TALLINN UNIVERSITY OF TECHNOLOGY
Faculty of Social Sciences
Tallinn Law School

Somaly Nguon

Cambodia's Effort on Cybersecurity Regulation:
Policy and Human Rights' Implications

Master Thesis

Supervisor: Agnes Kasper, PhD.
Tanel Kerikmäe, PhD.

Tallinn 2017

I hereby declare that I am the sole author of this Master Thesis and it has not been presented to any other university of examination.

Somaly Nguon

“ .....” 2017

The Master Thesis meets the established requirements

Supervisor: Agnes Kasper, PhD.,
Tallinn Law School,
Tallinn University of Technology, Tallinn, Estonia.

“ .....” 2017

Tanel Kerikmäe, PhD**.,**
Tallinn Law School,
Tallinn University of Technology, Tallinn, Estonia.

“ .....” 2017

Accepted for examination “ .....” 2017

Board of Examiners of Law Master’s Theses

……

Table of Contents

List of Abbreviations

ICT	Information and Communication Technologies
IT	Information Technology
SNWs	Social Networking Websites
MPTC	Ministry of Post and Telecommunication
RGC	Royal Government of Cambodia
NiDA	National ICT Development Authority
CamCERT	National Cambodia Computer Emergency Response Team
GAIS	Government Administration Information System
EAS	Electronic Approval System
ITU	International Telecommunication Union
ASEAN	Association of Southeast Asia Nations
APEC	Asia-Pacific Economic Cooperation
EU	European Union
UN	United Nations
CCHR	Cambodia Center for Human Rights
NGOs	Non-governmental Organizations
OECD	The Organization of Economic Corporation and Development
OpTPB	Operation The Pirate Bay
CCDCOE	Cooperative Cyber Defense Center of Excellence
DDoS	Distributed Denial of Service
NACC	National Anti-Cybercrime Committee
UDHR	Universal Declaration on Human Rights
ICCPR	International Covenant on Civil and Political Right
ICESCR	International Covenant on Economic Social and Cultural Rights

List of Figures

Introduction

Information and communication technologies (ICTs) and the trend toward digitalization are growing. The advancement of Information Technology (IT) and the expansion of the Internet have an unexpectedly useful service serving as a kind of laboratory for research, governance, intergovernmental institutions, social and economical development, as well the ability to disseminate information across the globe.[1] Moreover, the growth of online digital media enables us to communicate easier, enjoy free flow of information sharing, and exercise freedom of expression via Social Networking Websites (SNWs), such as personal blog, Facebook and Twitter, etc.[2]

The growing of modern technologies is an advantage for the betterment of human being, yet it also creates a concern in relation to security in cyberspace. New technologies, computer and Internet originate new trend of crime. This means that computer functions such as software programs and Internet capabilities can be manipulated to conduct criminal activities in cyberspace. A person is capable of conducting criminal activities by just sitting in front of computer and using Internet to attack on other computer's system. This kind of criminal activity is being known as "Cybercrime". According McDowell, M. and Householder, A. (2015), "as long as you have a computer and connect it to a network, you are vulnerable to someone or something else accessing or corrupting your information".[3]

Cambodia is one of the developing countries in ASEAN. Indifferent from other countries, the nation is also a victim of cybercrime. Cambodian population is around 15.82 million while 68% of the total population is under 30 years old.[4] The Cambodian Genocide was carried out by Khmer Rouge regime led by Pol Pot between 1975 and 1979 in which an estimation of more than two million people died and most of the infrastructures were destroyed. Until 1993, Cambodia was transformed to be a democratic country and held its first national election.[5] The majority of Cambodian people are low educated and also lack access to information, which can

[1] Marsoof, A. Online Social Networking and the Right to Privacy: The Conflicting Rights of Privacy and Expression.
[2] Ibid.
[3] McDowell, M. Householder, A. Good Security Habits. What is Cyber Security? Blimline, B. (Ed.). Today's Insurance Professionals 2016, 73 (1), p 14. Available at: http://c.ymcdn.com/sites/www.internationalinsuranceprofessionals.org/resource/resmgr/Today_s_Insurance_Professionals_magazine/Spring2016_Mag_FINALWEB.pdf (20.12.2016)
[4] UN, World Statistics Pocketbook:Cambodia. Available at: http://data.un.org/CountryProfile.aspx?crName=Cambodia (12.10.2016)
[5] Kong, P. Overview of the Cambodian Legal and Judicial System. Introduction to Cambodian Law. Hor, P., *et al* (Eds.). Phnom Penh, Konrad-Adenauer-Stiftung 2012, p 7-8.

help them make a rational decision.

