Commentary

Vol 3, Issue 11, 05 August, 2021

Cybersecurity in Cambodia: Awareness as a First Step

Riccardo Corrado, PhD* and Morokot Sakal, MEng**

ASEAN, the association consisting of ten countries, namely Brunei, Cambodia, Indonesia, Lao PDR, Malaysia, Myanmar, The Philippines, Singapore, Thailand, and Vietnam, also known as ASEAN Member States (AMS), has attracted a lot of interest due to the ongoing growth and strong economic potential, with Cambodia being one of the fastest-growing economies in the region and the world. An important element of the recent growth of ASEAN in general, and Cambodia in particular, has been connected to the digitalization wave that has invested the world. Regarding digitalization, the Information Communication Technology (ICT) has been recognized as, and it is going to continue to be the major driver in every aspect of the multifaceted national growth process for decades to come, and a fundamental factor to support Cambodia's sustainable and inclusive growth.

Along with the digital growth in the region and the country, cybersecurity is emerging as a relatively new field essential for Cambodia. Specifically, cybersecurity has become a foundational element underpinning the achievement of socio-economic goals of modern economies (ITU, 2018), and it is fundamental for Cambodia to strengthen its savviness and its capabilities in this field. Cybersecurity is not completely new to the Kingdom, with computer-related offenses being introduced for the first time in the Cambodian Criminal Code (2009) in the Articles 317-320 and 427-432, but being referred to a very general way, as offenses relative to the IT sector (Nguon & Srun, 2019). Following the National Cyber Security Index (NCSI), a global index that measures the preparedness of countries to prevent cyber threats and manage cyber incidents, Cambodia scores very low. Currently, at the regional level, Cambodia, together with the other AMS, has only agreed in principle to general non-binding principles, yet unable to develop new norms (Van Raemdonck, 2021).

Considering the importance of cybersecurity for inclusive sustainable growth of the Cambodian economy, and accounting for the current relatively low strength in terms of cybersecurity, a fundamental aspect to consider and foster is represented by awareness (CGTech, 2021). Specifically, an information campaign raising awareness within the country, together with effective policies for cybersecurity, are essential elements to foster cyber hygiene and protect the country and the citizens from the risks coming from the cyberworld. In the remaining of this paper, we first offer an overview of the current scenario in terms of cybersecurity in the ASEAN region, with a specific focus on Cambodia. Then, we offer an overview of the most common cyberattacks, explaining how they work and thus offering the basis for understanding them, and for being aware of the risks coming from the digital world, followed by a well-known approach conceptualized by Sun Tzu in his famous work "The Art of War: if you know your enemy, you need no fear".

* **Dr. Riccardo Corrado** is an assistant professor and chair of the ICT program at the American University of Phnom Penh (AUPP) and advisor to the Cambodian Ministry of Post and Telecommunications. He is also a collaborator on the STEAM program of the AUPP High School-Foxcroft Academy.
** **Mr. Morokot Sakal** is a researcher and instructor at the American University of Phnom Penh (AUPP), and collaborator on the STEAM program of the AUPP High School-Foxcroft Academy.

Cybersecurity: ASEAN and Cambodia

In terms of cyber vulnerabilities, a 2016 study showed that the Asia-Pacific region is 80 percent more likely to be targeted by hackers, compared to the rest of the world (FireEye, 2018), with the Philippines being one of the top targets in the world. The term *Cybersecurity* is used in subnational, national and transnational context, including a wide array of threats related to the digital sphere, and it is bringing along a new field of interest related to cybercrime control and prevention activities (Dupont & Whelan, 2021). Considering the increasing exposure to attacks that individuals, companies and also governmental agencies are facing due to the incredibly fast pace that digitalization is spreading in the world, Cambodia, along with the other AMS, created a Ministerial Conference on Cybersecurity (AMCC), with the goal to develop a common strategy to adopt at the regional level, addressing topics such as cybersecurity control and resilience protection (Van Raemdonck, 2021). Within the AMCC, a coordinating committee on cybersecurity (ASEAN Cyber-CC) was created with the role to work cross-sectorally with relevant stakeholders on cybersecurity-related issues (Van Raemdonck, 2021). Currently, the region lacks a general overarching regulation on cybercrime (Van Raemdonck, 2021), which also presents in the Kingdom (Nguon & Srun, 2019). Specifically, even though there is ongoing cooperation on cybercrime between AMS, a common understanding of the definition of cybercrime is still missing, and there is still a clear insufficiency in terms of a common approach for addressing cybersecurity threats in the region (Van Raemdonck, 2021). Specifically, AMS have agreed in principle to eleven voluntary, non-binding principles, defined in the 2015 report by the UN Group of Governmental Experts (UNGGE), but unable to develop new norms and instead basing their cooperation on practical implementation of the UNGGE ones (Van Raemdonck, 2021).

