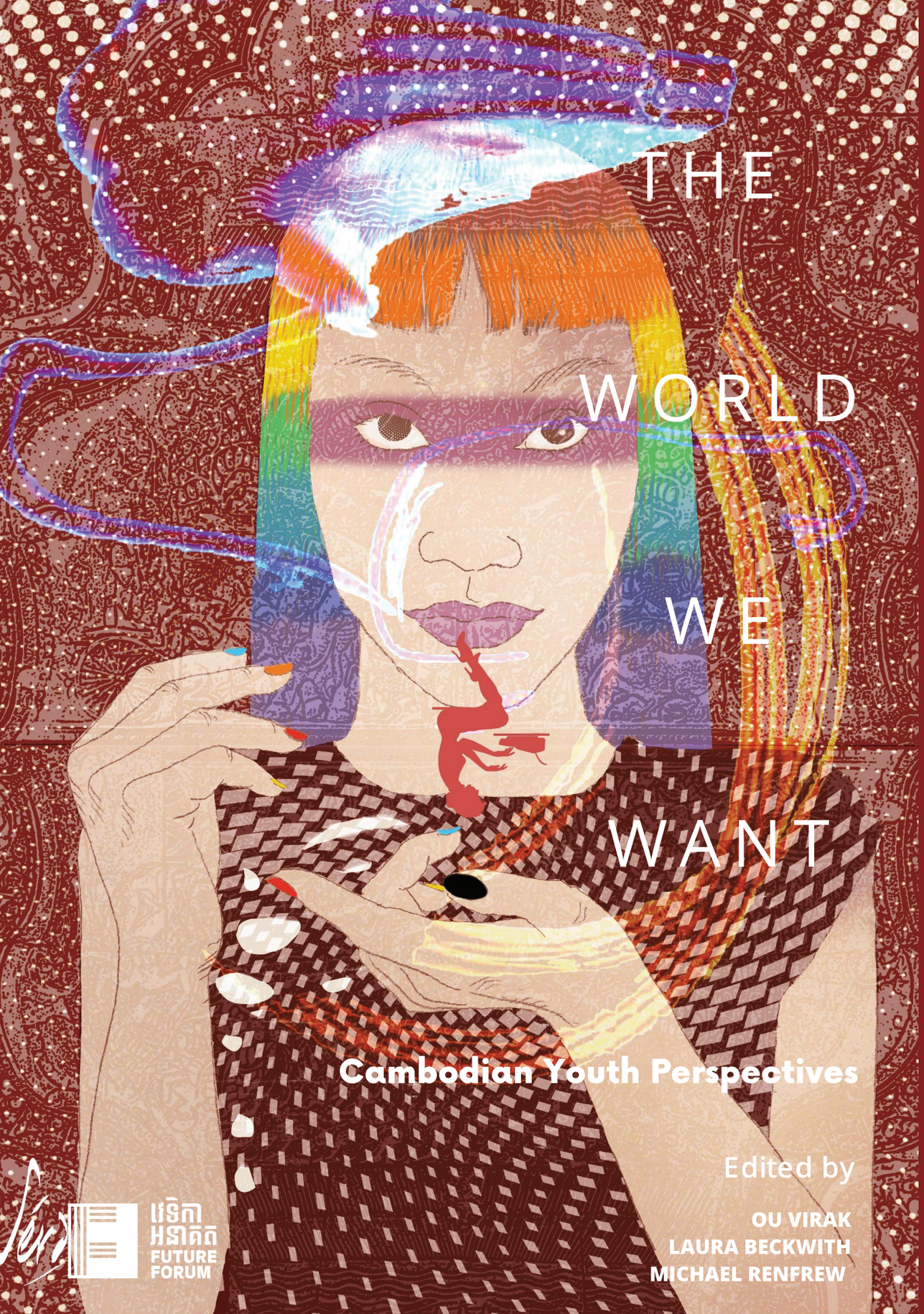

THE WORLD WE WANT

Cambodian Youth Perspectives

Edited by

OU VIRAK
LAURA BECKWITH
MICHAEL RENFREW

FUTURE FORUM

Core Donor

Sverige

In Partnership With

UNITED NATIONS CAMBODIA

secdev.foundation

វេទិកាអនាគត
FUTURE FORUM

The World We Want

Edited by

OU VIRAK
LAURA BECKWITH
MICHAEL RENFREW

Chapter 7 | The Role of the Government in Promoting the Cyber Security Infrastructure