In the last few years, Cambodia has achieved significant progress in promoting the use of ICT to improve the administration system and service to citizens and entrepreneurs.[6] However, the country is lagging far behind technology development, and the policy area concerned with the regulation of online behavior is a profound implication for essential human rights such as privacy, freedom of expression and information in an interconnection era. Current legislation fails to keep pace with digital development that severely threatens the fundamental human rights.[7]

The Cambodian government announced in 2012 that it was in the process of drafting Cambodia's Cybercrime law, which Internet community fears that it could extend traditional media restraint online.[8] After the announcement was made, a hacker group called NullCrew launched its campaign named Operation The Pirate Bay (OpTPB) to attack Cambodian websites in protest of Internet censorship and the arrest of Gottfrid Svartholm Warg, the 27-years old co-founder of torrent sharing site The Pirate Bay. OpTPB targeted several websites of Cambodian businesses and government organizations, including the armed force. As result, OpTPB leaked highly confidential information and posted a number of passwords for other hacktivist groups to use. Another hacktivist collective, Anonymous, also instigated a cyber war against Cambodia in protest of the arrest of Warg. Over 5,000 documents were successfully stolen and leaked from Cambodia's Ministry of Foreign Affairs.[9] Followed the above incidents, the Cambodian government announced new law requiring surveillance cameras in the Internet cafes. The law has mandated that all Internet cafes and telephone centers install surveillance cameras and retain footage for at least three months.[10]

Cambodia's Ministry of Post and Telecommunication (MPTC) reported Internet penetration in Cambodia increased from 20 thousands in 2008 to over 7.16 million by June 2016, around 46%

---

[6] Cheang, S., Sang, S. Sate of Cybersecurity and the Roadmap to Secure Cyber Community in Cambodia. International conference on availability, reliability and security, IEEE 2009. pp 652-657, p 652. doi: 10.1109/ARES.2009.144

[7] Freedom House, Freedom on the Net: Cambodia, Report 2013, p 8-9. Available at: https://freedomhouse.org/sites/default/files/resources/FOTN%202013_Cambodia.pdf (26.09.2016)

[8] Ibid.

[9] YMAC, Security: How can we enhance cybersecurity in ASEAN? Youth Model ASEAN Conference 2016, p 2. Available at: http://www.sp.edu.sg/ymac/documents/securitycybersecurity.pdf (20.09.2016)

[10] Mong Palatino, "Cambodia: Mandatory Internet Surveillance Cameras", Global Voice, 09.12.2012. Available at: https://globalvoices.org/2012/09/09/cambodia-mandatory-internet-surveillance-cameras/ (20.09.2016)

of the total population of around 15.82 million.[11] Cambodia is currently known as a home to the largest youth and adolescent population in the South East Asia region, and they are active on social media, particularly Facebook. Social media agency in Singapore has released an infographic on the digital statistical indicators that number of active social media users in Cambodia increased from 3.4 million in 2016 to 4.9 million in 2017.[12]

Civil societies expressed concerns that leaked draft law on cybercrime has begun to threaten the freedom on Internet through its broad terms used under Article 28 of the drafted law. Under Article 28 of the draft law regulates the users' expression behavior regarding content and websites. People who "establish contents deemed to hinder sovereignty and integrity of the country or government agencies and ministries, incite or instigate, generate insecurity and political cohesiveness, and damage the moral and cultural values, etc. are punishable from one to three years imprisonment and fine from five hundreds U.S. dollar to one thousand and five hundreds U.S. dollar (500-1500$)".[13]

ICT development in Cambodia is still at the crucial stage comparing to other countries in the region. Cambodia has one of the lowest Internet connectivity rate in Southeast Asia according to Information Society Statistical profile in Asia Pacific published by International Telecommunication Union (ITU) in 2009.[14] National ICT Development Authority (NiDA) was in charge of ICT development of Cambodia, has been integrated into MPTC's structure. The National Cambodia Computer Emergency Response Team (CamCERT) was established in December 2007 in order to deal with cybersecurity and cybercrime matters. There is also Cybercrime Unit in the National Police department in charge of telecommunication crime. Cambodia left over many important tasks concerning securing cybersecurity according to Cyber willingness profile published by ITU in 2014.[15] Cyberwellness in Cambodia has been discussing in a small circle among scholars because it is seems to be new topic in this small and less developed country.

