.

Outside of ASEAN, two countries that have been proactive in mitigating cyber security risks in the region are Japan and Singapore. They have both been working diligently to create regional cybersecurity centres: the ASEAN-Japan Cybersecurity Capacity Building Centre in Bangkok and the ASEAN-Singapore Cybersecurity Centre of Excellence in Singapore, respectively. The Japan-ASEAN Integration Fund 2.0 supported regional cybercrime efforts by funding the ASEAN Cyber Capacity Development Project, which ran from 2016 to 2018, via the ASEAN Secretariat and with the Singapore Ministry of Home Affairs as the project proponent. This project brought together over 380 participants and over 50 trainers and experts to strengthen the ability of ASEAN countries to combat cybercrime and work together in the region, and produced a tailored report for each ASEAN country, outlining recommendations for handling cybercrime (Interpol 2018). Japan's Cybersecurity Capacity Building Centre was launched in 2018 to address the cybersecurity talent shortage aiming to tackle the increasing number of cyberattacks in the region. The centre has two goals for 2020: to increase cybersecurity expertise in the ASEAN region through the creation of technical courses, and to raise cybersecurity awareness through the competition ASEAN Cyber SEA Game (JAIF 2018). Meanwhile, Singapore is focusing more on cyber diplomacy efforts and their alignment with policy, strategy, legislation and operations (Ministry of Communications and Information, Singapore 2018). If these centres can join forces, they will be able to tackle the shortage of cyber capacity at both the technical and governance (policy) level. (These two centres focus on developing human resources for cybersecurity rather than developing common unified cybersecurity framework, programs or strategy for ASEAN.)

2.4 Cybersecurity legislation

Embedding regional cybersecurity strategy in future ASEAN joint policies is the end goal. In the meantime, each ASEAN member state must first enact laws and regulations to formalise national cyber governance programs. As of mid-2019, only three ASEAN member states had specific laws in place to combat cybersecurity threats: Singapore (Cybersecurity Act, March 2018), Vietnam (Law on Cybersecurity, January 2019) and Thailand (Cybersecurity Act, May 2019). Two additional countries, Malaysia (Computer Crime Act, 1997) and the Philippines (Cybercrime Prevention Act, 2012), have cybercrime laws. The intentions behind cybersecurity law and cybercrime law differ, however: cybersecurity focuses on the security of computer systems, while cybercrime focuses on criminal actions that involve computer systems.

Despite the growing grey area between the terms cybersecurity and cybercrime, policymakers should use the same definitions throughout formal communications. In lay terms, cybersecurity is usually used to refer to prevention, protection and cybersecurity resilience framework, and may include institutional arrangements, power of authority, compliance and standards, and enforcement of corporate compliance. Under cybersecurity law, an offence may involve picking a lock to gain access to a government building. Cybercrime, on the other hand, usually includes all types of cyber offences, investigative powers and procedures, international cooperation mechanisms, and government and private sector agencies in charge of cybersecurity. The punishment for cybercriminals is imprisonment and/or a fine. A cybercrime may involve tricking individuals to transfer funds to a foreign bank account. Cybersecurity breaches and cybercrimes target different victims and use different methods of attack, as summarised in Table 1.

Table 1: Cybersecurity vs. cybercrime

	Cybersecurity	**Cybercrime**
Attack type	technical, computer-focused	non-technical, human-focused
Target victim	infrastructure, government, businesses	individuals, families
Example	malware, denial of service	cyberbullying, internet scams

Policymakers need to consider both types of legislation when planning national cybergovernance strategy. Enacting cybersecurity law requires more specialised expertise than cybercrime law, but there are serious consequences of not having a legal framework to govern both elements.

3. Cyber governance efforts in Cambodia

Cambodia is the fastest growing economy in the ASEAN region and one of the fastest growing in the world, with annual GDP growth of 7.5 percent in 2018 (World Bank 2019). Alongside impressive economic growth, companies and organisations in Cambodia are rapidly expanding their use of technology, in part driven by the large young population; the current median age is only 25.6. From 2017 to 2019, the number of social media users increased by 71 percent from 4.9 million to 8.4 million, half of Cambodia's current population (Kepios Analysis 2019). While these promising circumstances bode well for Cambodia as a whole, rapid technological advancement could leave the country vulnerable to cyberattack. Without a clearly communicated cybergovernance strategy, efforts will remain siloed between private organisations and various government ministries. The word "cyber" in cybergovernance is not one that changes the meaning or elements of "good governance." Cybergovernance is about managing cyber risk through policy and oversight. As such, it requires sound ICT infrastructure, transparent leadership, qualified human resources and adequate funding.

3.1 Current state of cyber maturity

As Cambodia begins to develop a cybergovernance framework, there must be a set methodology and metrics to track progress. The Australian Strategic Policy Institute's International Cyber Policy Centre began such an effort in 2014, and included Cambodia in its surveys (ASPI 2014, 2017). The 2017 survey assessed 25 countries against nine factors: organisational structures, existing legislation/regulation, international engagement, computer emergency response teams (CERTs), military applications, government-business dialogue, digital economy, public awareness and internet penetration. Comparing the survey results for Cambodia in 2014 and 2017, little progress seems to have been made. However, the survey does reveal key elements of the current state of cybergovernance in Cambodia. Primarily, although there are still problems with cyber awareness, infrastructure, cybersecurity expertise and international cooperation, the government has started drafting law for the advancement of Cambodia's ICT infrastructure. In addition, the survey references the formation of Cambodia's national computer emergency response team, CamCERT. The development of a CERT is a crucial step in a nation's cybergovernance strategy. A CERT is responsible for dealing with cybersecurity incidents that affect a nation's internet community, and the CERT team is responsible for everything from announcing public security alerts and warnings to collecting cyberattack traffic from government servers. CERTs are especially important for countries in the early stages of cybergovernance because there are international standards

and global communities for information exchange, such as FIRST, the Forum of Incident Response and Security Teams. CamCERT is not a member of FIRST and lacks adequate cybersecurity expertise to mitigate cyber risk in the country effectively (Korea International Cooperation Agency 2014).

After the integration in October 2013 of the National ICT Development Authority into the Ministry of Posts and Telecommunications (MPTC), the ICT Security Department was established under the General Department of ICT with CamCERT as one of its offices. Although this department comes under the MPCT, it plays an important role in supporting and coordinating cyber incidents across Cambodia. It also helps other ministries and private sector organisations to reskill and upskill (i.e. futureproof) their workforce. Given the growing risk of cyberattacks, the Anti-Cybercrime Department, a specialised unit under the National Police of Cambodia, was established in 2016. This is the only department where victims of a cyberattack can lodge a complaint and build a case to investigate the attack and catch the cybercriminal.

3.2 Politically targeted cyberattacks

Cambodia in the past few years has experienced multiple politically targeted cyberattacks. In 2017, several senior members of the Cambodian National Rescue Party acknowledged that their email accounts had been hacked. The Ministry of Justice's Facebook account was also hacked, posting opposition party campaign events before the June commune elections (Mech and Sassoon 2017). Prime Minister Hun Sen has been targeted on many occasions. In 2019, his official Facebook account was hacked, and it was claimed that the hackers had deleted and added new content "to cause confusion in society" (Chheng 2019). The consequences of cyberattacks aiming to interfere with national elections can be particularly serious, especially when the international community is involved. Over the period of the 2018 Cambodian general election, there was a large spike in hacking attempts "to provide the Chinese government with widespread visibility into Cambodian elections and government operations" (Henderson et al. 2018). In an investigation by the industry-leading cybersecurity company, FireEye, researchers traced the malicious software to the Chinese espionage group dubbed TEMP.Periscope (Henderson et al. 2018). Additionally, in an interview with *Time Magazine*, a FireEye senior manager for cyber espionage spoke about China's strong interest in the general election given that Chinese companies, private and state-owned, have invested billions of dollars in Cambodia, adding that "any upheaval in Cambodia would be an issue for China considering their close partnership" (Seiff 2018). As the use of new technologies increases in Cambodia, such attacks may occur more frequently and with greater consequences if systems are left vulnerable.