Dechkunn CHHAY

Future Scenario

On a fine Monday morning, July 24, 2039, Soriya was walking towards her office. Suddenly, her phone rang. A notification pops up on her screen. She checks and sees an email from the Ministry of Health. According to the email, the Ministry was writing to inform her that her personal account for her health insurance is outdated and she needs to click on the link provided in the email to review her account. “Something is fishy,” she thought. Having been regularly informed by the Cambodian National Cybersecurity Agency (CNCA) on social media of potential hackers and cyber-attacks, Soriya is well-equipped to handle this kind of situation. She immediately contacts the CNCA to inquire about the email. The official responds in a timely manner and successfully identifies that the email was not sent from the Ministry. “Whew!” she exclaimed. For Soriya, it was not a problem if she were to mistakenly click on that link. If the hacker were to try to use her login information, it would prompt a message to the e-Ministry of Health application on her phone to alert her to any suspicious attempts to use her information on another device. Thus, it will allow her to successfully update her login information and secure all of her data.

Cambodia in the late 2030s is applauded as one of the states in Southeast Asia with the most robust cyber security apparatus. However, this was not always the case. The Royal Government of Cambodia (RGC) prioritized its efforts to strengthen the security of Cambodia's cyberspace as the country digitized its economy. Following the COVID-19 pandemic in the 2020s, government institutions turned to the internet, social media, and other technological platforms in order to deliver their services to the public. In the post pandemic period, many governmental institutions of the RGC realized that they should continue to harness the benefits of technology and the internet. As a result, those institutions continue to further develop the existing platforms established during the COVID-19 pandemic, making their services more efficient and attractive for the Cambodian public. However, in its haste to move the services online, the RGC neglected to ensure the security layer of those platforms was sufficient and many users, as well as their own platforms, were victims of hacking, phishing, and other types of cyberattacks.

During this period, the Cambodian National Cyberspace Agency (CNCA) was established with the main objective of protecting the cyberspace of Cambodia. The CNCA also has a variety of

operations and missions ranging from conducting capacity-training programs for Cambodian cyber security and network security professionals, holding campaigns for raising cyber awareness among Cambodian citizens, as well as publishing real-time incidents and weekly reports on cyber-attacks for research purposes. Once the RGC recognized that its digital infrastructure had become one of its most vulnerable critical infrastructures, it realized this was an issue which needed a lot of attention and protection. This specialized unit is composed of many professionals hailing from backgrounds such as law and network security. The institution has collaborated with many local and international cyber security communities, university, private-sector organizations and enterprises, and foreign cyber security specialized agencies and units in order to develop a strong national cyber security protection program as well as a resilient response and recovery plan. Cambodia has been regionally and internationally recognized as one of the most active players in promoting government participation in developing a strong cyber security layer for the country's and the region's cyberspace.

Introduction

The need to develop a strong cyber security system to protect the country's digital infrastructure comes with the adoption of Industry 4.0 technologies. The Royal Government of Cambodia (RGC) is eager to adopt the new and innovative technologies of Industry 4.0 to quickly realize a digitized economy in order to "complete the transition into a digital economy by 2023" (Chan et al., 2021, p.1). However, to achieve such an ambitious plan, Cambodia needs to tackle the main issues that will hinder the Kingdom from achieving its goal. A report from the United Nations Development Programme (UNDP), *The Adaptation and Adoption of Industry 4.0 in Cambodia,* points to the underdevelopment of cyber security regulations as one of the barriers to widespread adoption of new Industry 4.0 technologies in developing countries, including Cambodia (Navarrete et al., 2020, p. 28-50). It is very important to ensure that digital infrastructure is protected with an effective security layer. This chapter will explain the key factors underlying the issues of the cyber security layer of Cambodia's digital infrastructure and recommend five areas in which Cambodia can focus in order to develop strong and robust security for the Kingdom's cyberspace.

Context Analysis

Malware Attacks and Cyber Security Awareness

The security layer of Cambodia's digital infrastructure is fragile and prone to cyberattacks. In November 2014, a group of Cambodian university students were able to hack into a total of 30 government websites (Sany and Wilwohl, 2014). In addition, in November 2019, seven official Facebook pages of Cambodian national and sub-national institutions were the targets of

cyberattacks from actors outside of Cambodia (Voun, 2019). According to Kaspersky Lab's report in 2019, Cambodia experienced 4,590,076 online cyberattacks which affected around 30 percent of the Kingdom's internet users. The report saw an increase of 2,835,938 cyberattacks compared to the previous year (Flynn, 2019). This indicates that Cambodia has become an increasingly popular target of cyberattacks and other cyber-related crimes.