---

[11] MPTC, Fact Sheet on Telecommunication Sectors. June 2016. Available at: http://www.mptc.gov.kh/site/detail/607 (10.01.2017)
[12] Joseph Soh, "Cambodia's 2017 Social Media and Digital Statistics", Geeks 09.02.17. Available at: http://geeksincambodia.com/cambodias-2017-social-media-digital-statistics/ (14.02. 2017)
[13] Article 19, Cybercrime Law, Draft V.1, unofficial translation to English, Art.28. Available at: https://www.article19.org/data/files/medialibrary/37516/Draft-Law-On-CyberCrime_Englishv1.pdf
[14] ITU, Information Society Statistical Profile Asia and the Pacific, 2009. p 17. Available at: http://www.itu.int/ITU-D/ict/material/ISSP09-AP_final.pdf (26.09.2016)
[15] ITU, Global Cybersecurity Index & Cyberwellness Profiles. 2015. p 117-118. Available at: http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf (26.09.2016)

This research aims to study on Cambodia's effort in combating against cyberthreats; should Cambodia have this particular cybercrime law. Does the current draft law address the cyber threats? Whether it is necessary and proportionate? This research also aims to propose international good practices that could be taken into account and suggest some concrete steps that the Royal Government of Cambodia (RGC) may consider implementing for a better development in combating against cyber threat and serve the best interest of online community in Cambodia.

This research will focus on the analysis of RGC's current effort regarding cybersecurity regulation and policy that will play the important part in the context of Cambodia. Moreover, this research will include comparative study and discussion on international and regional legislation cooperation in combating against cybercrime. In addition to discussion on the process of drafting cybercrime law, this thesis will also concentrate on the controversial issues concerning human rights obligations and freedom in cyberspace. In order to achieve the aim of this research, the author have to answer to main research questions as following:

- **What are the main components of Cambodia's cybersecurity policy and how it was developed?**
- **Is the draft law on cybercrime in the line with the international human rights obligations of Cambodia?**

Critical review of legislation and policy documents, comparative study of the policy processes, and analysis of the case law will be used as research methodology for this research. The qualitative method has been used in order to describe and analyze for an improvement of the controversy-drafted law on cybercrime in Cambodia. This research is achieved by conducting extensive desk research, and the collection of documents and data based on the basic literature on policy and strategy of cooperation, legal sources, relevant statistic, reports from NGOs, presentation, speeches, including press media released.

In order to create the critical analysis and logical flow in this thesis, the author divided the research into four main chapters. The first chapter will define the cybercrime in the context of Cambodia including the categories of crime in cyberspace, while the introduction to ICT development and other relevant statistics is presented in the introduction part. Cybercrime has been defined differently in different legal systems. No act is considered as crime unless the law

prescribes it. Most of the categories of cybercrime are still beyond the reach of law.[16] Therefore, understanding of the scope and nature of cybercrime in Cambodia is very important because the specific law concerning this issue is still in the drafting process. Besides, this chapter will also identify what is perceived as a threat in cyberspace? And what are the responses to these threats?

There is no any common agreement on the definition of cybercrime, while various legal aspects are involved.[17] Therefore, second chapter going to discuss on the main elements of the current cybersecurity policy. Whether cybercrime can be accommodated within the existing legal framework or does it require other different measures? Cybercrime is a complicated interrelation aspect, which is difficult to control and govern through traditional legal system. In order to cope with such techno-sophisticated criminality, adoption of appropriate legislation and effective mechanism is needed. Domestic law alone cannot achieve in combating against the misuse of ICTs for criminal activities, regional and international legal cooperation is required to assist this process.[18]

Harmonized legal frameworks help developing countries to overcome challenges in combating against cybercrime. Developing countries need a better understanding of the national and international implications of growing cyber threats, to access the requirements of the existing national, regional and international instruments, and to assist countries in establishing a sound legal foundation.[19] Since the threats can originate anywhere around the globe, the challenges are intrinsically international in scope and necessitate international cooperation, investigative assistance, and procedural provision.[20] In this context, Cambodia is not quite different from another similar developing countries. Cambodian Criminal Code mentioned about cybercrime, but it fails to provide detail procedure and mechanism, while the controversial cybercrime law is still in the drafting process.