3.3 Cambodia's cyber-related laws and regulations

At the time of writing, a new version of Cambodia's Draft Law on Cybercrime is being discussed within the Ministry of Interior. Many changes are expected to be made to the original draft law released in 2014. Because the new version of the draft law has yet to be publicly shared, the analysis below is based on the unofficial English translation of the government's Draft Law on Cybercrime released in 2014 (RGC 2014a, b).

The stated objectives of the 2014 unofficial Draft Cybercrime Law are to combat offences committed by computer systems and to ensure the safety of developing technologies. To enforce the law, a National Anti-Cybercrime Committee, chaired by the prime minister, is to be established (RGC 2014a). Overall, the structure and content of the draft law address standard cybercrime concerns such as illegal access, data espionage and intellectual property theft, and define punishments for each offence. But there are issues, specifically concerning

Article 28 that are concerning given the permissible restrictions on free speech (see Textbox 1). Similar legislation has been used in Malaysia, Myanmar, Thailand and Vietnam to restrict criticism of the government. In Malaysia, for example, a freelance graphic artist posted on Facebook a caricature of the Malaysian prime minister resembling a clown and was fined USD7,700; after the hearing, the artist's lawyer said the judge did not provide any grounds for the ruling (Sipalan 2018). According to the Constitution of the Kingdom of Cambodia, "Khmer citizens shall have the freedom to express their personal opinions, the freedom of the press, of publication and of assembly" (RGC 2010, 14). However, the constitutional right to free speech has not always been upheld for traditional media (Cambodian Center for Human Rights 2013), and the worry is that the Cambodian government will use the new cybercrime law to control content posted online as well.

Textbox 1: Cambodia's 2014 Draft Cybercrime Law: Article 28 on Contents and Websites

Any persons who engage in activities set forth in the following:

1. Establishing contents that deemed to **hinder the sovereignty and integrity of the Kingdom of Cambodia** is a punishable offense of incarceration from one to three years and fine of five hundred to fifteen hundred US dollars.
2. Publications that deemed to **incite or instigate the general population that could cause one or many to generate anarchism** is punishable of incarceration from one to three years and fine of five hundred to fifteen hundred US dollars.
3. Publications or continuation of publication that deemed to **generate insecurity, instability, and political cohesiveness** is a punishable office of incarceration from one to three years and fine of five hundred to fifteen hundred US dollars.
4. Publications or continuation of publication that deemed to be **non-factual which slanders or undermined the integrity of any governmental agencies, ministries**, not limited to departments, federal or local levels, is a punishable offense of incarceration from one to three years and fine of five hundred to fifteen hundred US dollars.

Source: RGC 2014a, 12–13

As the emboldened text emphasises, people in Cambodia can be punished based on vague, undefined terminology that is at the discretion of the government to define given that the enforcing committee is chaired by the prime minister rather than an independent body. For example, the fourth point states that non-factual publications about the government are considered an offence punishable by law, but at the same time, it is at the discretion of the government to determine which publications are "non-factual." The government can use these laws to threaten to prosecute journalists, human rights activists and anyone who criticises government officials or the ruling political party's views. The use of the law in this manner is a direct threat to online freedom of expression and has fuelled ongoing debate that started long before the internet. What restrictions on freedom of expression and personal privacy should people have to concede to in the interest of national security? If Cambodia's draft cybercrime law is passed, the final wording in Article 28 will lay the foundation for how the country handles the governance of the internet. The Cambodian government has denied any suppression of internet freedom, and when discussing the government's monitoring of local media's internet activities and usage, Cambodia's Ministry of Information spokesperson said it "will benefit the public and help stop the sharing of 'provocative information' that can cause social chaos" (Khidhir 2018). Again, this raises the question of who should define "provocative information". Governments that restrict freedom of expression and conduct mass data collection may argue that they can better control online threats by reducing

malicious online behaviours and by monitoring the internet for illegal activities. While this may be true in some cases, these practices can also encourage the spread of biased information and propaganda and target minorities to fulfil political agenda. On top of the Cambodian government's past censorship of traditional media, concerns about the potential misuse of law enforcement are intensified because the new cybercrime law has been drafted secretively, without pre-legislative scrutiny from cybersecurity experts, research centres or industry (Nguon 2017). With the urgency and complexity of cybercrime, which affects all aspects of society, cybercrime regulation must be a collaborative effort between the public, private and academic sectors.

By December 2019, the government had approved several new draft laws, including the Criminal Procedure Code, Law on Telecommunications, E-Commerce Law, Consumer Confidence Law, and the Sub-decree on Digital Signatures.

3.4 Cybersecurity capacity building

Under the current efforts of the Ministry of Posts and Telecommunications, the Department of ICT Security has set up various programs to improve the cyber capability of government officers, private sector organisations and key stakeholders. Workshops, seminars and training have been organised to enhance and strengthen the skills of individuals and organisations that provide or intend to provide online applications or services for citizens/customers.

To test cyber incident response readiness and the crisis management capabilities of chief information officers or the officials in charge of IT in each ministry, an annual cyber exercise codenamed Cyber Angkor has been conducted since 2017. The objective of this exercise is to simulate a cyberattack in order to familiarise response officers with good incident processes and procedures, as well as cyber crisis management and recovery.

Attracting young talent to the cybersecurity profession is really important for Cambodia to secure its cyber infrastructure and online services countrywide. But, increasing young people's participation in cybersecurity is not an easy task as they have not been taught or prepared by their university or college for a career in cybersecurity and computer forensics. To overcome this challenge, the Department of ICT Security organises an annual cyber competition for university students and the general public under 30 years old. The winner goes on to compete regionally in the ASEAN Cyber SEA Game and the Singapore Cyber Conquest.

Another challenge is understanding the risk of cybersecurity to both organisations and individuals. Management often fails to ringfence funds allocated to cybersecurity programs as they are considered an expense rather than an investment. Raising awareness of some key aspects of cybersecurity is therefore needed to bring everyone on board. StaySafeOnlineCambodia is a national campaign to raise cybersecurity awareness for anyone seeking to increase their expertise and knowledge on cyber risks.

4. Recommendations

4.1 Identified gaps in Cambodia's cybergovernance

Four key gaps emerge from the analysis of Cambodia's cybergovernance efforts and underlying motivations: government transparency, human and technical resources, regional collaboration, and tangible quantitative goals. That these gaps exist is not at all surprising for a developing country, even when technology is taken out of the picture. As an emerging economy, Cambodia is still in the initial stages of establishing its own highly skilled

workforce and creating partnerships with other countries and international corporations. Taking advantage of these circumstances, the government has used the opportunity to bolster its power by suppressing and restricting opposing viewpoints. Although these fundamental obstacles will remain for some time, the use of international standards, frameworks and metrics can help Cambodia put an organised system in place to protect its critical infrastructure from cyberattacks, the fundamental objective. Protecting critical infrastructure, such as public health, transport, telecommunication and utility systems, is the government's main responsibility. To that end, the government must build a unified front, including the public, private and academic sectors, to provide the insight and collaboration required to develop cyber strategy and deal with complex problems. Cambodia set aggressive goals in its vision to become a fully developed country by 2050 (Seangly 2013), including investing heavily in digital infrastructure, transforming Phnom Penh, Siem Reap and Battambang into smart cities, joining the ASEAN Smart Cities Network, and embracing Industry 4.0 in manufacturing (ASEAN 2018c). A large-scale cyberattack on critical ITC infrastructure before these technologies are fully implemented and secured could severely hinder their efficacy and expansion, and therefore, have direct negative consequences for Cambodia's economic growth. It is imperative that Cambodia prioritises a well thought out cybergovernance strategy before these technologies are implemented rather than act in an ad hoc manner once increased levels of digitalisation make critical infrastructure even more vulnerable.