In addition, Cambodia still faces another challenge related to cyberattacks which involves the behavioral aspect of the internet and network users. In 2020, the Ponemon Institute and IBM Security conducted a Cost of Data Breach Study of over four hundred organizations in seventeen countries. They found that the third highest cause of data breaches was due to human errors. This includes employees within organizations who failed to protect their organization's digital infrastructure due to negligence or errors. This accounted for 23 percent of the total data breaches of organizations that were surveyed (Ponemon Institute and IBM Security, 2020, p.30). The vulnerability of the Cambodian population of internet users to cyberattacks is related to a general lack of awareness of cyber security. Ayu Kusumastuti and Astrida Fitri Nuryani conducted a study on the digital literacy levels of ASEAN member states. The study used five main indicators in assessing digital literacy: information literacy, computer literacy, media literacy, communications literacy, and technology literacy. According to the study, digital literacy in Cambodia is the lowest in the ASEAN region with a mean rank of 15.60, significantly below ASEAN's average rank of 20.5 (Kusumastuti and Nuryani, 2020, p.30-31).

Institutions and Mechanisms to Combat Cyber Crimes and Incidents

In terms of providing a mechanism to combat cyberattacks, the Royal Government of Cambodia established a specialized unit called Cambodia Computer Emergency Response Team (CamCERT) in 2007. CamCERT provides a point of contact for any incidents involving Cambodia's cyberspace. Cyberspace includes elements of information systems infrastructures such as the Internet, telecommunications networks, computer systems, and embedded processors and controllers (National Institute of Standards of Technology, n.d.). CamCERT has jurisdiction over monitoring the National Information Infrastructure and government servers (CamCERT, 2017a). Furthermore, CamCERT has a responsibility to inform Internet users about any cyberattacks or incidents that occur on the Internet as well (CamCERT, 2017b). CamCERT is under the authority of the Information and Communications Technology (ICT) Security Department which is a department within the Ministry of Post and Telecommunications (MPTC). In addition to CamCERT, a specialized unit in combating cyberattacks and cyber-related incidents was also established under the Anti-Cybercrime Department of the National Police of Cambodia in 2016. This is the institution where complaints can be lodged and investigations can be launched to catch cybercriminals (Cambodia Development Resource Institute, 2020)

CamCERT is still young and needs to cooperate with many stakeholders in order to effectively deliver its mission and operations. The establishment of CamCERT is crucial to the development of a response and recovery plan based on international standards. However, there are challenges remaining to ensure these standards are met. For example, CamCERT is not a member of the Forum of Incident Response and Security Teams (FIRST), the international platform which brings together a total of 574 cyber security teams from 97 different countries to forge a safer cyberspace (Forum of Incident Response and Security Teams, 2021). Thus, CamCERT lacks the level of cyberthreat expertise needed to mitigate cyberattack risks effectively. CamCERT is also not a member of the Asian Pacific Computer Emergency Response Team (APCERT) unlike the CERTs of Laos, Myanmar and Vietnam (Asia Pacific Computer Emergency Response, n.d.). This may obstruct CamCERT from accessing better opportunities to connect and collaborate systematically with the other response teams regionally and internationally.

Cyber Security Legal Framework

Cambodia lacks a cohesive legal framework to govern its cyberspace. As the Cyber Security Law is being drafted, existing legal measures to combat cyber-related issues and crimes can be found in various laws such as the Criminal Code of the Kingdom of Cambodia (2009), Law on Telecommunications 2015, and the Internet National Gateway Law (2021). These legal instruments are still insufficient to fully protect the country's cyberspace because of the lack of a common and clear concept of what is considered a cybercrime. The terms which are mentioned in the existing legal instruments are too vague and broad with no concise explanation. Thus, the lack of a specific definition of the term may present difficulties to the authorities who wish to impose appropriate measures on cyber criminals (Nguon and Srun, 2019).

References to cybercrimes are made in several articles of the Criminal Code of the Kingdom of Cambodia (2009). Articles 317 to 320 refer to cyber security crimes as the "Infringement on the secrecy of correspondence and telecommunications'' (Ministry of Justice, 2009). Cybercrimes are also referred in Articles 427 to 432 as the "offences in the information technology sector" with no further explanation on what actions can be considered as the offences in the IT sector. According to Article 427, these crimes refer to the act of "having access to a system of automated data processing or maintaining access to it" and the act "which has resulted in either deletion or modification of the data contained in the system" (Ministry of Justice, 2009). The Law of Telecommunications (2015) is another legal mechanism which explicitly mentions security in the field of ICT. Article 80 states that the "establishment, installation and utilization of equipment in the telecommunications sector, if these acts lead to national insecurity, shall be punished by sentences from seven to fifteen years imprisonment" (Ministry of Posts and Telecommunication,

2015). However, this applies only to security within the telecommunications sector of Cambodia, and not to other forms of cybercrimes and cyber-related incidents.