The eleven principles are divided into two categories. The first category is comprising five principles that refer to limitations to respect, with the second category that includes six good practices to follow. Specifically, the first category includes the following principles: (1) “states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs”; (2) “states should not conduct or knowingly support ICT activity that intentionally damages critical infrastructure”; (3) “states should take steps to ensure supply chain security, and should seek to prevent the proliferation of malicious ICT and the use of harmful hidden functions”; (4) “states should not conduct or knowingly support activity to harm the information systems of another state’s emergency response teams (CERT/CSIRTS) and should not use their own teams for malicious international activity”; (5) “states should respect the UN resolutions that are linked to human rights on the internet and to the right to privacy in the digital age” (CCDCOE, 2021). Furthermore, a list of six good practices to follow were added to the previous five limitations: (1) “states should cooperate to increase stability and security in the use of ICTs and to prevent harmful practices”; (2) states should consider all relevant information in case of ICT incidents; (3) states should consider how best to cooperate to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs; (4) “states should take appropriate measures to protect their critical infrastructure”; (5) “states should respond to appropriate requests for assistance by other states whose critical infrastructure is subject to malicious ICT acts”; (6) “states should encourage responsible reporting of ICT vulnerabilities and should share remedies to these” (CCDCOE, 2021). With these premises, it is important to highlight the fact that currently, how exactly AMS should act when actual incidents occur is still unclear (Van Raemdonck, 2021).

In addition to regional cooperation, Cambodia, together with the other AMS, showed its commitment to cooperating on cybersecurity outside of its borders, and more specifically with the EU, with a 2019 joint statement on cybersecurity cooperation. Regarding this cooperation, the EU and ASEAN

confirmed the commitment to contribute to the advancement of an open, safe, stable, accessible, and peaceful ICT environment (Van Raemdonck, 2021). This intensified commitment answers to the increasing concern over cyberattacks targeting the AMS. According to the consulting firm Kearney, possible threats to ASEAN region have intensified and this intensification is forecasted to grow in the future (Kearney, 2018). Kearney stated that growing interconnectedness will in fact fuel the systematic risk, making the region only "as strong as its weakest link", while the rapid technological evolution is representing an important factor in enhancing the difficulty of monitoring and responding to cyber threats, especially due to the increasing adoption of encryption, multi-cloud operations, Internet of Things (IoT) and operation technology (Kearney, 2018).

Furthermore, focusing specifically on Cambodia, currently, the cybersecurity overall capabilities in the country are lacking. Following the NCSI index, a global index that measures the preparedness of countries to prevent cyber threats and manage cyber incidents, Cambodia ranks low. Specifically, the NCSI index measures countries' cybersecurity capacities that are implemented by the central government, and Cambodia was ranked in the 122nd position, with a score equal to 15.58 and a digital development index of 34.41 (NCSI, 2021). In comparison, Thailand was ranked 71st with an index equal to 42.86 and a digital development index of 55.08, Malaysia was ranked 22nd with an index equal to 72.73 and a digital development index of 62.61, and Singapore was ranked 16th with an index equal to 80.52 and a digital development index of 80.94 (NCSI, 2021). Additionally, Cambodia also ranks low (102nd in the world) in the digital readiness index of Cisco (2019), and is still lacking in cybersecurity training, with currently no universities offering programs focusing on this specific field.

