ISSN 1560-7607 / ISBN 978-99950-52-05-8

CAMBODIA DEVELOPMENT REVIEW

A publication of CDRI—Cambodia's leading independent development policy research institute

VOLUME 23, 2019 $4.00

30th ANNIVERSARY CDRI 1990 - 2020

CYBERGOVERNANCE IN CAMBODIA: CURRENT STATE AND FUTURE PRIORITIES

Introduction

This article discusses cybersecurity issues, cybercrime and cyber governance in Cambodia, by reviewing current policy and governance systems in place in Cambodia and other ASEAN countries and assessing the strategies and plans of ministries, research centres and big international companies.

Individuals, government agencies and organisations are increasingly dependent on complex technology ecosystems to communicate and interact with their peers, business partners and customers, share and access information, provide data for improved decision making and performance, and increase reach and profitability. Digital technology platforms have proved even more essential during the present COVID-19 outbreak. At the same time, cyberattacks are occurring with greater frequency and severity. Individuals, politicians, board members and executives are increasingly aware that technology-based innovations and initiatives open doors to cyber risks and pose ever greater governance challenges.

Cyber governance and cybersecurity are relatively new topics, at least in Cambodia. This study aims to raise awareness and spark meaningful dialogue by making research findings available to policymakers, government officials and business leaders for strategising, developing and improving their cybersecurity framework (i.e. governance, technology, capacity and cooperation). It is expected that researchers and practitioners will expand on these findings and keep up with emerging technologies and the rapid pace of technological change in Cambodia.

Cambodia is working hard to strengthen its cybersecurity governance to minimise the potential risks from an increasingly interconnected world, October 2019