The National Internet Gateway (NIG) is the latest addition to the legal instruments that shape Cambodia's position with respect to the security of the Kingdom's cyberspace. Article 12 states that "NIG operators shall cooperate with relevant authorities in collecting national revenue, assuring safety, public order, dignity, culture, tradition, and custom of the society, as well as preventing and cracking down on crimes'' (Royal Government of Cambodia, 2019). However, this clause has received criticism from national civil society organizations and international organizations over its vagueness in the definition of "safety" and "security". In addition, the Draft Law on Cyber Crimes has also come under similar criticism as the draft has been under several revisions since 2014 (Human Rights Watch, 2020).

Critical Information Infrastructure (CII)

Critical Information Infrastructure (CII) refers to the interconnected information systems and networks used by the government to determine what are the assets that are essential for the functioning of the economy and social welfare of the country (U.S. Department of Homeland and Security, 2011, p.10). Different governments may have different definitions of what is considered critical infrastructure. In the United States, the Cybersecurity and Infrastructure Security Agency (CISA) defines sixteen critical infrastructures to be so vital to the United States that any disruptions would produce dire consequences on the security, national economic security, national public health or safety of the United States' population (Cybersecurity and Infrastructure Security Agency, n.d.). In Myanmar, the government defines CII assets in their Draft Cyber Security Law. There are eight infrastructures which are identified to be the CII of Myanmar including e-government services and electronic information and infrastructure of various industries ranging from finance to natural resources (Myanmar Centre for Responsible Business, 2021). Overall, governments tend to identify similar elements to be CII. In a study conducted by the OECD, OECD Member States commonly identified critical assets to be assets in the field of energy, finance, healthcare, food and agriculture and government facilities, among others (Gordon and Dion, 2008, p.5). Cambodia is also facing similar threats in these sectors. For instance, the Kingdom has faced several attacks in the banking and finance sector. In 2012, the National Bank of Cambodia was reported to be hacked and vital information regarding individuals' identification was leaked (Li, 2013). In 2016, Ou Phanarith, director of ICT Security at the Ministry of Posts and Telecommunications warned that Cambodian financial institutions were particularly vulnerable to cyber fraud as new forms of cybercrimes have developed in recent years (Kotoski, 2016).

Regional Cooperation on Cyber Security in the ASEAN region

Cambodia is considered to be one of the countries least committed to cyber security in the Southeast Asia region. According to the Global Cybersecurity Index 2020 Cambodia ranked last in Southeast Asia with a score of only 19.12 comparing to its neighboring countries such as Lao P.D.R. (20.34), Thailand (86.5), and Vietnam (94.55). In the Asia-Pacific region, Cambodia ranked 26th out of 38 countries in the region with a global rank of 132nd out of 193 countries total (International Telecommunication Union, 2020, p. 27-30) (See Table 1). However, the regional ASEAN member states in general lag behind other parts of the world in strengthening cyber-security. Data has shown that ASEAN member states spent an estimated US$1.9 billion in 2017, equating to only 0.06 percent of the region's gross domestic product (GDP) on cyber security (Strengthening ASEAN's cyber security, 2018) which is lower than a global average of 0.13 percent (A.T. Kearney, 2018).

Table 1: GCI Ranking 2020, ASEAN Member States

Country	Score	Regional Rank	Global Rank
Singapore	98.52	1	4
Malaysia	98.06	2	5
Indonesia	94.88	6	24
Vietnam	94.55	7	25
Thailand	86.5	9	44
Philippines	77	13	61
Brunei Darussalam	56.07	16	85
Myanmar	36.41	18	99
Lao P.D.R.	20.34	25	131
Cambodia	19.12	26	132

Source: International Telecommunications Union, 2020

Recognizing the importance of protecting the cyberspace of the region, the ASEAN Member States altogether released a joint statement on the ASEAN Declaration to Prevent and Combat Cybercrime in 2017 (ASEAN, 2017). This declaration signifies the official beginning of cooperation between ASEAN Member States in forging unifying anti-cybercrime measures. The declaration

was endorsed after the 11th ASEAN Ministerial Meeting on Transnational Crime in September 2020 and adopted by the Head of States of the ASEAN Member States (ASEAN, 2017). This declaration set a milestone for ASEAN's dedication in protecting its regional cyberspace.