As aforementioned, one of the most important steps for the country to enhance cybersecurity readiness should be raising awareness and knowledge. It is essential to equip Cambodians with a better understanding of the possible threats and attacks, how they are carried out and how they work in order to address vulnerabilities and avoid harmful behaviors. Thus, what are the typologies of cyberattacks that AMS, Cambodia included, are currently suffering from and how do they work? The first step consists of raising awareness and informing the public about the typology of attacks, and in what they consist of, something that is provided in the following of this paper.

Cyberthreats: What and How

Following the International Criminal Police Organization (INTERPOL), improving awareness of cybercrime and cybersecurity is an essential step for combatting cybercrime (INTERPOL, 2020). According to a recent report from one of INTERPOL's partners, namely Kaspersky, a global leader in cybersecurity solutions and services, 14 million phishing attempts against internet users were detected in Southeast Asia, only in the first six months of 2019 (INTERPOL, 2020). With a specific focus on the AMS, botnets have been reported to be on the rise, mainly targeting the financial sector and its customers, which is a sector, known as the Fintech one, that is still young and growing fast in Cambodia. For this reason, it requires a lot of attention, because it is easy to attract unwanted attention from possible attackers (Lim & Sek, 2020). Following Palo Alto Networks, one of the major companies in the world for cybersecurity, a botnet is a network of computers that have been infected by malware, and due to this alien software, they are under the control of a malicious attacker, also knowns as the bot-herder (Palo Alto Networks, 2021). In a botnet, the bot-harder can control each individual machine, which de facto represents one of the bots, and through the bot, the central entity can carry out a coordinated criminal action (Palo Alto Networks, 2021). Furthermore, the control is not static and in fact, since botnets remain under the control of the malicious attacker, the infected machines can keep receiving updates and thus,

change their behavior to sustain the attack over time (Palo Alto Networks, 2021).

However, botnets, are only one of the major threats to which Cambodia is exposed. INTERPOL, in this regard, identified in business e-mail compromise (BEC), phishing, ransomware, e-commerce data interception, crimeware-as-a-service and cyber fraud as the major threats in the region as well (INTERPOL, 2021). To better protect ourselves from these threats, it is essential to have a clear understanding of what these threats are. Regarding the first one, namely BEC, in this type of cyber-attack, attackers send an email that appears as a legitimate request, coming from a known or familiar source, thus inducing trust in the receiver (FBI, 2021). An example could be represented by an attacker using a similar email to a legit one, an email that the company used to rely on. These messages look like they are coming from a trusted source in order to trick the victims into sharing or revealing confidential information, and thus offering the opportunity for the attackers to obtain useful information related to company accounts, calendars and data that can be later used to carry out the BEC schemes (FBI, 2021).

As for phishing, this cyber threat refers to when the attackers attempt to deceive users into an action that will trigger the attack. For instance, the victim could be tricked into clicking a bad link that will download malware, or direct the victim to the desired website where a malicious attack can be carried out. Phishing can be conducted via a text message, social media or by phone, but commonly the term 'phishing' is mainly used to describe attacks carried on via email, and capable to reach millions of users due to the nature of email communication while hiding between the usually huge load of the so-called ‘benign emails’ (NCSC, 2021). Regarding ransomware, INTERPOL defines it as “a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid” (INTERPOL, 2021). Within the family of ransomware, the sub-family known as crypto-ransomware encrypts certain files on infected systems forcing users to pay the ransom to obtain a decryption key (INTERPOL, 2021). In addition to the BEC, phishing and ransomware, another cyber threat listed as a common cyberattack in Cambodia is the so-called e-commerce data interception. Specifically, e-commerce data interception is a specific type of malware designed to be usually injected into websites to steal customer payment data from online stores, like credit cards numbers and credentials (INTERPOL, 2021).

Additionally, another major threat for Cambodia is represented by the increasing number of cases of crimeware-as-a-service (CaaS). CaaS is defined as a business model used in the underground market where illegal services are offered to interested malicious buyers for conducting cybercrimes in an automated manner (Sood & Enbody, 2013). In the CaaS model, the process is automatized to the level that the buyer (malicious attacker) has to only purchase a crimeware service and a compromised infrastructure, without having to spend efforts in compromising an infrastructure themselves, infecting systems, launching distributed denial-of-service (DDoS) attacks or stealing financial information like credit card numbers (Sood & Enbody, 2013). In simple words, this can be seen as hiring illegal cyber contractors for perpetrating cyber-attacks to interested attackers who do not have the skills or simply do not want to be involved directly in the attack (Sood & Enbody, 2013). Finally, the most generic and known threat is the so-called cyber fraud, which de facto simply represents any fraudulent action perpetrated digitally.