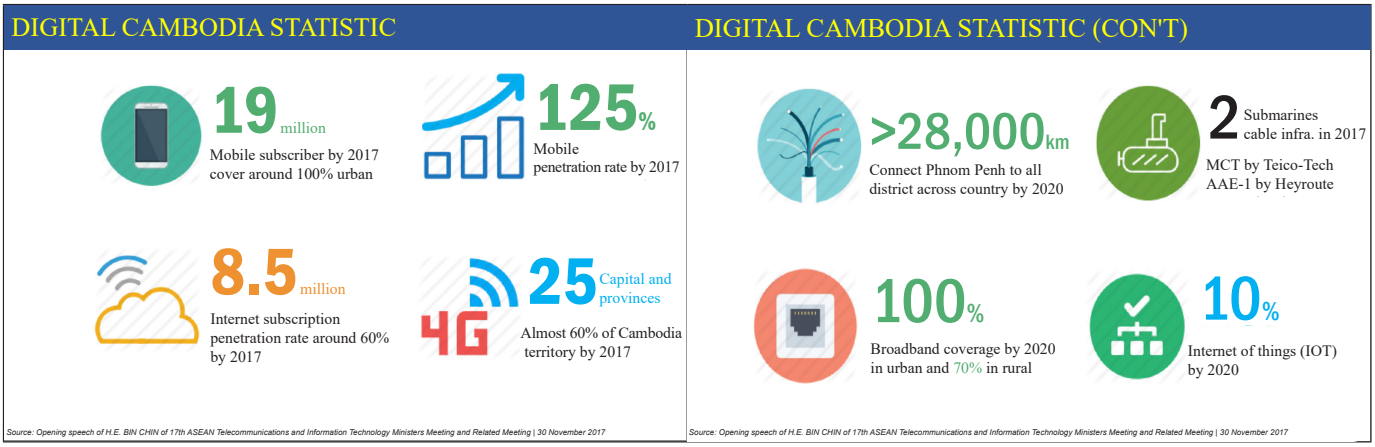
Cybersecurity in Cambodia and globally

The Cambodian economy grew 7.5 percent in 2018 (World Bank 2019), making it the

In this Issue

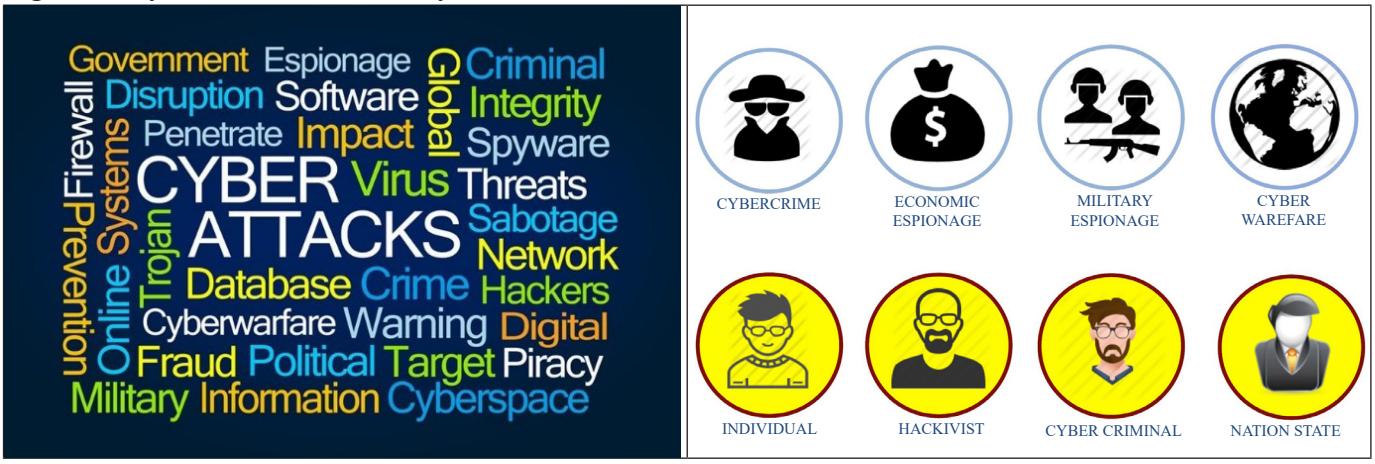
Citation: A CDRI Publication. 2019. "Cybergovernance in Cambodia: Current State and Future Priorities." *Cambodia Development Review* vol. 23, 2019: 1–6.

Figure 1: Digital statistics in Cambodia



Source: Ou 2018 (with the author's permission)

Figure 2: Cyberattack vulnerability



Sources: Ou 2018 (with the author's permission)