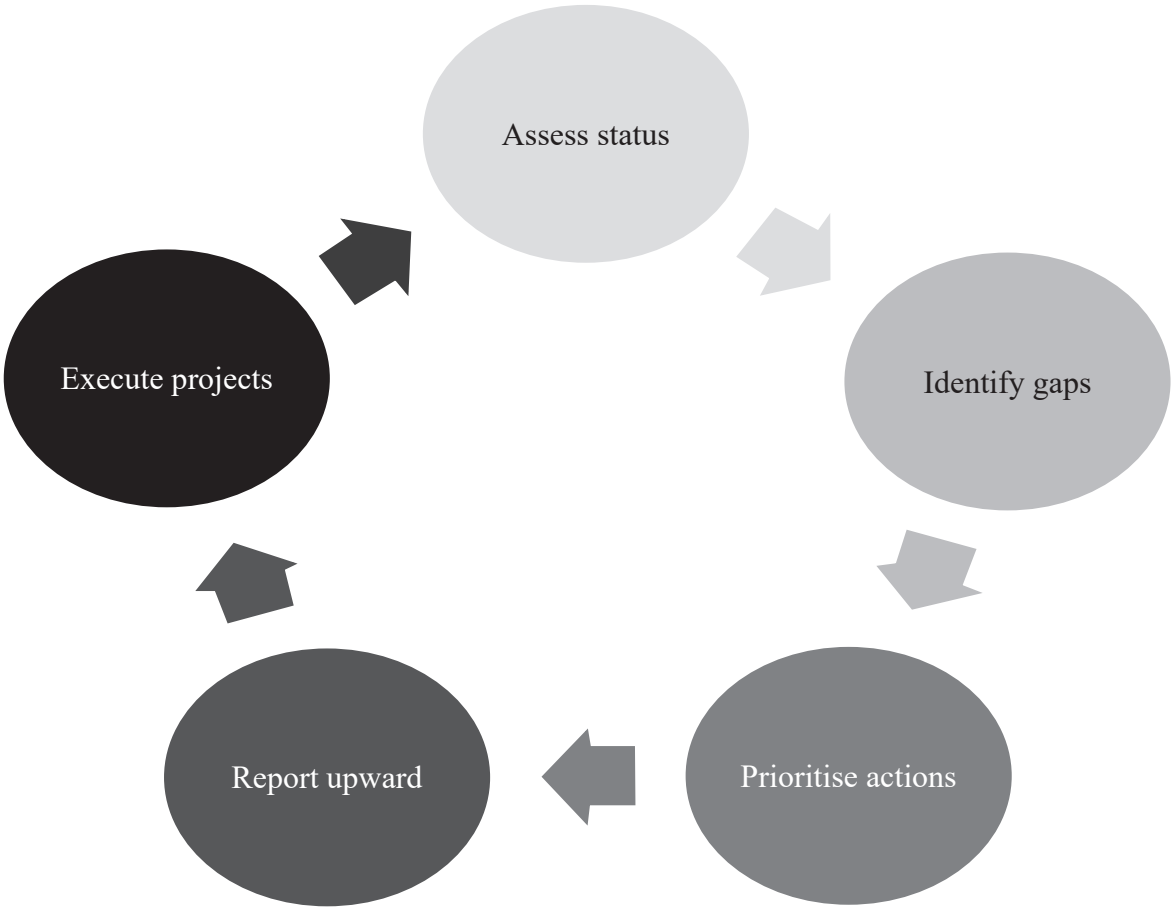
4.2 Building a cybergovernance program

Cybersecurity is complex because it touches every industry, involves all levels of government, and can have a direct financial impact on the economy. Financial risk assessments have long relied on time-tested economic models, but all risks, such as strategic, reputational, compliance and cybersecurity risk, can be modelled and mitigated in similar ways using estimates of their financial impact. Cybersecurity is unique in that cyber risk becomes a component of each of these risks. For example, a cybersecurity breach can harm an organisation's reputation, force an organisation to adjust its business strategy, and prompt new compliance requirements. Thus, cyber risk management must take a top-down, risk-based approach to properly and promptly identify and oversee cyber threats. The government should consider the following in building its cybergovernance program:

1. National strategy to protect critical information infrastructure
2. Public-private sector collaboration
3. Cybersecurity regulations
4. Adoption of cybersecurity standards
5. Regional information sharing
6. Cybersecurity awareness and outreach
7. Capacity building
8. International collaboration and cooperation

Each of these activities represents a project that should be continuously monitored for progress and achievement of specific metrics by a central cybergovernance authority, comprising government and non-government stakeholders, whose sole responsibility is the resilience of Cambodia's digital infrastructure.

Figure 2: Top-down approach to cybersecurity



International best practices should be used to gauge the current level of cybersecurity resilience so that gaps in preventative measures can be identified. Once any gaps are found, they should be prioritised based on their risk to Cambodia's digital infrastructure, including an analysis of the threats and the likelihood of cyberattacks. Once high-priority risks have been identified, solutions can be properly proposed to senior leaders for sponsorship and funding. Cybersecurity can often be a difficult topic because it involves a lot of jargon and technical language, which can be a barrier to communication. The alignment of specific, agreed-upon cyber metrics among stakeholders to achieve cyber resilience goals can build greater confidence and support for those involved. It is the responsibility of the designated cybergovernance body to ensure these stakeholders take a proactive approach to reach their targets and can apply cybersecurity regulatory compliance requirements to achieve their objectives.

4.1.1 Cybersecurity law and regulation

A good example of a diligently planned cybersecurity law is Singapore's Cybersecurity Act 2018. The Act goes into great detail about the expectations for organisations involved with critical information infrastructure in Singapore and clearly defines what the government can and cannot do in the protection of national security (Republic of Singapore 2018). Rather than stating vague, all-inclusive offences and an unclear balance of power, as in Cambodia's Draft Cybercrime Law, Singapore's Cybersecurity Act focuses on encouraging cooperation and transparency between the private and public sectors.

Textbox 2: Singapore Cybersecurity Act 2018 – Part 4: Responses to Cybersecurity *Threats and Incidents*

1) Where information regarding a cybersecurity threat or incident has been received by the Commissioner, the Commissioner may exercise […] the powers mentioned in subsection (2) as are necessary to investigate the cybersecurity threat or incident, for the purpose of –
   (a) assessing the impact or potential impact of the cybersecurity threat or incident;
   (b) preventing any or further harm arising from the cybersecurity incident; or
   (c) preventing a further cybersecurity incident from arising from that cybersecurity threat or incident.

2) The powers mentioned in subsection (1) are the following:
   (d) require, by written notice, […] any person to answer any question or to provide a signed statement in writing concerning the cybersecurity threat or incident;
   (e) require, by written notice, any person to produce to the incident response officer any physical or electronic record, or document, or a copy of the record or document, that is in the possession of that person, or to provide the incident response officer with any information, which the incident response officer considers to be related to any matter relevant to the investigation;
   (f) without giving any fee or reward, inspect, copy or take extracts from such record or document or copy of the record or document mentioned in paragraph (b);
   (g) examine orally any person who appears to be acquainted with the facts and circumstances relating to the cybersecurity threat or incident and reduce to writing any statement made by the person so examined.

3) Any person who –
   (h) wilfully misstates or without reasonable excuse refuses to give any information, provide any statement or produce any record, document or copy required of the person by an incident response officer under subsection (2); or
   (i) fails, without reasonable excuse, to comply with an order issued by a Magistrate […], shall be guilty of an offence and shall be liable on conviction to a fine not exceeding US$3,600 or to imprisonment for a term not exceeding six months or to both.

Source: Republic of Singapore 2018, 24–26

To reiterate, there are underlying differences between cybercrime law and cybersecurity law, but the effects of cybersecurity threats on Cambodia's critical infrastructure are much greater than the offences outlined in Cambodia's Draft Cybercrime Law. However, Cambodia does not have to start from scratch as it is developing its cybergovernance strategy at a time when there is an abundance of regulations and frameworks to use as a basis for its cybergovernance program.