Considering the numerous cyber risks that are mentioned above and accounting for ASEAN being a region under the radar of cyber attackers, what can a country like Cambodia do?

On Cambodia: What to do to alleviate the impacts?

As previously mentioned, the first step for protecting against cyberattacks is represented by

awareness. Awareness, however, is not the panacea to the problem, but simply the first step for tackling this uprising issue. The right approach is represented by following a framework of action to be implemented at the national level, capable to offer a clear process for paving the path toward a smart, informed and effective schema for dealing with cyberattacks. In this regard, INTERPOL defined a framework of action for reducing the global impact of cybercrime, based on four pillars for supporting cybersecurity. Specifically, the four pillars defined by INTERPOL include (1) enhancing cybercrime intelligence for effective response, (2) strengthening cooperation for joint operations against cybercrime, (3) developing regional capacity and capabilities to combat cybercrime and (4) promoting good cyber hygiene for safer cyberspace (INTERPOL, 2020).

Analyzing these four pillars, the first one identified by the INTERPOL is based on enhancing cybercrime intelligence for effective response. Nouh et al. (2016) on this regard, identify through a literature review of the research body on cybercrimes six major areas of interests, namely detection of communities and organizational structure, behavioral analysis and interaction patterns, disruption of criminal networks, profiling cybercriminals, identifying the disruptive event and predicting offline events, and extraction and identification of online criminal contents. The authors also propose a framework, called CCINT framework, designed to help analysts in making sense out of large numbers of datasets (Nouh et al., 2016), and designed to support the six key steps in the analytical process (Heuer, 1999), namely defining problem, generating hypotheses, collecting information, evaluating hypotheses, selecting the most likely hypothesis, and continuous monitoring of new information (Nouh et al., 2016).

Regarding the second pillar, it consists of strengthening cooperation for joint operations against cybercrimes. As aforementioned, even though there is ongoing cooperation on cybercrime between the AMS, a clear understanding of the definition of cybercrime and a common approach to address cyber-related issues are still missing. The Convention on Cybercrime of the Council of Europe, known as the Budapest Convention, is currently the only binding international instrument addressing cybercrimes and international cooperation in cyberspace, and within ASEAN, only the Philippines ratified it. This is a pillar that needs to be strengthened in Cambodia.

Furthermore, the third pillar defined by the INTERPOL consists of developing regional capacity and capabilities to combat cybercrime. In this regard, the RAND Corporation Research, a research organization that aims to develop solutions to public policy challenges, created a set of guidelines and recommended approaches to enhance national-level cybersecurity capacity building programs while supporting the creation of holistic policy and investment strategies aiming to tackle challenges posed by cyber threats (Bellasio et al., 2018). The RAND guidelines comprise of five dimensions, namely cybersecurity policy and strategy; cybersecurity culture and society; cybersecurity education, training and skills; legal and regulatory frameworks; and standards, organizations and technologies (Bellasio et al., 2018). These five dimensions are required to be built and developed to assure the national level cybersecurity capacity building.

Finally, the last pillar identified by the INTERPOL is represented by the promotion of good cyber hygiene for safer cyberspace. Vishwanath et al. (2020) conceptualize cyber hygiene as the cybersecurity guidelines for online consumers to protect the safety and integrity of personal information on internet-connected devices. The Canadian Centre for Cyber Security, which is the department of the Government of Canada for cybersecurity, identifies the guidelines for general prevention in patch for regular update of devices, protection of internet-connected devices, careful use of Wi-Fi networks, backup of important data

and quick response when notified or even if just suspect that the user device has been infected. NortonLifeLock Inc., the software company specialized in cybersecurity software and services, defined nine steps to follow for maintaining good cyber hygiene. The nine steps include installing reputable antivirus and malware software, use network firewalls, update software regularly, set strong passwords, use multifactor authentication, employ device encryption, back up regularly, keep your hard drive clean and secure the router (Norton, 2021).