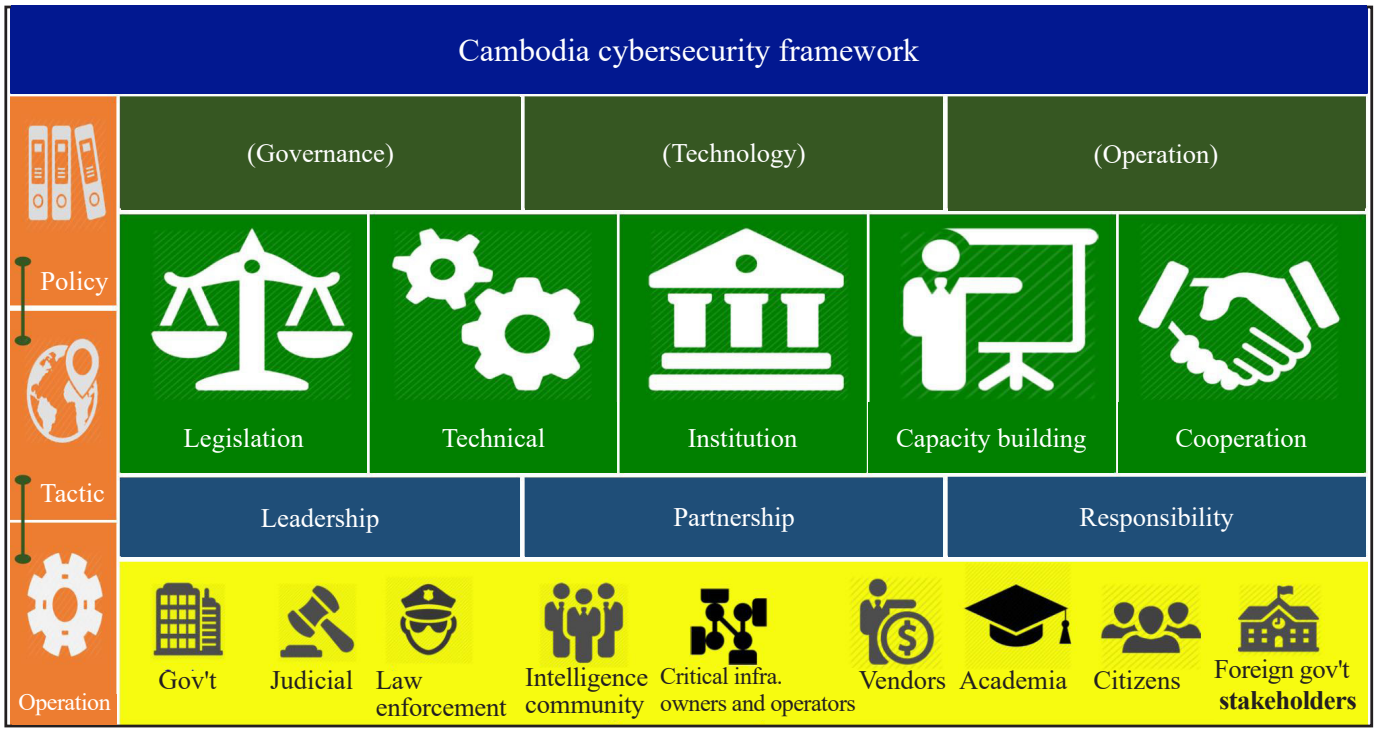
fastest growing economy in the ASEAN region and one of the fastest growing economies in the world. Alongside impressive economic growth, government institutions, companies and organisations in Cambodia are rapidly expanding their use of technology, as shown in Figure 1. This increased digitalisation has been largely driven by the large young population – the nation's median age is currently 25.6 years.

From 2017 to 2019, the number of social media users increased by 71 percent from 4.9 million to 8.4 million, almost half of Cambodia's current population (Kepios Analysis 2019). Although these statistics are promising for Cambodia as a whole, such rapid technological advancement could make the country more susceptible to cyberattack unless the cybersecurity framework is improved. Cybercriminals are using more advanced and scalable tools to breach user privacy, and they are getting results.

Cybercriminals (individuals, hacktivists and/or state sponsored cybercriminals) target the weakest link, and it is common for large companies to fall prey to cyberattack through third-party partners, suppliers and vendors in their supply chain.

The need for a cybersecurity governance framework is being increasingly recognised as a key aspect of reducing cyber risk. Cyber security, including its governance, was rated the sixth of 10 global priorities for 2019, ahead of combating transnational terrorism and promoting global health, and is among the world's most pressing policy challenges (Council of Councils 2019).

Figure 3: Cambodia's cybersecurity framework



Source: Ou 2018 (with the author's permission)

Cambodia's cybersecurity framework

At least in theory, Cambodia's cybersecurity framework consists of governance (legislation, technical capacity, and leadership), technology (technical and institutional capacity) and operation (capacity building, cooperation and partnership), as well as many key actors, such as government agencies and departments, the judiciary, law enforcement agencies, the intelligence community, critical infrastructure owners and operators, vendors, academia, the citizenry, and foreign stakeholders.

As far as cyber governance is concerned, at the time of writing, a new version of Cambodia's 2014 Cybercrime Draft Law was being discussed within the Ministry of Interior. Many amendments are expected to be made to the original draft. Because the latest draft law is not yet available to the public, the following analysis draws on the unofficial 2014 draft document (Khmer and English).