Policy Recommendations

This analysis of Cambodia's contemporary cyber security context shows that the Kingdom still needs to take appropriate steps in order to effectively and urgently secure its cyberspace. Cambodia needs to prioritize five main areas: i) Establishing a specialized unit to govern its cyberspace, ii) Developing a comprehensive legal framework which aligns with internationally recognized standards, iii) Promoting a strong and vibrant cyber security ecosystem, iv) Nourishing an empowered digital citizen, v) Creating a protection program and recovery plan for the CII.

Establishing a Single Specialized Cyberspace Governing Unit

Establishing a dedicated unit responsible for national cyber security policy development is a necessary step to enforce the laws and regulations that have been put into place to govern cyberspace. This unit should be given a wide scope of action, including the mandate to develop a cohesive national cyber security strategy with concrete initiatives. These initiatives would include providing protection over critical infrastructure, mobilizing the necessary resources to respond to cyberattacks, defining cyber security standards to be used across governmental institutions, and executing educational programs to raise cyber-awareness among the public as well as training for IT Security professionals. For instance, in Singapore, the Cyber Security Agency (CSA) of Singapore was established in 2015 to protect the city-state's Critical Information Infrastructure; monitor the cyberspace for cyberthreats and allocate necessary resources to mitigate the risks; certify and validate the system's security assurance; and conduct outreach programs to enrich the cyber security ecosystem and good cyber hygiene practices among the public (Cyber Security Agency, n.d.).

Currently, there is no such centralized unit to govern the Kingdom's cyberspace, as CamCERT's responsibilities are limited. Instead of having multiple agencies to govern Cambodia's cyberspace, establishing a single dedicated institution which expands on the mandates of CamCERT is more efficient because it will prevent unintentional bias towards any institutions during budget and resource allocation as well as prevent potential inter-governmental competition for resources (International Telecommunication Union, 2018, p.18). In Singapore, following the establishment of the CSA, the responsibility of overseeing 11 critical sectors fell under a single authority so that the protection of the city-state's cyberspace would become more efficient (Cyber Security Agency, 2021). The staff from the institutions which were previously

responsible for cyber security protection such as the Ministry of Home Affairs' Singapore Infocomm Technology Security Authority and Infocomm Development Authority's Singapore Computer Emergency Response Team (SingCERT) were also transferred to the new agency (Tham, 2016). Establishing this complex specialized unit requires in-house technical skills and expertise. In order to tackle this issue, the specialized agency must involve other stakeholders including other governmental institutions, private sector actors, and civil society organizations in order to adequately fill the capacity gap. In addition, the specialized unit should prioritize international collaboration. CamCERT should consider becoming a member of regional and international computer emergency response teams such as FIRST and APCERT. Such collaborations would enable Cambodia to effectively tackle cyber incidents across boundaries as well as exchange expertise and standards for securing cyberspace.

Development of Cyber Security Legal Framework and International Standards

The RGC has been developing a draft cyber security law under the supervision of the Ministry of Post and Telecommunications. While developing the law, the RGC should consult with stakeholders in the private sector and civil society in order to develop a comprehensive framework that can provide protection for businesses, individuals, and public institutions alike. The legal framework can be developed in accordance with the Budapest Convention, an international treaty that has been signed by more than sixty states. The Budapest Convention, also known as the Convention on Cybercrime, is the only existing multilateral treaty which addresses cybercrimes. It was proposed by the Council of Europe in 2001 and currently, the majority of the signatories are countries in North America and Western Europe. The Budapest Convention has not received endorsement from the governments of Russia, Brazil, India, and China due to Article 32 which permits extraterritorial searches. Russia and China have been active supporters of cyber sovereignty, meaning the government has authority over cyberspace within its territory's border (Chen, 2017). At the regional level, strong collaboration between ASEAN Member States can support the development of a legal framework for regional cyberspace. The majority of the ASEAN Member States are not signatories of the Budapest Convention. Currently, only the Philippines has signed. ASEAN has many dialogue platforms such as the ASEAN Summit and the Asia-Europe Meeting (ASEM) which are platforms to engage the major powers in dialogues. As such, Cambodia, through ASEAN, can advocate for the establishment of a new convention which would invite all major powers such as China, the US, and Russia to the negotiation table in order to develop common international standards and a framework that would take all states' interests into consideration.