Chapter three is going to discuss on the international human rights aspects in cyberspace. We will look through the human rights obligation of the RGC and assess whether the draft law on cybercrime complies with these human rights standards or not. In order to accomplish this chapter, author will do the analysis on the fundamental human rights in cyberspace based on the

[16] Dalei, P., Brahme, T. Cyber Crime and Cyber Law in India: An Analysis. IJHAS 2013, 2(4) ISSN 2277-4386, pp 106-109, p 107-108.
[17] Chowbe, V. An Introduction to Cyber Crime: General Considerations. SSRN 2011, p 7-8. Available at: https://ssrn.com/abstract=1766234 (20.10.2016)
[18] ITU, Understanding Cybercrime: Phenomena, Challenges and Legal Response. 2012, p 2. Available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf (04.10.2016)
[19] Ibid, p 4.
[20] Ibid.

international legal instruments that Cambodia ratified and the implementation along with case studies.

Chapter four will be the comparative analysis based on the cybersecurity dimensions. Author will compare the Cambodian Practice to China, Japan and Singapore. The Standing Committee of China's legislature adopted the Cybersecurity Law on November 07, 2016, and the law will come into effect from June 01, 2017.[21] The newly passed China's Cybersecurity Law resulted in controversy discussion on the broadly framed defined terms and its direction toward a much more heavily regulated Chinese Internet and IT sector.[22] On the other hand, Singapore is a developed country and transforms into a smart nation in the region. Singapore has several Acts for the safeguard in the cyberspace including the Personal Data Protection Act, Telecommunication Act and Banking Act. Moreover, Singapore also has the Computer Misuse and Cybersecurity Act of 1993 and a revised edition in 2007.[23]

In addition to the existing acts, the Singapore Government announced that a new separate Cybersecurity Act will be tabled in Parliament in 2017 with the expectation that the new Act will institute standards for incident reporting, audits and risk assessments. The new Act will complement the existing computer Misuse and Cybersecurity Act, which will continue to govern cybercrime investigation in Singapore.[24] In this comparative study, author is going to analyze on the steps that Cambodia have skipped and what are the possible consequences? What should have been done for securing the cyberspace?

Based on the analysis of four chapters above, author will do the summary and propose concrete steps to redraft the law as appropriate in the conclusion part.

[21] Ron Cheng, "China Passes Long-Awaited Cyber Security Law", Forbes, 09.11.2016. Available at: http://www.forbes.com/sites/roncheng/2016/11/09/china-passes-long-awaited-cyber-security-law/#2653934b6868 (20.11.2016)
[22] New Comprehensive Chinese Cybersecurity Law Approved, Squire Pattion Boggs, 2016, p 1. Available at: http://www.squirepattonboggs.com/~/media/files/insights/publications/2016/11/New-Comprehensive-Chinese-Cyber-Security-Law-Approved/Comprehensive-Chinese-Cybersecurity-Law-Alert.pdf (10.01.2017)
[23] Tan, T. B. We, Cittizens of Smart Signapore: Data Protection in Hyper-connected Age. RSIS Commentaries, No. 036, 2016, p 1. Available at: http://hdl.handle.net/10220/40253 (10.01.2017)
[24] A Peek into Singapore's New Cybersecurity Act. Baker Mckenzie, 26.10.2016. Available at: http://www.bakermckenzie.com/en/insight/publications/2016/10/peek-into-the-new-cybersecurity-act/ (10.01.2017)

1. Overview of Cybersecurity

1.1. ICT Development in Cambodia

Global expansion of digital media, networks, and ICTs become new powerful technological revolution in the history of humankind. Due to the rapid pace of technology development, great expansion of Internet access, and the increase in the use of ICTs by private sector, business, communities, and governments around the world become the major piece of today's global economy and development.[25] Moreover, according to a research, the modern technology has provided a great assistance for the society as well.[26] However, vulnerabilities always come along with the enormous benefits created from dependency on networked ICTs due to lack of security measures and proper understanding of viable risks. Cybersecurity is the pressing and controversial topic in all national, regional and international level, while number of cyber attacks significantly increased.[27]

Cambodia is a less-developed nation in South East Asia with lowest Internet connection in the region. Researchers, policy makers, and international stakeholders have increasingly focused on how this small nation can use ICTs to most effectively bridge the global digital divide. Cambodia is a latecomer to the Internet with commercial service in 1997. Having the lowest Internet penetration in South East Asia as well as the highest price, in June 2001 the estimated number of Internet users in Cambodia was 8.000 equal to 0.07% of the total population. The MPTC functions as policy maker, regulator, and operator on the Cambodian Internet market. Until mid-2001 only four ISPs were operated in the country,[28] however the number of Internet subscribers steadily increased.