The objectives of the 2014 Draft Cybercrime Law were to combat offences committed by computer systems (any device or suites of interconnected devices) and to ensure the safety of and protect all legitimate rights and interests of legal and natural persons, and of Cambodia. The National Anti-Cybercrime Committee (NACC) was to be established, chaired by the prime minister, to devise strategies, action plans and related measures in cybersecurity and information systems for the government. The law was also to grant "judicial policy" power to the secretary general and deputy secretary-general of the NACC Secretariat to arrest and investigate action against suspects (Article 15).

Overall, the content of the draft law addresses standard cybercrime concerns such as illegal access, data espionage and intellectual property theft, and defines penalties for each offence. But there are issues, specifically concerning Article 28, that may restrict the right to freedom of expression. Paragraph 4 of Article 28, for instance, states that nonfactual 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 "nonfactual."

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.

Key findings and recommendations

Four key gaps emerge from the analysis of Cambodia's cyber governance efforts and underlying motivations:

- government transparency
- human and technical resources
- regional collaboration
- tangible quantitative goals.

Recommendation 1: Cambodia is in the initial stages of establishing its own cybersecurity framework by addressing the above four main gaps, especially in transparency and due protection of human rights and national interests, developing a highly skilled workforce for a digital future, and forging strategic partnerships with other countries and international corporations. Although the fundamental obstacles of being a developing country will remain for some time, the use of international best practices including standards and frameworks can help Cambodia put well-functional and effective systems in place to protect its critical ICT facilities and users from cyberattacks.

Cambodia has set ambitious goals in its vision to become a fully developed country by 2050 (Seangly 2013), including investing heavily in building digital infrastructure, developing smart cities and embracing Industry 4.0 in manufacturing (ASEAN 2018). A large-scale cyberattack on these technologies before they are fully implemented and secured could severely hinder their efficacy and expansion, and therefore have direct negative consequences for Cambodia's economic growth.

Recommendation 2: Protecting critical infrastructure, such as public health, transport, telecommunications and utility systems, is the government's main responsibility and should be addressed by a unified front including the public, private and academic sectors.

Recommendation 3: Cybersecurity law and regulation must be enacted. A good example of diligently planned cybersecurity law is Singapore's Cybersecurity Act 2018. The Act stipulates in fine detail exactly what is expected of organisations involved with critical infrastructure in Singapore, and defines clearly what the government can and cannot do in the protection of national security. Rather than stating vague offences and an unclear balance of power, Singapore's Cybersecurity Act focuses on ensuring cooperation and transparency between the private and public sectors.

Cambodia's cybersecurity law should focus on preventing and responding to technical cyberattacks targeting infrastructure, government and businesses given that the potential impacts of cybersecurity attacks on Cambodia's economy and critical infrastructure are far greater than on the offences and criminalisation of publications currently targeted in the 2014 Draft Cybercrime Law.

Recommendation 4: Building a systemic cybersecurity and governance program, as cybersecurity framework is complex, touches every industry and way of life, involves all levels of government, and can have a direct financial impact on the economy and society. The government should consider the following in building its cyber governance program: a national strategy to protect critical infrastructure, public-private sector collaboration, cybersecurity regulation, adoption of cybersecurity standards, regional information sharing, community awareness, and capacity building. Each of these activities represents a project that should be continuously monitored for progress and achievement of specific metrics by the NACC (a central cyber governance authority), comprising government, key businesses and other nongovernment stakeholders, whose sole responsibility is the resilience of Cambodia's digital systems.

There are many recognised cybersecurity standards and frameworks on which to build a cyber-governance program. The National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (NIST 2018) was developed in the United States

in response to rapid technological advancement and increasing cybersecurity threats. It is rapidly growing in popularity because of its risk-based approach and use of clear and comprehensible language. Cambodia should be inspired by it in its efforts 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.