Currently in Cambodia, to the best of the authors' knowledge, no studies have investigated the awareness of Cambodian citizens and the level of cybersecurity measures adopted by companies or even governmental bodies. In general, it can be said that Cambodia is lagging behind other countries when it comes to cybersecurity (Lim & Sek, 2020; Nguon & Srun, 2019), even if recently, the country has experienced an intensification of efforts aiming to fight against cyberattacks through the strengthening of local and international mechanisms (Lim & Sek, 2020). At this moment, cybersecurity awareness is generally low, and the overall digital literacy is still low as well (Cisco, 2019; Corrado et al., 2019; Corrado & Tungjan, 2019), even if multiple actions and projects from the government have been initiated aiming to tackle this issue (Corrado, Khat, et al., 2021; Corrado, Pretorius, et al., 2021).

Thus, considering the four pillars defined by INTERPOL, and adopting existing frameworks in the literature, for example, like the one offered by RAND (Bellasio et al., 2018), Cambodian policymakers should tackle as soon as possible the cybersecurity aspect of the digital growth journey that Cambodia has initiated, to foster economic growth, leveraging the affordances of ICT and within a safe digital environment for the public and private sectors.

Conclusion and Suggestion

Cambodia, like many other AMS, is increasingly becoming a target for cyberattacks. The vulnerabilities and risks connected to these attacks are also becoming more worrisome due to the increasing usage of digital solutions both in the private and public spheres. Thus, it becomes incumbent to strengthening the current abilities of Cambodia, both from the governmental perspective and from the citizen's one. An effective campaign cannot be conducted individually by each ASEAN member, but it should start as a cooperation framework of action at the international level, and in the case of Cambodia, strong cooperation should be established within ASEAN. At this moment, only a general non-binding agreement has been reached between the AMS, but no clear framework and guidelines have been crafted. This is the first important gap to fill. Secondly, a national framework of action should take place within the country, adopting a framework already existing in the literature, with appropriate tuning phase tailored to the specific Cambodian ecosystem.

In conclusion, Cambodia should be a strong promoter in the region for the creation of a common ASEAN framework for cybersecurity, while creating a national framework of action relying on the four major pillars identified by INTERPOL: enhancing cybercrime intelligence for effective response, strengthening cooperation for joint operations against cybercrime, developing regional capacity and capabilities to combat cybercrime and promoting good cyber hygiene for safer cyberspace (INTERPOL, 2020).

References

Bellasio, J., Flint, R., Ryan, N., Sondergaard, S., Monsalve, C. G., Meranto, A. S., & Knack, A. (2018). *Developing Cybersecurity Capacity: A proof-of-concept implementation guide*. https://doi.org/10.7249/RR2072

CCDCOE. (2021). *CCDCOE*. https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-

norms-of-behaviour-highlighting-aspects-of-international-law/

CGTech. (2021). *The Importance of Cyber Security Awareness | CyberGuard Technologies*. CyberGuard Technologies Limited. https://www.ogl.co.uk/the-importance-of-cyber-security-awareness

Cisco. (2019). *Cisco Digital Readiness 2019*. https://www.cisco.com/c/m/en_us/about/corporate-social-responsibility/research-resources/digital-readiness-index.html#/country/KHM

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

Corrado, R., Khat, S., & Nhean, P. V. (2021). The Role of Cambodian Universisties in Preparing Cambodia for a Digital Economy. In R. Weiß & R. Hör (Eds.), *Digitalization and Sustainable Development* (pp. 76–84). Konrad Adenauer Stiftung, Cambodia. https://www.kas.de/en/web/kambodscha/single-title/-/content/digital-insights-2

Corrado, R., Pretorius, E., & van der Westhuizen, G. (2021). Undergraduate Students' Experiences of the Use of MOOCs for Learning at a Cambodian University. *Education Sciences*, *11*(7), 336. https://doi.org/10.3390/educsci11070336

Corrado, R., & Tungjan, P. (2019). Teachers' Motivation and Quality Education Represent the Key for the Change in Cambodia. *TICC International Conference Proceedings*. 4th Thailand International College Consortium Conference, Pattaya, Chonburi, Thailand.