In the past few years, Cambodia has been enjoying significantly in the digital prospect. The continuing increase in the Kingdom's digital statistics is authentication to the country's thrust to embrace the digital age. Due to the expansion of Internet connection and competitive price among ISPs in the country, the total number of Internet subscribers notably increased from 20.000 in 2008 to over 7.16 million by June 2016, around 48% of the total population of around 15.82 million. The number of service providers in Cambodia's telecom market also improves,

[25] Kaper, A. The Fragmented Securitization of Cyber Threats. Regulating eTechnologies in the European Union. Kerikmäe, T. (Ed.). Springer 2014, p 157-159.
[26] Schwabe, W. Need and Prospect for Crime-fighting Technology: The Federal Role in Assisting State and Local Law Enforcement. Washington, D.C. Rand, 1999, p 2.
[27] Kasper (2014), *supra note* 25.
[28] ITU, Khmer Internet: Cambodia Case Study. 2002, p 13-16. Available at: http://www.itu.int/itudoc/gs/promo/bdt/cast_int/79475.pdf (20.10.2016)

where the operators expand their service to both urban and rural areas all over the country with a competitive price. This improvement contributes a lot to the country's development while 68% of the total population is under 30-year old. In 2016, there were 33-registered wired Internet services providers are operating in the Kingdom of Cambodia.[29] It is a huge difference in number if compared to 2001, where the ISPs were only four in the Kingdom.

Internet Subscribers	June 2016	Market Share (%)
Internet Mobile	7, 074,483	98,81
Wired Internet	82,926	1.16
Total	**7,157,409**	**100**

Figure 1. Internet subscribers and market share in June 2016.[30]

No.	Services	Operators
1	Mobile	9
2	Fixed Line	9
3	ISPs	33
4	VOIP	22
5	DNS (.kh)	2,844
6	Internet Cafe	217

Figure 2. Cambodia's Telecom Market in June 2016.[31]

1.1.1. E-Application: The Development Dilemma

E-applications have the great potential contribution to the country's development and are considered as the backbone of the economic, especially smart countries. E-government, e-

[29] MPTC, Fact Sheet on Telecommunication Sectors. *Supra note* 11.
[30] Ibid.
[31] Ibid.

commerce, e-education, and e-health play important roles to enhance the economic growth, democracy and social evolvement. As one of the least developed countries, Cambodia face many challenges for transforming this country into e-country. Integrate ICTs into country development plan is not an easy task for Cambodia, because there are numbers of impediments including: poverty, poor infrastructure, weak institution, and low levels of literacy and ICT awareness. [32]

Estonia is a good case study when we want to do analysis on how e-application work in the development sector. Estonia startled the world when this country launches it e-service by issuing e-residencies.[33] Estonia embraces with its advance e-government service and gets more attention from other countries outside EU as well. Around 95% of Estonian sign documents digitally by using active ID-card, 96% of taxpayers declared their taxes through electronic, and 99.6% of the bank transactions are being done online.[34] Through above example, we clearly see how tremendously important ICTs sector is to this country.

1.1.1.1. E-Government

Integrating ICTs into government infrastructure will create friendly environment for citizens to participate in the political activities, improve transparency and governance accountability, cost saving, attract more investors to the country and motivate the innovation. ICTs solution for facilitating the governance at different levels has been developed over the past decade. When we discuss e-government, it is not only referred to the information available on the government websites, but also referred to ICTs solution to assist administrative works such ICTs tools, programs and other strategies, which enables an easier access to the services than the traditional public administrative one. According to European Union, Electronic Government or E-Government refers to *"e-government uses digital tools and systems to provide better public services to citizens and business"*.[35]

Cambodia faces a number of barriers in transforming the process in to e-Government as its public sectors still experience corruption and poor public administration, and lack adequate transparency and accountability in the exercise of public decision-making as well as the delivery

[32] ITU, Khmer Internet: Cambodia Case Study. 2002. *supra note* 28. p 22.