Recommendation 5: Building a cyber-governance program using a model such as the NIST Cybersecurity Framework would help provide a common language to communicate cyber risk across the different levels of government and industry sectors overseeing Cambodia's critical digital infrastructure. Moreover, current cybersecurity policies, training and solutions should define future goals, prioritise innovation, and track and communicate progress to stakeholders. This could be accomplished by breaking down cybersecurity and governance into related core areas for development:

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

Recommendation 6: International best practices should be adapted and used to systematically assess and monitor the current level of cybersecurity resilience so that gaps in preventative and mitigating measures can be identified. Once these gaps are found, they should be prioritised based on the degree of risk posed to Cambodia's digital infrastructure systems, including an analysis of the threats and likelihood of cyberattack. Once plausible risks/threats have been identified, solutions can be proposed to senior leaders for sponsorship and funding.

Recommendation 7: Cybersecurity is a topic that everyone must understand, and the ICT community and specialists should help simplify information and use less jargon and technical language which can be a barrier to clear communication and awareness raising.

Recommendation 8: Aligning specific, agreed-upon metrics between stakeholders to achieve cyber resilience goals from the outset can build greater confidence and support for those involved. It is the responsibility of the designated cyber governance body to ensure stakeholders take a proactive approach to meeting their targets and can adhere to compliance requirements and cybersecurity regulation to achieve their objectives.

Recommendation 9: Cybersecurity expertise can be developed through cooperation and exchange. ASEAN has made significant progress in developing regional cyber governance initiatives that Cambodia can tap into. Specifically, Cambodia should consider strong involvement with 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 (JAIF 2018). These skills fit directly with the NIST Cybersecurity Framework's technical needs and will develop Cambodian cybersecurity professionals with specialised skillsets. Cambodia can also use this training program as a model to create its own cybersecurity courses in universities and professional education and training programs.

Recommendation 10: Cybersecurity certification can be developed for individuals and businesses that already have cybersecurity expertise and comply with industry standards set either by government or a regional private standards body. Many industries use self-regulation because standards bodies can adapt to emerging technologies quicker and protect consumers better than if they were to rely solely on government processes. 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. Plus, 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.

Conclusion

The numbers of connected users and devices in Cambodia are rapidly increasing, and the repercussions of inaction to build a national cybersecurity and governance framework is an unacceptable risk to Cambodia's citizens and economy. Efforts must start from the top, with the active involvement of all key agencies, businesses and citizenry for better coordinated and sustainable outcomes. To recognise cyberattack risks to critical infrastructure, the government should consider putting its officials and concerned business owners through cybersecurity awareness training to create a baseline understanding of threats in their respective fields before enacting cybersecurity or cybercrime regulation.

Once the government has set clear objectives of what it wants to achieve, government officials should organise a diverse committee of public and private institutions to develop cybersecurity regulation that focuses on protecting Cambodia's critical infrastructure while also acknowledging citizens' online privacy as a human right. These policies should also encourage Cambodian businesses to look to the government for resources to strengthen their cybersecurity programs. Cambodia has already set up a computer emergency response team, and the team should be provided the necessary human resources, funding and technical training to be the central contact for the government and private businesses to turn to for up-to-date information and briefings on cybersecurity threats and vulnerabilities.

Lastly, the government should consider conducting a NIST Cybersecurity Framework assessment, starting with the sectors that have the largest impact, such as e-commerce and e-government. Citizens and businesses are quickly relying on these services for online banking, business-to-business transactions, utility payments, and so on. A phased cybersecurity assessment would allow for more accurate target completion dates and further collaboration between ministries.

References

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

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.

NIST (National Institute of Standards and Technology). 2018. Framework for Improving Critical Infrastructure Cybersecurity. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Ou Phannarith. 2018. "Cybercrime and Legislation in Cambodia." Paper presented at the AFIN and Cybersecurity Workshop, Phnom Penh, Cambodia, 3 April 2018.

Republic of Singapore. 2018. Cybersecurity Act 2018.

RGC. 2014. Unofficial Draft of Cybercrime Law. https://www.ccimcambodia.org/wp-content/uploads/2014/10/draft_cybercrime_law_en.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.

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.