Fostering a Healthy Cyber Security Ecosystem

In order to build a strong security layer for the country's digital infrastructure, the government must promote a healthy cyber security ecosystem which involves assistance from many stakeholders such as public citizens, professionals, and private-sector organizations by enabling cyber security firms to thrive, developing the technical capacities of cyber security professionals, and raising the awareness of citizens in cyber security. Since Cambodia's main obstacle is the lack of cyber security experts and professionals in the national labor market, the government needs to focus on strengthening the in-house capacity through cooperation between the local cyber security startups and companies, foreign cyber security professionals, and university professors and students. Firstly, the government needs to attract cyber security enterprises to invest in the cyber security infrastructure of the Kingdom. To ensure that the market environment is attractive to foreign cyber security enterprises, the government must ensure that the legal framework related to protecting cyber security is in line with international standards as mentioned in the previous section. Secondly, the RGC should instill a culture of sharing and cooperation between foreign and local cyber security companies. The RGC, through the National Cybersecurity Agency, can establish and implement awareness and skill-building programs and workshops in order to build a strong sense of cooperation between the stakeholders. In addition to the capacity building programs, the RGC should also provide economic and administrative incentives for accredited cyber security firms and service providers to conduct capacity training on cyber security for Cambodian professionals and their targeted customers.

To ensure that there is a sufficient supply of cyber security professionals in the long run, the CNCA should establish a hub that links private sector actors with universities and other higher education institutions. The RGC should support the establishment of cyber security related programs in higher education systems at both undergraduate and graduate levels, with the assistance of the private cyber security sector. That workforce can become qualified professors and researchers on cyber security issues and further expand the number of cyber security experts in higher education institutions. The National Cybersecurity Agency can play a role of facilitating connections between professionals and experts from cyber security related industries and universities and other higher education institutions.

Nourishing an Empowered Digital Citizen

The RGC should also consider implementing programs to raise cyber security awareness among the Cambodian public, especially among youths. Currently, CamCERT has made an effort to inform the general public about issues of cyber security and the public can receive effective guidance and real-time reports of incidents from trusted government sources. However, with the

rapidly increasing use of ICT in daily lives, especially in professional environments, it is important for the government, through the CNCA, to establish a comprehensive strategy which focuses on educating the general public to become "smart users". Smart users means that the public has acquired knowledge of digital safety skills as well as their human rights on the internet (Nguyen and Thong, 2021, p.14). To increase smart users among the public, the CNCA must develop a strategy based on a collective, human-centered, and rights-based approach. Firstly, the CNCA must acknowledge that educating the general public to become smart users is a long-term project. Thus, the institution needs to collaborate with relevant local and foreign stakeholders who possess sufficient skills and resources to implement the required capacity-building programs. Secondly, the programs should be developed with the objective of ensuring the general public has the basic capacity to protect their data and information from cyberattacks and to take responsive measures to solve the issues if incidents were to arise. These digital safety skills include the ability to identify cyber risks, evaluate the risks, and take appropriate measures to mitigate the risks. Thirdly, the programs should also focus on introducing and instilling the knowledge of important rights to the general public such as their rights to data protection and privacy so that they can utilize the legal framework to protect their data and information on the internet.

Creating a protection program and recovery plan for the CII

The RGC should also identify the most critical infrastructure which should be given priority for protection. Critical Information Infrastructure has typically been a frequent target for cyberattacks. Thus, it is appropriate to prioritize protecting critical assets for the country based on their value in ensuring the welfare of the economy, society, and national security. Firstly, the CNCA should conduct a thorough study in order to assess and prioritize the sectors that urgently need to be protected from cyberattacks. Doing so can ensure that the budget and resources will be effectively allocated to invest in those identified critical assets and infrastructure. The identification of critical infrastructure should also be included in the Draft Cybercrime Law to guarantee that the infrastructure will receive appropriate protection from any cyber-related crimes and incidents. Secondly, the RGC must develop a national incident response and recovery plan in order to mitigate the risks and effects of cyberattacks and cyber-related crimes on the CII. There should be clearly defined reporting procedures for the victims of cyberattacks or cyber-related crimes. Currently, there is no single point of contact for reporting incidents and the victims are left to deal with various agencies such as CamCERT and the Anti Cybercrime department. For CamCERT, there is a lack of a clear reporting procedure on its official website, especially in the Khmer language. Thirdly, there should be a robust mobilization plan in order to respond effectively to cyberattacks. This plan should include what level of governmental agencies deal with what types or levels of cyber incidents. By having a concrete cyber security response

and recovery plan, all public and private stakeholders would have clear and specific roles in mitigating the risks. The CamCERT and Anti Cybercrime department, as well as other future institutions, will have distinct mandates and responsibilities so they can effectively operate together for an integrated response against cyberattacks of any type and scale.

