ISSUE: 2022, No. 01

# AVI PERSPECTIVE

**Cambodia | 15 Februaty 2022**

## Cybersecurity Legislation in Cambodia: Policy to Improve Cyber Readiness and Resilience

*SANG Sinawong,[a] PhD*
*KONG Phallack, [b] LLM, LLB, & DDS*
*OU Phannarith, [c] MBA*
*CHHEM Siriwat, [d] MDTM*

## Executive Summary

- Advancements in digital technology applications, coupled with high digital adoption rates, have resulted in increased interconnectivity and more efficient communication – ultimately boosting the economy and benefitting the society in Cambodia. However, increased digital adoption and interconnectivity correspondingly lead to more potential cybersecurity risks.
- Cambodia may learn from cybersecurity resolutions of international organisations and cybersecurity laws of established nations in ASEAN, Asia, and beyond to reinforce national cybersecurity legislation as a policy instrument to improve cybersecurity readiness and resilience for the government, companies, organisations, and individuals.
- The key factor for cybersecurity legislation in Cambodia should be to establish a compliance regime to raise the safety and security bar, to strengthen and improve the cybersecurity resilience of Critical Information Infrastructure (CII) sectors – which are related to national security, the economy, and society. These essential services provided by governments and firms, used by citizens, all rely on the communication and storage of essential or confidential information. As such, CIIs must be protected in order to maintain the effective operation of a nation.

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

# សេចក្តីសន្និដ្ឋានអត្ថបទ

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

## Introduction

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

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

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

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

There are relevant laws and regulations with provisions related to cybersecurity issues such as the Criminal Code, Law on Telecommunications, E-Commerce Law, Consumer Protection Law and Sub-decree on 'Digital Signature'. However, no cybersecurity law exists in Cambodia yet. As such, on 8th June 2020, the Ministry of Post and Telecommunications (MPTC) established a working group to draft the Law on Cybersecurity in Cambodia. This working

group was tasked to draft the Law on Cybersecurity, research relevant cybersecurity laws in the region and beyond, and cooperate with relevant ministries and stakeholders to ensure that the draft law is aligned with national and international legal standards. Prior to developing the draft law, the working group prepared the following concept note to create a common understanding of the concepts of cybersecurity, which will act as the foundation for drafting the Law on Cybersecurity in Cambodia.

## Concepts of Cybersecurity

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

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

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

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

**Table 1: Cybersecurity vs Cybercrime**

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

*(Source: CDRI (2020))*

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

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

## Development of Legal Framework on Cybersecurity

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

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

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

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

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

Law. Cambodia will be the third country in ASEAN to have both a Cybercrime Law and Cybersecurity Law.

## Review of Cybersecurity Laws in Selected Countries

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

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

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

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

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

In Estonia, the Cybersecurity Act was promulgated on 23rd May 2019 to provide requirements for the maintenance of state and local authorities' network and information systems essential for the functioning of the society, liability and supervision, as well as the prevention and resolution of cyber incidents. Furthermore, the law explores single points of contact and competent authorities, principles of ensuring cybersecurity, cyber incident registry, the exercise of state and administrative supervision, violations of requirements of Act, proceedings, identification of service providers, provisions governing the amendment of other Acts, and entry into force of Act. The Cybersecurity Act of Estonia provides General Provisions; Obligations for Ensuring Cybersecurity; Ensuring Cybersecurity; State and Administrative Supervision; Liability; and Implementing Provisions (Riigi Teataja 2018).

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

## Policy Recommendations for Cambodia's Cybersecurity Legislation

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

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

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

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

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

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

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

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

## Conclusion

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

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

## References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

National Assembly of Vietnam. 2018. "Law on Cybersecurity." Hanoi: National Assembly of Vietnam.

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

Republic of Singapore. 2018. *"CYBERSECURITY ACT 2018."* Singapore.

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

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

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

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

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

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

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