4.1.2 Cybersecurity frameworks

There are many recognised cybersecurity standards, frameworks and metrics that Cambodia can draw on to build its cybergovernance program. This paper adopts the National Institute of Standards and Technology's (NIST 2018) framework for improving critical information infrastructure cybersecurity for two reasons: its risk-based approach and use of non-technical language. The NIST cybersecurity framework (CSF) was developed in the United States under an executive order during the Obama administration, and the latest version, v1.1, was released in 2018. The document was created in response to rapid technological advancement and increasing cybersecurity threats, which Cambodia is beginning to experience, aiming "to enhance the security

and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties" (The White House 2013). The framework specifies a clear-cut path for Cambodia to assess its current cybersecurity position, define future goals, prioritise innovation, and track and communicate progress to stakeholders. To do this, the NIST CSF defines the "Framework Core", which provides the crucial components for a dynamic cybergovernance program (see the Appendix: NIST Cybersecurity Framework). At the highest level, the Framework Core is used to assess the development of cybergovernance strategies for:

1. Identifying assets to understand cyber risk in context;
2. Protecting assets by implementing safeguards;
3. Detecting cyber anomalies as they occur;
4. Responding to cyber events when they are detected; and,
5. Recovering from cyber incidents after they occur.

Each of these areas is a part of a successful cyber risk and governance strategy, and progress in each area of implementation should be regularly evaluated against the maturity scale NIST provides:

1. Partial – ad hoc, reactive processes;
2. Risk-informed – managed, yet inconsistent processes;
3. Repeatable – standardised, consistently-applied processes; and,
4. Adaptive – continuously-evolving processes governed by policy.

Building a cybergovernance program using a framework such as the NIST CSF provides a common language to communicate cyber risk across different levels of government and diverse industry sectors responsible for overseeing Cambodia's critical ICT infrastructure.

4.1.3 Cybersecurity metrics

A cybergovernance program's success not only depends on achieving target goals, but also on defining the correct metrics in the first place. Given this, the next stage in the development of the program is carefully planning and clearly defining quantitative metrics to ensure the metrics lead to the desired outcome. Many metrics influence each other so they will prompt ministries to work together and coordinate their efforts rather than operate independently in silos. The Center for Internet Security (2010), for example, clearly defines cybersecurity metrics, broken down into relevant functions, shown in Table 2.

Table 2: Cybersecurity metrics

Function	Management perspective	Defined metrics
Incident management	How well do we detect, accurately identify, handle, and recover from security incidents?	• Mean cost of incidents • Number of incidents • Mean time to incident recovery
Vulnerability management	How well do we manage the exposure of the organisation to vulnerabilities by identifying and mitigating known vulnerabilities?	• Mean time to mitigate vulnerabilities • Number of known vulnerabilities • Mean cost to mitigate vulnerabilities
Patch management	How well are we able to maintain the patch state of our system?	• Patch policy compliance • Mean time to patch • Mean cost to patch
Configuration management	What is the configuration state of the systems in the organisation?	• Percentage of configuration compliance • Configuration management coverage • Current anti-malware compliance
Change management	How well do changes to system configurations affect the security of the organisation?	• Mean time to complete changes • Percent of changes with security reviews • Percent of changes with security exceptions
Application security	Can we rely on the security model of business applications to operate as intended?	• Percent of critical applications • Risk assessment coverage • Security testing coverage
IT security spending	What is the level and purpose of spending on information security?	• IT security spending as a percent of IT budget • IT security budget allocation

5. Conclusion: Cambodia 2025

The numbers of connected users and devices in Cambodia are rapidly increasing, and the repercussions of inaction to build a national cybergovernance strategy are an unacceptable risk to Cambodia's citizens and economy. Increasing collaboration with ASEAN and pushing cybersecurity as a national priority are two pivotal and attainable ambitions Cambodia can work towards in the next five years.

5.1 Regional collaboration

ASEAN has made significant progress in developing regional cybergovernance initiatives that Cambodia could tap into. Specifically, Cambodia should consider strong involvement in and assign a team to the ASEAN-Japan Cybersecurity Capacity Building Centre. One of the centre's goals is to train ASEAN cybersecurity experts in cyber defence, computer forensics and malware analysis. This skills training fits directly with the technical needs of NIST CSF and will produce Cambodian cybersecurity professionals with specialised skillsets. In addition, the centre is increasing cyber capacity among youth through its competition – the ASEAN Cyber SEA Game. Cambodia should consider using this as an example by setting up continuing education programs for Cambodian primary and secondary school teachers to incorporate

basic cybersecurity concepts into their curriculums as well as encourage universities to add cyber-focused courses to their degree programs. For professionals, Cambodia should also consider continuing education in the form of technical and strategy-based cyber certifications. Regionally recognised certifications can incentivise post-university learning and help Cambodian businesses better vet their applicants. Further, cyber certification could also be granted to businesses complying with industry standards set either by government or a regional private standards body. For example, in the United States, the Payment Card Industry Data Security Standards were created by a council of industry experts who obligate credit card companies (e.g. VISA and Mastercard) to adhere to security controls to reduce credit card fraud. A self-regulated standards organisation can adapt readily to emerging technologies such as e-commerce, and better protect consumers. These added security controls do not simply become an added cost for businesses either; they become a business driver and competitive advantage by promoting data security and privacy for their customers.

5.2 National priorities

For meaningful cybergovernance efforts to materialise, senior officials must prioritise resources and spending to spur action. Cybergovernance efforts start from the top and ministries must therefore agree on the intentions of cybersecurity strategy and break down siloes in order to optimise efficiency and avoid duplication of effort. To recognise the risks of a cyberattack to critical information infrastructure, the government should consider putting its officials through cybersecurity awareness training to create a baseline understanding of threats to their respective fields before enacting cybersecurity or cybercrime regulation. When the government has a clear objective of where it wants to be, government officials should organise a diverse committee of public and private institutions to develop cybersecurity regulation that focuses on protecting Cambodia's critical information infrastructure while also acknowledging citizens' online privacy as a human right. When addressing cybercrime in regulation, illegal actions should be overtly defined and represent the values of Cambodian citizens. These policies should also encourage Cambodian businesses to look to the government for resources to strengthen their cybersecurity programs. Cambodia has already set up CamCERT, a computer emergency response team. CamCERT, as the central contact for the government and private businesses to turn to for up-to-date cybersecurity threats and vulnerabilities, should be equipped with adequate qualified human resources, funding and technical training. In addition, if given the resources to join and take part in FIRST, the global Forum for Incident Response and Security Teams, CamCERT could gain access to valuable expertise and insight and take part in a developed, international information exchange to stay up to date on the latest cybersecurity trends. Lastly, the government should consider conducting an NIST CSF assessment, starting with the sectors that have the largest impact, such as e-commerce and e-government. Citizens and businesses are increasingly relying on e-services for online banking, B2B transactions, voting, paying utility bills, and so on. Yet these services are being developed without a security-by-design approach, meaning, placing an emphasis on cybersecurity at the time of development rather than afterwards. By using a phased assessment, the government could simultaneously address the most critical threats, test new processes and adapt quickly using lessons learned. A phased assessment would also allow for more accurate target completion dates and further collaboration between ministries. Each ministry, along with their assessment leads, would be able to gain valuable insights from each other and merge their strategies in a unified cybergovernance program.

References

ASEAN (Association of South East Asian Nations). 2017. *ASEAN Declaration to Prevent and Combat Cybercrime.* https://asean.org/wp-content/uploads/2017/11/ASEAN-Declaration-to-Combat-Cybercrime.pdf.

ASEAN. 2018a. *ASEAN Leaders' Statement on Cybersecurity Cooperation.* https://asean.org/wp-content/uploads/2018/04/ASEAN-Leaders-Statement-on-Cybersecurity-Cooperation.pdf.

ASEAN. 2018b. *ASEAN-United States Leaders' Statement on Cybersecurity Cooperation.* https://asean.org/storage/2018/11/ASEAN-US-Leaders-Statement-on-Cybersecurity-Cooperation-Final.pdf.

ASEAN. 2018c. *Smart City Action Plans.* Singapore: ASEAN Smart Cities Network.

ASEAN. 2019. *ASEAN-EU Statement on Cybersecurity Cooperation.* https://asean.org/storage/ 2019/08/ASEAN-EU-Statement-on-Cybersecurity-Cooperation-FINAL.pdf.