Conclusion

Ultimately, Cambodia needs to step up and prioritize strengthening its cyber security system. Incapacity to build a strong and robust cyber security system could lead to two main complications. Firstly, it could prevent Cambodia from benefiting fully from the digital economy. Malware attacks and other incidents will cause economic losses for the Kingdom. Cambodia will remain the country with the poorest cyber security in the region. As ASEAN collectively aims to digitize the regional economy, Cambodia may be put into a disadvantageous position. Thus, it is important for Cambodia to focus on securing the cyber security layer to align with the increasing dependence of the country's economic and social activities on new digital technologies. Secondly, looking towards the future cyber security is one of the main concerns among Cambodians. As people are becoming more dependent on the internet and technology in both of their personal and professional life, cyber security will inevitably become a major concern for everyone with respect to the safety and security of their own data and information. For Cambodian citizens like Soriya, having good cyber security infrastructure will make them feel safe and confident on digital platforms, the same way they feel confident in the physical world where law enforcement of the society is well-developed and strengthened. Cambodians will not only benefit from strong institutions and legal frameworks, but also from the programs which the CNCA will implement to strengthen basic digital safety skills among the Cambodians themselves. Many Cambodians will be more equipped to protect their data and information online and to take appropriate measures when cyber-related incidents occur.

References

ASEAN, (2017, November 14). *ASEAN Human Rights Declaration*. Retrieved from: http://asean.org/wp-content/uploads/2017/11/ASEAN-Declaration-to-Combat-Cybercrime.pdf

Asia Pacific Computer Emergency Response Team (n.d.). Member Teams. Retrieved from: https://www.apcert.org/about/structure/members.html.

A.T. Kearney. (2018). *Cybersecurity in ASEAN: An Urgent Call to Action.* Retrieved from: https://www.kearney.com/documents/20152/989824/Cybersecurity+in+ASEAN.pdf/2e0fb55c-8a50-b1e3-4954-2c5c573dd121

Cambodia Development Resource Institute. (2020). *Cybergovernance in Cambodia: A Risk-Based Approach to Cybersecurity*. Retrieved from: https://cdri.org.kh/wp-content/uploads/SP18_cybersecurity.pdf.

CamCERT. (2017a, May 9). *What We Do*. [website] Retrieved from: https://www.camcert.gov.kh/en/what-we-do/.

CamCERT. (2017b, May 9) *Who We Are.* [website] Retrieved from https://www.camcert.gov.kh/en/who-we-are/.

Chan, P., Chhem, S., and Nay, D. (2021). Developing Cambodia's Digital Economy: Youth's Perspective*.* 7th Annual NBC Macroeconomic Conference, 1. Retrieved from: https://www.nbc.org.kh/download_files/macro_conference/english/S6_Development_Cambodia_Digital_Economy_Youth_Perspective.pdf.

Chen, Q. (2017, August 03). Time for Asean to get serious about cyber crime*. The Diplomat*. Retrieved from: https://thediplomat.com/2017/08/time-for-asean-to-get-serious-about-cyber-crime/

Cyber Security Agency. (2021, July 19). *FAQ*. [website] Retrieved from: https://www.ifaq.gov.sg/csa/apps/fcd_faqmain.aspx

Cyber Security Agency (n.d.). CSA: Our Organisation. [website] Retrieved from: https://www.csa.gov.sg/Who-We-Are/Our-Organisation.

Cybersecurity and Infrastructure Security Agency. (n.d.). Identifying Critical Infrastructure During COVID-19. Cybersecurity and Infrastructure Security Agency. Retrieved from: https://www.cisa.gov/identifying-critical-infrastructure-during-covid-19.

Flynn, G. (2019, August 26). Cambodia to Host International cyber security Conference. *Khmer Times*. Retrieved from: https://www.khmertimeskh.com/636876/cambodia-to-host-international-cyber security-conference/.

Forum of Incident Response and Security Teams. (2021) FIRST Members around the world. Retrieved from: https://www.first.org/members/map.

Gordon, K., and Dion, M. (2008). *Protection of 'Critical Infrastructure' and the Role of Investment Policies Relating to National Security*. Paris, France: Organisation for Economic Co-operation and Development. Retrieved from: https://www.oecd.org/daf/inv/investment-policy/40700392.pdf

Human Rights Watch. (2020, November 13). *Cambodia: Scrap Draft Cybercrime Law*. Retrieved from: https://www.hrw.org/news/2020/11/13/cambodia-scrap-draft-cybercrime-law.