[33] Kerikmäe, T. Särav, S. E-Residency: A Cyberdream Embodied in a digital Identity Card? The Future of Law and eTechnologies. Kerikmäe, T. Rull, A. (Eds.). Springer 2016, p 57-58.

[34] Ibid.

[35] Nyman-Metcalf, K. e-Government in Law and by Law: The Legal Framework of e-Government. Regulating eTechnologies in the European Union. Kerikmäe, T. (Ed.). Springer 2014, p 33-35.

of the public service.[36] E-government aims at overcoming economic, social, and environmental challenge, which will lead to a more open and flexible collaboration between citizens and government agencies; subsequently increase the efficiency and effectiveness of the service. In order to achieve e-government implementation, introducing new technologies, operational model for information system, cloud computing, and other systematic cooperation are extremely important.[37] Some examples of e-government application includes e-voting, e-residency, and e-signature, etc.[38]

RGC introduced it e-Government project in 2002, which comprised of several programs, such as Government Administration Information System (GAIS) and other cyber system for financial, banking and custom.[39] The GAIS involves four practical applications: an electronic approval system (EAS), a vehicle registration system, a resident registration system, and a real estate registration system. EAS allow the ministries to exchange documents both internally and externally, which cut down unnecessary delays and result in better public service.[40] This process requires more technical solution and experts. Therefore, a successful e-government implementation needs a greater cooperation between public and private partnership.

1.1.1.2. E-Commerce

E-commerce is not widely used in Cambodia due to the limited capacity of electronic facilities and knowledge on how ICTs works for the business transaction. Another reason why e-ecommerce is not popular because of the lack of trust in the system, and there is no specific law to guarantee the safeguard of election traction yet. Cambodian enjoys traditional business transaction (face to face offer and acceptance culture) to endure that it is 100% success. E-commerce has been defined as "the sharing of business information, maintaining business relations, and the conducting business transactions by mean of telecommunication networks". [41]

Different types of IT sectors covering to create the discipline of e-commerce include electronic

---

[36] Sang, S. et al. E-government adoption in Cambodia: a partial least squares approach. Transforming Government: People, Process and Policy 2010, 4 (2), pp 138-157, p 38-139. DOI 10.1108/17506161011047370 (05.02.2016)

[37] Zissis, D. Lekkas, D. Securing e-Government and e-Voting with an open cloud computing architecture. Government Information Quarterly 2011, 28 (2), pp 239-251, p 139-141. Doi:10.1016/j.giq.2010.05.010 (25.11.2016)

[38] Kerikmäe (2016), *supra note* 33.

[39] Cheang (2009), *supra note* 6.

[40] Sang (2010), *supra note* 36.

[41] Zwass, V. Electronic Commerce and Organizational Innovation: Aspects and Opportunities. International Journal of Electronic Commerce 2003, 7 (3), pp 7-37, p 8. Available at: http://www.jpedia.org/ijecnew/zwass-20031.pdf (15.12.2016)

message, email and fax, sharing a corporate digital library, electronic document interchange utilizing EDI and electronic fund transfer. Electronic publishing to promote marketing, advertising, sale, and customer support are also in the category of e-commerce. The e-commerce activities keep increasing due to the expansion of Internet and innovation of new technologies and ICTs tools. E-commerce activities in Cambodia also increase in the last few years because large number of Cambodian young people are active online and would bring a lot of business opportunities for young entrepreneurs in Cambodia and contribute to economic growth in the country. Cambodia has been drafting the E-commerce law to facilitate and regulate online business operation for investors and customers. [42]

In order to keep pace with social and economic development during the ASEAN integration, harmonization of law is extremely important. The progress toward harmonization has been the strongest in the area of electronic transaction law and cybercrime law. For the time being, 9 out of 10 member states in ASEAN now having electronic transaction legislation in place. Cambodia has not yet passed electronic transaction legislation, however draft law has been developed. Cambodia and the Lao People's Democratic Republic do not have cybercrime law, while other 8 members enacted this legislation.[43] According to the review on status of e-commerce law harmonization in ASEAN, Cambodia demonstrates the slowest legislation process.