ASPI (Australian Strategic Policy Institute). 2014. *Cyber Maturity in the Asia-Pacific Region 2014: Creating a Regional Cyber Security Metric.* Research Report. Barton: Australian Strategic Policy Institute.

ASPI. 2017. *Cyber Maturity in the Asia-Pacific Region 2017.* Research Report. Barton: Australian Strategic Policy Institute.

Bangkok Post. 2016." Hackers Take out Thai Court Websites over Koh Tao Ruling." *Bangkok Post*, 13 Jan 2016. www.bangkokpost.com/thailand/general/824932/hackers-take-out-thai-court-websites-over-koh-tao-ruling.

Cambodian Center for Human Rights. 2013. *Repression of Expression: The State of Free Speech in Cambodia.* Phnom Penh: Cambodian Center for Human Rights.

Center for Internet Security. 2010. *The CIS Security Metrics.* www.itsecure.hu/library/image/CIS_ Security_Metrics-Quick_Start_Guide_v1.0.0.pdf.

Chang, Lennon. 2017. "Cybercrime and Cyber Security in ASEAN." In *Comparative Criminology in Asia,* edited by Jianhong Liu, Max Travers and Lennon Y.C. Chang, 135–148. Cham, Switzerland: Springer.

Chheng Niem. 2019. "Hun Sen's Facebook Hacked." *Phnom Penh Post*, 26 Feb 2019. www.phnompenhpost.com/national/hun-sens-facebook-hacked.

Cimpanu, Catalin. 2018. "Some of the Biggest ISPs Hit by Some of the Biggest DDoS Attacks in the Country's History." *Zero Day*, 8 Nov 2018. www.zdnet.com/article/cambodias-isps-hit-by-some-of-the-biggest-ddos-attacks-in-the-countrys-history/https://blog.apnic.net/2019/06/25/ddos-tsunami-a-cambodian-case-study/.

Clark, Helen. 2017. "The Alleged Chinese Hacking at Vietnam's Airports Shows That the South China Sea Battle Isn't Just in the Water." 6 Dec 2017. www.huffpost.com/entry/china-hack-vietnam-south-china-sea_b_11357330.

Council of Councils. 2019. *Ranking the Top Global Challenges*. Report Card on International Cooperation. www.cfr.org/interactive/councilofcou ncils/reportcard2019/#!/ranking/2019.

Dobberstein, Nikolai. 2018. *Cybersecurity in ASEAN: An Urgent Call to Action.* www.atkearney.com/documents/20152/1792707/Cybersecurity+in+ASEAN%E2%80%94An+Urgent+Call+to+Action.pdf/1e25fefa-8ecb-9f50-e262-2467ac4ea458?t=1544723905824.

Google and Temasek. 2016. "e-conomy SEA: Unlocking the $200 Billion Digital Opportunity in Southeast Asia." www.thinkwithgoogle.com/_qs/documents/4859/e-conomy_handout_1_2016 0525_eXq5Gdl.pdf.

Henderson, Scott, HYPERLINK "https://www.fireeye.com/blog/threat-research.html/category/etc/tags/fireeye-blog-authors/cap-steve-miller" \o "View all entries filed under 'Fireeye - Authors : Steve Miller'" Steve Miller , HYPERLINK "https://www.fireeye.com/blog/threat-research.html/category/etc/tags/fireeye-blog-authors/dan-perez" \o "View

all entries filed under ‘Fireeye - Authors : Dan Perez’” Dan Perez , HYPERLINK “https://www.fireeye.com/blog/threat-research.html/category/etc/tags/fireeye-blog-authors/marcin-siedlarz” \o “View all entries filed under ‘Fireeye - Authors : Marcin Siedlarz’” Marcin Siedlarz , HYPERLINK “https://www.fireeye.com/blog/threat-research.html/category/etc/tags/fireeye-blog-authors/ben-wilson” \o “View all entries filed under ‘Fireeye - Authors : Ben Wilson’” Ben Wilson and HYPERLINK “https://www.fireeye.com/blog/threat-research.html/category/etc/tags/fireeye-blog-authors/ben-read” \o “View all entries filed under ‘Fireeye - Authors : Ben Read’” Ben Read . 2018. “Chinese Espionage Group TEMP. Periscope Targets Cambodia Ahead of July 2018 Elections and Reveals Broad Operations Globally.” *FireEye,* 11 Jul 2018. www.fireeye.com/blog/threat-research/2018/07/chinese-espionage-group-targets-cambodia-ahead-of-elections.html.

Interpol. 2018. “ASEAN Cyber Capacity Development Project.” www.interpol.int/en/Crimes/Cybercrime/Cybercrime-training-for-police/ASEAN-Cyber-Capacity-Development-Project-ACCDP.

JAIF (Japan-ASEAN Integration Fund). 2018. “ASEAN-Japan Cybersecurity Capacity Building Centre (Step 2).” https://jaif.asean.org/support/project-brief/asean-japan-cybersecurity-capacity-building-centre.html.

Kepios Analysis. 2019. “Digital in Cambodia.” https://datareportal.com/digital-in-cambodia.

Khidhir, Sheith. 2018. “Cybercrime Laws and Conflicts of Interest.” *ASEAN Post,* 9 Oct 2019. https://theaseanpost.com/ article/cyber crime-laws-and-conflicts-interest.

Kingdom of Thailand. 2019. *Cybersecurity Act, B.E. 2562.*

Korea International Cooperation Agency. 2014. *Summary on Cambodian ICT Masterplan 2020.* Seongnam-si: Korea Information Society Development Institute.

Majid, Mahfuz Bin Dato’ Ab DSP. 2013. *Cybercrime: Malaysia.* www.mcmc.gov.my/skmmgovmy /media/General/pdf/DSP-Mahfuz-Majid-Cybercrime-Malaysia.pdf.

Mech Dara and Alessandro Sassoon. 2017. “Breaking: Ministry of Justice Facebook Page Hacked*.” Phnom Penh Post*, 20 May 2017. www.phnompenhpost.com/national/breaking-ministry-justice-facebook-page-hacked.

Menon, Naveen S. G. 2015. *The ASEAN Digital Revolution.* www.atkearney.com/documents/10192 /7567195/ASEAN+Digital+Revolution.pdf/86c51659-c7fb-4bc5-b6e1-22be3d801ad2.

Ministry of Communications and Information, Singapore. 2018. “Opening Remarks by Mr S Iswaran, Minister for Communications and Information.” The ASEANMinisterial Conference on Cybersecurity, 19 Sep 2018. www.mci.gov.sg/pressroom/news-and-stories/pressroom/ 2018/9/opening-remarks-by-mr-s-iswaran-at-the-asean-ministerial-conference-on-cybersecurity.

Ministry of Health, Singapore. 2018. “Singhealth’s IT System Target of Cyberattack.” www.moh.gov. sg/news-highlights/details/singhealth’s-it-system-target-of-cyberattack.

NIST (National Institute of Standards and Technology). 2018. *Framework for Improving Critical Infrastructure Cybersecurity.* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.041620 18.pdf.

Nguon Somaly. 2017. “Cambodia’s Effort on Cybersecurity Regulation: Policy and Human Rights Implications.” Master’s thesis*,* Tallinn University of Technology, Estonia.

Norton. 2013. *2013 Norton Report.* www.symantec.com/content/en/us/about/presskits/b-norton-report-2013-singapore.pdf.

Ponemon Institute. 2017. *2017 Cost of Data Breach Study.* Traverse City, MI: Ponemon Institute.

Ponemon Institute. 2019. *Cost of a Data Breach Report 2019*. www.all-about-security.de/fileadmin/ micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Report_final.pdf.