Dupont, B., & Whelan, C. (2021). Enhancing relationships between criminology and cybersecurity. *Journal of Criminology*, *54*(1), 76–92. https://doi.org/10.1177/00048658211003925

FBI. (2021). *Business Email Compromise*. Federal Bureau of Investigation. https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise

FireEye. (2018). *Cyber Evolution: En Route to Strengthening Resilience in Asia-Pacific*. https://www.fireeye.com/offers/wp-cyber-evolution-apac.html

Heuer, R. J. (1999). *Psychology of intelligence analysis*. Center for the Study of Intelligence, Central Intelligence Agency.

INTERPOL. (2020). *ASEAN Cyberthreat Assessment 2020*. INTERPOL Global Complex for Innovation. https://www.interpol.int/en/content/download/14922/file/ASEAN_CyberThreatAssessment_2020.pdf?inLanguage=eng-GB

INTERPOL. (2021). *ASEAN Cyberthreat Assessment 2021*. INTERPOL Global Complex for Innovation. https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-charts-top-cyberthreats-in-Southeast-Asia

ITU. (2018). *Guide to developing a national cybersecurity strategy*. International Telecommunication Union. https://www.itu.int:443/en/myitu/Publications/2020/02/28/15/28/Guide-to-developing-a-national-cybersecurity-strategy---Strategic-engagement-in-cybersecurity

Kearney. (2018). *Cybersecurity in ASEAN: An Urgent Call to Action*. Kearney. https://mngdp.sang.gov.sa/wp-content/uploads/2021/04/Cybersecurity-in-

ASEAN%E2%80%94An-Urgent-Call-to-Action.pdf

Lim, M., & Sek, S. (2020). Cyberwarfare and Its Implications for Cambodia. *AVI Perspective*, *2020*(1). https://asianvision.org/archives/publications/avi-perspective-issue-2020-no-01

NCSC. (2018). *Phishing attacks: Defending your organisation*. https://www.ncsc.gov.uk/guidance/phishing

NCSI. (2021). *NCSI Ranking*. https://ncsi.ega.ee/ncsi-index/?type=c

Nguon, S., & Srun, S. (2019). Cambodia v. Hackers: Balancing Security and Liberty in Cybercrime Law. In *E-Governance in Cambodia* (pp. 76–95). Konrad-Adenauer-Stiftung, Cambodia. https://www.kas.de/en/web/kambodscha/single-title/-/content/how-digital-tech-can-help-fix-cambodia-s-broken-education-and-healthcare-systems

Norton. (2021). *Good cyber hygiene habits to help stay safe online*. https://us.norton.com/internetsecurity-how-to-good-cyber-hygiene.html

Nouh, M., Nurse, J. R. C., & Goldsmith, M. (2016). Towards Designing a Multipurpose Cybercrime Intelligence Framework. *2016 European Intelligence and Security Informatics Conference (EISIC)*, 60–67. https://doi.org/10.1109/EISIC.2016.018

Palo Alto Networks. (2021). *What is a Botnet?* Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-botnet

Sood, A. K., & Enbody, R. J. (2013). Crimeware-as-a-service—A survey of commoditized crimeware in the underground market. *International Journal of Critical Infrastructure Protection*, *6*(1), 28–38. https://doi.org/10.1016/j.ijcip.2013.01.002

Van Raemdonck, N. (2021). *Cyber Diplomacy in Southeast Asia*. Vrije Universiteit Brussels. https://eucyberdirect.eu/wp-content/uploads/2021/05/dd-southeast-asia-nb-fb-nvr-09-05.pdf

Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*, *128*, 113160. https://doi.org/10.1016/j.dss.2019.113160

Cambodia Development Center
Cambodia Development Center (@cd.centerkh)
Cambodia Development Center
Cambodia Development Center (t.me/cdcenterkh)
Building E, University of Puthisastra, #55, Street 180-184, Sangkat Boeung Raing, Khan Daun Penh
info@cd-center.org | (+855) 10 950 456 www.cd-center.org

មជ្ឈមណ្ឌលអភិវឌ្ឍន៍កម្ពុជា
Cambodia Development Center