International Telecommunication Union (ITU). (2018). Guide to Developing a National Cybersecurity Strategy. Retrieved from: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

International Telecommunication Union (ITU). (2020). Global cyber security Index 2020. Retrieved from: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Kotoski, K. (2016, May 05). Banks warned on growing threat of cyber fraud. *The Phnom Penh Post*. Retrieved from: https://www.phnompenhpost.com/business/banks-warned-growing-threat-cyber-fraud

Kusumastuti, A., and Nuryani, A. (2020). Digital Literacy Levels in ASEAN (Comparative Study on ASEAN Countries). Proceedings of the Proceedings of the 13th International Interdisciplinary Studies Seminar, 30-31 October 2019, Malang, Indonesia. Retrieved from: https://doi.org/10.4108/eai.23-10-2019.2293047

Li, M. (2013, June 07). Web hacks a risk for banks. *The Phnom Penh Post*. Retrieved from: https://www.phnompenhpost.com/business/web-hacks-risk-banks

Ministry of Justice. (2009). General Provisions for the Implementation of Criminal Law. Retrieved from: https://www.trc.gov.kh/wp-content/uploads/2016/03/Law-on-Telecommunicaiton-in-Eglish-Unofficial-Translation.pdf

Ministry of Posts and Telecommunications. (2015). Law on Telecommunications. Retrieved from: https://www.trc.gov.kh/wp-content/uploads/2016/03/Law-on-Telecommunicaiton-in-Eglish-Unofficial-Translation.pdf

Myanmar Centre for Responsible Business (2021, February 12). Analysis of the Provisions of the Draft Cyber Security Law. Retrieved from http://www.myanmar-responsiblebusiness.org/pdf/2021-cyber-security-bill-legal-analysis.pdf

National Institute of Standards of Technology. (n.d.). Cyberspace – Glossary. Computer Security Resource Center. Retrieved from https://csrc.nist.gov/glossary/term/cyberspace.

Navarrete, J. C., Ayala, D. L., Gómez , C. L., and Palladino, M. (2020). *Adaptation and Adoption of Industry 4.0 in Cambodia*. Phnom Penh, Cambodia: United Nations Development Programme. Retrieved from: https://www.undp.org/content/dam/cambodia/docs/ResearchAndPublication/2020/Industry%204.0%20Report%20Final.pdf

Nguon, S., and Srun, S. (2019). Cambodia v. Hackers: Balancing Security and Liberty in Cybercrime Law. *Digital Insights*, 76–95. Retrieved from: https://www.kas.de/documents/264850/7993338/Chapter+5.pdf/14d17599-c508-93a7-73d4-0f0cba039de1?version=1.0&t=1579754366354.

Nguyen, D. Q., and Thong, L. K. (2021). *Shifting from Cybersecurity to Digital Safety. Innovating Policies to Address the Digital Age's Safety Challenges in Vietnam- A Discussion Paper*. Unpublished manuscript.

Ponemon Institute, and IBM Security. (2020). IBM: Cost of a Data Breach Report 2020. Retrieved from: https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf.

Royal Government of Cambodia. (2019). SUB-DECREE on Establishment of National Internet Gateway. Retrieved from: https://www.trc.gov.kh/wp-content/uploads/doc/Internet-Gateway-23.pdf

Sany, S., and Wilwohl, J. (2014, April 23). Hackers Arrested in Joint Operation with FBI. *The Cambodia Daily*. Retrieved from: https://english.cambodiadaily.com/news/hackers-arrested-in-joint-operation-with-fbi-57065/.

Strengthening ASEAN's cyber security (2018, December 03). Strengthening ASEAN's cyber security. *The ASEAN Post.* Retrieved from: https://theaseanpost.com/article/strengthening-aseans-cybersecurity

Tham, I. (2016, January 19). New Cyber Security Agency to be set up in April, Yaacob Ibrahim to be minister in charge of cyber security. *The Straits Times*. Retrieved from: https://www.straitstimes.com/singapore/new-cyber-security-agency-to-be-set-up-in-april-yaacob-ibrahim-to-be-minister-in-charge-of.

U.S. Department of Homeland and Security. (2011). *Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise*. Retrieved from: https://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf

Voun, D. (2019, November 20). Interior Ministry Regains Control of Seven Hacked Gov't Facebook Pages. *The Phnom Penh Post.* Retrieved from: https://www.phnompenhpost.com/national/interior-ministry-regains-control-seven-hacked-govt-facebook-pages.

www.futureforum.asia

Core Donor

Sverige

In Partnership With

UNITED NATIONS CAMBODIA

secdev.foundation