Republic of Singapore. 2018. *Cybersecurity Act 2018*.
Republic of the Philippines. 2012. *Cybercrime Prevention Act*.
RGC (Royal Government of Cambodia). 2010. *The Constitution of the Kingdom of Cambodia.* www.wipo.int/edocs/lexdocs/laws/en/kh/kh009en.pdf.
RGC. 2014a. *Cybercrime Law Draft V.1.* Unofficial Translation to English. www.article19.org/data/ files/medialibrary/37516/ Draft-Law-On-CyberCrime_Englishv1.pdf.
RGC. 2014b. "Draft Law on Cybercrime (Khmer)." https://data.opendevelopmentmekong.net/dataset/5 d691b53-3585-43db-8852-17d0b5834f1d/resource/ef0154d3-7998-494f-9817-dca2d14d2d03/ download /draftcybercrimelawkh.pdf.
Seangly Phak. 2013. "'Developed' by 2050: PM." *Phnom Penh Post*, 7 Jun 2013. www.phnompenhpost. com/national/%E2%80%98developed%E2%80%99-2050-pm.
Seiff, Abby. 2018. "Chinese State-Linked Hackers in Large Scale Operation to Monitor Cambodia's Upcoming Elections, Report Says". *TIME*, 11 Jul 2018. https://time.com/5334262/chinese-hackers-cambodia-elections-report/.
Sipalan, Joseph. 2018. "Malaysian Court Jails, Fines Artist for Clown Caricature of PM". *Reuters*, 20 Feb 2018. www.reuters.com/article/us-malaysia-politics/malaysian-court-jails-fines-artist-for-clown -caricature-of-pm-idUSKCN1G40K4.
Socialist Republic of Vietnam. 2018. *Law on Cybersecurity*.
The White House. 2013. "Improving Critical Infrastructure Cybersecurity." *Executive Order 13636*. Washington DC: Federal Register.
Trend Micro. 2016. "Data Protection Mishap Leaves 55M Philippine Voters at Risk". *Trend Micro*, 6 Apr 2016. https://blog.trendmicro.com/trendlabs-security-intelligence/55m-registered-voters-risk-philippine-commission-elections-hacked/
World Bank. 2019. *Cambodia Annual GDP Growth*. https://data.worldbank.org/indicator/NY.GDP.M KTP.KD.ZG?%20end=2018&locations=KH&most_recent_value_desc=true&start=1994&view=chart.
World Economic Forum. 2014. *Risk and Responsibility in a Hyperconnected World.* Insight Report. www3.weforum.org/docs/WEF_RiskResponsibility_HyperconnectedWorld_Report_2014.pdf.

Appendix: NIST Cybersecurity Framework

Function	Category
Identify	**Asset Management:** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
	Business Environment: The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
	Governance: The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
	Risk Assessment: The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
	Risk Management Strategy: The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
	Supply Chain Risk Management: The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.
Protect	**Identity Management, Authentication and Access Control:** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
	Awareness and Training: The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.
	Data Security: Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
	Information Protection Processes and Procedures: Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
	Maintenance: Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.
	Protective Technology: Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
Detect	**Anomalies and Events:** Anomalous activity is detected, and the potential impact of events is understood.
	Security Continuous Monitoring: The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
	Detection Processes: Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.

Respond	**Response Planning:** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.
	Communications: Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).
	Analysis: Analysis is conducted to ensure effective response and support recovery activities.
	Mitigation: Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.
	Improvements: Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
Recover	**Recovery Planning:** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.
	Improvements: Recovery planning and processes are improved by incorporating lessons learned into future activities.
	Communications: Restoration activities are coordinated with internal and external parties (e.g. coordinating centres, internet service providers, owners of attacking systems, victims, other computer security incident response teams, and vendors).

CDRI Working paper series

WP 120) Ros Vutha, Eam Phyrom, Heng Sambath and Ravy Sophearoth (December 2019) *Cambodian Academics: Identities and Roles.*

WP 119) Ven Seyhah and Hing Vutha (October 2019) *Cambodia in the Electronic and Electrical Global Value Chains.*

WP 118) Sothy Khieng, Sidney Mason and Seakleng Lim (October 2019) *Innovation and Entrepreneurship Ecosystem in Cambodia: The Roles of Academic Institutions.*

WP 117) Un Leang, Saphon Somolireasmey and Sok Serey (September 2019) *Gender Analysis of Survey on Cambodia's Young and Older Generation: Family, Community, Political Knowledge and Attitudes, and Future Expectations*

WP 116) Eng Netra, Ang Len, So Hengvotey, Hav Gechhong, Chhom Theavy (March 2019) *Cambodia's Young and Older Generation: Views on Generational Relations and Key Social and Political Issues*

WP 115) Mak Ngoy, Sok Say, Un Leang with Bunry Rinna, Chheng Sokunthy and Kao Sovansophal (May 2019) *Finance in Public Higher Education in Cambodia*

WP 114) Mak Ngoy, Sok Say, Un Leang with Bunry Rinna, Chheng Sokunthy and Kao Sovansophal (Apr 2019) *Governance in Public Higher Education in Cambodia*

WP 113) Ear Sothy, Sim Sokcheng, Chhim Chhun and Khiev Pirom (Dec 2017) *Rice Policy Study: Implications of Rice Policy Changes in Vietnam for Cambodia's Rice Policy and Rice Producers in South-Eastern Cambodia*

WP 112) Roth Vathana, Abdelkrim Araarz, Sry Bopharath and Phann Dalis (March 2017) *The Dynamics of Microcredit Borrowings in Cambodia*

WP 111) Ear Sothy, Sim Sokcheng and Khiev Pirom (March 2016) *Cambodia Macroeconomic Impacts of Public Consumption on Education – A Computable General Equilibrium Approach*

WP 110) Vong Mun (December 2016) *Progress and Challenges of Deconcentration in Cambodia: The Case of Urban Solid Waste Management*

WP 109) Sam Sreymom, Ky Channimol, Keum Kyungwoo, Sarom Molideth and Sok Raksa. (December 2016). *Common Pool Resources and Climate Change Adaptation: Community-based Natural Resource Management in Cambodia*

WP 108) Ly Tem (January 2016), *Leadership Pathways for Local Women: Case Studies of Three Communes in Cambodia*

WP 107) Chhim Chhun, Buth Bora and Ear Sothy (September 2015), *Effect of Labour Movement on Agricultural Mechanisation in Cambodia*

WP 106) Chhim Chhun, Tong Kimsun, Ge Yu, Timothy Ensor and Barbara McPake (September 2015), *Impact of Health Financing Policies on Household Spending: Evidence from Cambodia Socio-Economic Surveys 2004 and 2009*

WP 105) Roth Vathana and Lun Pide (August 2015), *Health and Education in the Greater Mekong Subregion: Policies, Institutions and Practices – the Case of Cambodia* in Khmer

WP 104) Sum Sreymom and Khiev Pirom (August 2015), *Contract Farming in Cambodia: Different Models, Policy and Practice*

WP 103) Chhim Chhun, Tong Kimsun, Ge Yu, Timothy Ensor and Barbara McPake (June 2015), *Catastrophic Payments and Poverty in Cambodia: Evidence from Cambodia Socio-Economic Surveys 2004, 2007, 2009, 2010 and 2011*

WP 102) Eng Netra, Vong Mun and Hort Navy (June 2015), *Social Accountability in Service Delivery in Cambodia*

WP 101) Ou Sivhouch (April 2015), *A Right-Based Approach to Development: A Cambodian Perspective*

WP 100) Sam Sreymom with Ouch Chhuong (March 2015), *Agricultural Technological Practices and Gaps for Climate Change Adaptation*

WP 99) Phay Sokcheng and Tong Kimsun (December 2014), *Public Spending on Education, Health and Infrastructure and Its Inclusiveness in Cambodia: Benefit Incidence Analysis*

WP 98) Srinivasa Madhur (August 2014), *Cambodia's Skill Gap: An Anatomy of Issues and Policy Options*

WP 97) Kim Sour, Dr Chem Phalla, So Sovannarith, Dr Kim Sean Somatra and Dr Pech Sokhem (August 2014), *Methods and Tools Applied for Climate Change Vulnerability and Adaptation Assessment in Cambodia's Tonle Sap Basin*

WP 96) Kim Sean Somatra and Hort Navy (August 2014), *Cambodian State: Developmental, Neoliberal? A Case Study of the Rubber Sector*

WP 95) Theng Vuthy, Keo Socheat, Nou Keosothea, Sum Sreymom and Khiev Pirom (August 2014), *Impact of Farmer Organisations on Food Security: The Case of Rural Cambodia*

WP 94) Heng Seiha, Vong Mun and Chheat Sreang with the assistance of Chhuon Nareth (July 2014), *The Enduring Gap: Decentralisation Reform and Youth Participation in Local Rural Governance*

WP 93) Nang Phirun, Sam Sreymom, Lonn Pichdara and Ouch Chhuong (June 2014), *Adaptation Capacity of Rural People in the Main Agro-Ecological Zones in Cambodia*

WP 92) Phann Dalis (June 2014), *Links between Employment and Poverty in Cambodia*

WP 91) Theng Vuthy, Khiev Pirom and Phon Dary (April 2014), *Development of the Fertiliser Industry in Cambodia: Structure of the Market, Challenges in the Demand and Supply Sidesand the Way Forward*

WP 90) CDRI Publication (January 2014), *ASEAN 2030: Growing Together for Economic Prosperity–the Challenges (Cambodia Background Paper)*

WP 89) Nang Phirun and Ouch Chhuong (January 2014), *Gender and Water Governance: Women's Role in Irrigation Management and Development in the Context of Climate Change*

WP 88) Chheat Sreang (December 2013), *Impact of Decentralisation on Cambodia's Urban Governance*

WP 87) Kim Sedara and Joakim Öjendal with the assistance of Chhoun Nareth (November 2013), *Gatekeepers in Local Politics: Political Parties in Cambodia and their Gender Policy*

WP 86) Sen Vicheth and Ros Soveacha with the assistance of Hieng Thiraphumry (October 2013), *Anatomy of Higher Education Governance in Cambodia*

WP 85) Ou Sivhuoch and Kim Sedara (August 2013), *20 Years' Strengthening of Cambodian Civil Society: Time for Reflection*

WP 84) Ou Sivhuoch (August 2013), *Sub-National Civil Society in Cambodia: A Gramscian Perspective*

WP 83) Tong Kimsun, Lun Pide and Sry Bopharath with the assistance of Pon Dorina (August 2013), *Levels and Sources of Household Income in Rural Cambodia 2012*

WP 82) Nang Phirun (July 2013), *Climate Change Adaptation and Livelihoods in Inclusive Growth: A Review of Climate Change Impacts and Adaptive Capacity in Cambodia*

WP 81) Hing Vutha (June 2013), *Leveraging Trade for Economic Growth in Cambodia*

WP 80) Saing Chan Hang (March 2013), *Binding Constraints on Economic Growth in Cambodia: A Growth Diagnostic Approach*

WP 79) Lun Pidé (March 2013), *The Role of Rural Credit during the Global Financial Crisis: Evidence From Nine Villages in Cambodia*

WP 78) Tong Kimsun and Phay Sokcheng (March 2013), *The Role of Income Diversification during the Global Financial Crisis: Evidence from Nine Villages in Cambodia*
WP 77) Saing Chan Hang (March 2013), *Household Vulnerability to Global Financial Crisis and Their Risk Coping Strategies: Evidence from Nine Rural Villages in Cambodia*
WP 76) Hing Vutha (March 2013), *Impact of the Global Financial Crisis on the Rural Labour Market: Evidence from Nine Villages in Cambodia*
WP 75) Tong Kimsun (March 2013), *Impact of the Global Financial Crisis on Poverty: Evidence from Nine Villages in Cambodia*
WP 74) Ngin Chanrith (March 2013), *Impact of the Global Financial Crisis on Employment in SMEs in Cambodia*
WP 73) Hay Sovuthea (March 2013), *Government Response to Inflation Crisis and Global Financial Crisis*
WP 72) Hem Socheth (March 2013), *Impact of the Global Financial Crisis on Cambodian Economy at Macro and Sectoral Levels*
WP 71) Kim Sedara and Joakim Öjendal with Chhoun Nareth and Ly Tem (December 2012), *A Gendered Analysis of Decentralisation Reform in Cambodia*
WP 70) Hing Vutha, Saing Chan Hang and Khieng Sothy (August 2012), *Baseline Survey for Socioeconomic Impact Assessment: Greater Mekong Sub-region Transmission Project*
WP 69) CDRI Publication (March 2012), *Understanding Poverty Dynamics: Evidence from Nine Villages in Cambodia*
WP 68) Roth Vathana (March 2012), *Sectoral Composition of China's Economic Growth, Poverty Reduction and Inequality: Development and Policy Implications for Cambodia*
WP 67) Keith Carpenter with assistance from PON Dorina (February 2012), *A Basic Consumer Price Index for Cambodia 1993–2009*
WP 66) TONG Kimsun (February 2012), *Analysing Chronic Poverty in Rural Cambodia Evidence from Panel Data*
WP 65) Ros Bansok, Nang Phirun and Chhim Chhun (December 2011), *Agricultural Development and Climate Change: The Case of Cambodia*
WP 64) Tong Kimsun, Sry Bopharath (November 2011), *Poverty and Evironment Links: The Case of Rural Cambodia*
WP 63) Heng Seiha, Kim Sedara and So Sokbunthoeun (October 2011), *Decentralised Governance in Hybrid Polity: Localisation of Decentralisation Reform in Cambodia*
WP 62) Chea Chou, Nang Phirun, Isabelle Whitehead, Phillip Hirsch and Anna Thompson (October 2011), *Decentralised Governance of Irrigation Water in Cambodia: Matching Principles to Local Realities*
WP 61) Ros Bandeth, Ly Tem and Anna Thompson (September 2011), *Catchment Governance and Cooperation Dilemmas: A Case Study from Cambodia*
WP 60) Saing Chan Hang, Hem Socheth and Ouch Chandarany with Phann Dalish and Pon Dorina (November 2011), *Foreign Investment in Agriculture in Cambodia*
WP 59) Chem Phalla, Philip Hirsch and Someth Paradis (September 2011), *Hydrological Analysis in Support of Irrigation Management: A Case Study of Stung Chrey Bak Catchment, Cambodia*
WP 58) Hing Vutha, Lun Pide and Phann Dalis (August 2011), *Irregular Migration from Cambodia: Characteristics, Challenges and Regulatory Approach*
WP 57) Tong Kimsun, Hem Socheth and Paulos Santos (August 2011), *The Impact of Irrigation on Household Assets*

WP 56) Tong Kimsun, Hem Socheth and Paulos Santos (July 2011), *What Limits Agricultural Intensification in Cambodia? The role of emigration, agricultural extension services and credit constraints*

WP 55) Kem Sothorn, Chhim Chhun, Theng Vuthy and So Sovannarith (July 2011), *Policy Coherence in Agricultural and Rural Development: Cambodia*

WP 54) Nang Phirun, Khiev Daravy, Philip Hirsch and Isabelle Whitehead (June), *Improving the Governance of Water Resources in Cambodia: A Stakeholder Analysis*

WP 53) Chann Sopheak, Nathan Wales and Tim Frewer (August 2011), *An Investigation of Land Cover and Land Use Change in Stung Chrey Bak Catchment, Cambodia*

WP 52) Ouch Chandarany, Saing Chanhang and Phann Dalis (June 2011), *Assessing China's Impact on Poverty Reduction In the Greater Mekong Sub-region: The Case of Cambodia*

WP 51) Christopher Wokker, Paulo Santos, Ros Bansok and Kate Griffiths (June 2011), *Irrigation Water Productivity in Cambodian Rice System*

WP 50) Pak Kimchoeun (May 2011), *Fiscal Decentralisation in Cambodia: A Review of Progress and Challenges*

WP 49) Chem Phalla and Someth Paradis (March 2011), *Use of Hydrological Knowledge and Community Participation for Improving Decision-making on Irrigation Water Allocation*

WP 48) CDRI Publication (August 2010), *Empirical Evidence of Irrigation Management in the Tonle Sap Basin: Issues and Challenges*

WP 47) Chea Chou (August 2010), *The Local Governance of Common Pool Resources: The Case of Irrigation Water in Cambodia*

WP 46) CDRI Publication (December 2009), *Agricultural Trade in the Greater Mekong Sub-region: Synthesis of the Case Studies on Cassava and Rubber Production and Trade in GMS Countries*

WP 45) CDRI Publication (December 2009), *Costs and Benefits of Cross-country Labour Migration in the GMS: Synthesis of the Case Studies in Thailand, Cambodia, Laos and Vietnam*

WP 44) Chan Sophal (December 2009), *Costs and Benefits of Cross-border Labour Migration in the GMS: Cambodia Country Study*

WP 43) Hing Vutha and Thun Vathana (December 2009), *Agricultural Trade in the Greater Mekong Sub-region: The Case of Cassava and Rubber in Cambodia*

WP 42) Thon Vimealea, Ou Sivhuoch, Eng Netra and Ly Tem (October 2009), *Leadership in Local Politics of Cambodia: A Study of Leaders in Three Communes of Three Provinces*

WP 41) Hing Vutha and Hossein Jalilian (April 2009), *The Environmental Impacts of the ASEAN-China Free Trade Agreement for Countries in the Greater Mekong Sub-region*

WP 40) Eng Netra and David Craig (March 2009), *Accountability and Human Resource Management in Decentralised Cambodia*

WP 39) Horng Vuthy and David Craig (July 2008), *Accountability and Planning in Decentralised Cambodia*

WP 38) Pak Kimchoeun and David Craig (July 2008), *Accountability and Public Expenditure Management in Decentralised Cambodia*

WP 37) Chem Phalla *et al.* (May 2008), *Framing Research on Water Resources Management and Governance in Cambodia: A Literature Review*

WP 36) Lim Sovannara (November 2007), *Youth Migration and Urbanisation in Cambodia*

WP 35) Kim Sedara and Joakim Öjendal with the assistance of Ann Sovatha (May 2007), *Where Decentralisation Meets Democracy: Civil Society, Local Government, and Accountability in Cambodia*

WP 34) Pak Kimchoeun, Horng Vuthy, Eng Netra, Ann Sovatha, Kim Sedara, Jenny Knowles and David Craig (March 2007), *Accountability and Neo-patrimonialism in Cambodia: A Critical Literature Review*

WP 33) Hansen, Kasper K. and Neth Top (December 2006), *Natural Forest Benefits and Economic Analysis of Natural Forest Conversion in Cambodia*

WP 32) Murshid, K.A.S. and Tuot Sokphally (April 2005), *The Cross Border Economy of Cambodia: An Exploratory Study*

WP 31) Oberndorf, Robert B. (May 2004), *Law Harmonisation in Relation to the Decentralisation Process in Cambodia*

WP 30) Hughes, Caroline and Kim Sedara with the assistance of Ann Sovatha (February 2004), *The Evolution of Democratic Process and Conflict Management in Cambodia: A Comparative Study of Three Cambodian Elections*

WP 29) Yim Chea and Bruce McKenney (November 2003), *Domestic Fish Trade: A Case Study of Fish Marketing from the Great Lake to Phnom Penh*

WP 28) Prom Tola and Bruce McKenney (November 2003), *Trading Forest Products in Cambodia: Challenges, Threats, and Opportunities for Resin*

WP 27) Yim Chea and Bruce McKenney (October 2003), *Fish Exports from the Great Lake to Thailand: An Analysis of Trade Constraints, Governance, and the Climate for Growth*

WP 26) Sarthi Acharya, Kim Sedara, Chap Sotharith and Meach Yady (February 2003), *Off-farm and Non-farm Employment: A Perspective on Job Creation in Cambodia*

WP 25) Chan Sophal and Sarthi Acharya (December 2002), *Facing the Challenge of Rural Livelihoods: A Perspective from Nine Villages in Cambodia*

WP 24) Kim Sedara, Chan Sophal and Sarthi Acharya (July 2002), *Land, Rural Livelihoods and Food Security in Cambodia*

WP 23) McKenney, Bruce, Prom Tola. (July 2002), *Natural Resources and Rural Livelihoods in Cambodia*

WP 22) Chan Sophal and Sarthi Acharya (July 2002), *Land Transactions in Cambodia: An Analysis of Transfers and Transaction Records*

WP 21) Bhargavi Ramamurthy, Sik Boreak, Per Ronnås and Sok Hach (December 2001), *Cambodia 1999-2000: Land, Labour and Rural Livelihood in Focus*

WP 20) So Sovannarith, Real Sopheap, Uch Utey, Sy Rathmony, Brett Ballard and Sarthi Acharya (November 2001), *Social Assessment of Land in Cambodia: A Field Study*

WP 19) Chan Sophal, Tep Saravy and Sarthi Acharya (October 2001), *Land Tenure in Cambodia: a Data Update*

WP 18) Godfrey, Martin, So Sovannarith, Tep Saravy, Pon Dorina, Claude Katz, Sarthi Acharya, Sisowath D. Chanto and Hing Thoraxy (August 2001), *A Study of the Cambodian Labour Market: Reference to Poverty Reduction, Growth and Adjustment to Crisis*

WP 17) Chan Sophal and So Sovannarith with Pon Dorina (December 2000), *Technical Assistance and Capacity Development at the School of Agriculture Prek Leap*

WP 16) Sik Boreak (September 2000), *Land Ownership, Sales and Concentration in Cambodia*

WP 15) Godfrey, Martin, Chan Sophal, Toshiyasu Kato, Long Vou Piseth, Pon Dorina, Tep Saravy, Tia Savara and So Sovannarith (August 2000), *Technical Assistance and Capacity Development in an Aid-dependent Economy: The Experience of Cambodia*

WP 14) Toshiyasu Kato, Jeffrey A. Kaplan, Chan Sophal and Real Sopheap (May 2000), *Enhancing Governance for Sustainable Development*

WP 13) Ung Bunleng (January 2000), *Seasonality in the Cambodian Consumer Price Index*

WP 12) Chan Sophal, Toshiyasu Kato, Long Vou Piseth, So Sovannarith, Tia Savora, Hang Chuon Naron, Kao Kim Hourn and Chea Vuthna (September 1999), *Impact of the Asian Financial Crisis on the SEATEs: The Cambodian Perspective*

WP 11) Chan Sophal and So Sovannarith (June 1999), *Cambodian Labour Migration to Thailand: A Preliminary Assessment*

WP 10) Gorman, Siobhan, with Pon Dorina and Sok Kheng (June 1999), *Gender and Development in Cambodia: An Overview*

WP 9) Teng You Ky, Pon Dorina, So Sovannarith and John McAndrew (April 1999), *The UNICEF/Community Action for Social Development Experience—Learning from Rural Development Programmes in Cambodia*

WP 8) Chan Sophal, Martin Godfrey, Toshiyasu Kato, Long Vou Piseth, Nina Orlova, Per Ronnås and Tia Savora (January 1999), *Cambodia: The Challenge of Productive Employment Creation*

WP 7) McAndrew, John P. (December 1998), *Interdependence in Household Livelihood Strategies in Two Cambodian Villages*

WP 6) Murshid, K.A.S. (December 1998), *Food Security in an Asian Transitional Economy: The Cambodian Experience*

WP 5) Kato, Toshiyasu, Chan Sophal and Long Vou Piseth (September 1998), *Regional Economic Integration for Sustainable Development in Cambodia*

WP 4) Chim Charya, Srun Pithou, So Sovannarith, John McAndrew, Nguon Sokunthea, Pon Dorina and Robin Biddulph (June 1998), *Learning from Rural Development Programmes in Cambodia*

WP 3) Kannan, K.P. (January 1997), *Economic Reform, Structural Adjustment and Development in Cambodia*

WP 2) McAndrew, John P. (January 1996), *Aid Infusions, Aid Illusions: Bilateral and Multilateral Emergency and Development Assistance in Cambodia.* 1992-1995

WP 1) Kannan, K.P. (November 1995), *Construction of a Consumer Price Index for Cambodia: A Review of Current Practices and Suggestions for Improvement*

Cambodia Development Resource Institute

☞ 56 Street 315, Tuol Kork

✉ PO Box 622, Phnom Penh, Cambodia

☎ +855 23 881 384/881 701/881 916/883 603

@ cdri@cdri.org.kh

🌐 www.cdri.org.kh

Price: USD3.00

9 789924 500186