Member Country	Electronic Transactions	Privacy	Cybercrime	Consumer Protection	Content Regulation	Domain Names
Brunei Darussalam	Enacted	None	Enacted	Partial	Enacted	Enacted
Cambodia	Draft	None	Draft	None	Draft	Enacted
Indonesia	Enacted	Partial	Enacted	Partial	Enacted	Enacted
Lao People's Democratic Republic	Enacted	None	None	Draft	Enacted	Partial
Malaysia	Enacted	Enacted	Enacted	Enacted	Enacted	Enacted
Myanmar	Enacted	None	Enacted	Enacted	Enacted	Enacted
Philippines	Enacted	Enacted	Enacted	Enacted	None	Enacted
Singapore	Enacted	Enacted	Enacted	Enacted	Enacted	Enacted
Thailand	Enacted	Partial	Enacted	Enacted	Partial	Partial
Viet Nam	Enacted	Partial	Enacted	Enacted	Enacted	Enacted

Figure 3. Status of e-commerce law harmonization in ASEAN as of March 2013.[44]

[42] Tian Shoahui, "Cambodia drafts E-commerce as online sale grow", Xinhua 06.11.2016. Available at: http://news.xinhuanet.com/english/2016-11/06/c_135809717.htm (10.01.2017)

[43] UNCTA, Review of e-commerce legislation harmonization in the Association of Southeast Asian Nations, 2013, p 5. Available at: http://unctad.org/en/publicationslibrary/dtlstict2013d1_en.pdf (25.11.2016)

[44] Ibid.

1.1.1.3. E-Education

While Cambodia is known as a home to the largest youth and adolescent population in the South East Asia region, it is also one the least educated population in the world. This resulted from the Khmer Rouge period where around 90% of Cambodians with a secondary or higher education were killed or fled the country.[45] Cambodia face many challenges in integrating ICT into educational system. In 2004, ICTs Policy and Strategy for education was adopted by Cambodian Ministry of Education, Youth, and Sport (MoEYS) with the support from UNESCO. The main aims for this ICT in education policy included: increased access to basic education for all using ICT as major tool; improved quality of basic education; and the creation of a workforce eligible to participate in the global knowledge-based economy.[46]

E-education or E-learning refers to the application of IT to the delivery of learning experiences. E-education takes place in formal electronic classroom, on corporate intranets used for just-in-time training, audio and video teleconferencing and in a variety of other technology-mediated learning space. E-education can be conducted in the form of Web-based learning, computer-based learning, virtual classrooms, and other digital collaboration.[47] Due to limitation of skill, knowledge, facilities and financial shortage, e-learning is not widely applied in Cambodia. We found some practices exist in higher education level such as university and private school.

The first e-Learning center appeared in Cambodia in 2012 under the support from Korean International Cooperation Agency (KOICA), with the outputs of one-million-USD project called "Strengthening CLMV Capacity for ASEAN Cyber University in Cambodia". This project was implemented in parallel with other three projects in Laos, Myanmar, and Vietnam in order to build the capacity of Cambodia's human resource through ASEAN Cyber University and the establishment of the E-Learning center. Another objective is to contribute to narrowing the digital technology gap, and enhance ICT cooperation among ASEAN member states.[48]

---

[45] ITU, Khmer Internet: Cambodia Case Study. 2002. *supra note* 28. p 22.
[46] Richardson, J. ICT in Education reform in Cambodia: Problems, Politics, and Policies Impacting implementation. The MIT Press 2008, 4 (4), pp 67-82, p 67-68. Available at: http://itidjournal.org/itid/article/viewFile/311/143 (25.11.2016)
[47] Weippl, E.R. Security E-Learning. New York, Springer 2005. p 6.
[48] KOICA, "The First e-Learning Center Appears in Cambodia", KOICA 04.05.2012. Available at: http://www.koicacambodia.org/the-first-e-learning-center-appears-in-cambodia/ (20.01.2017)

1.1.1.4. E-Health

According to WHO, e-Health is *"the use of information and communication technologies (ICTs) for health".*[49] The e-Health unit works with partners at the global, regional and country level to promote and strengthen the use of information and communication technologies in health development, from applications in the field to global governance. WHO's work in e-Health includes programs and projects in areas such as policy and governance, standardization and interoperability, research and global surveys, e-learning and capacity building, networking and South-to-South collaboration, as well as e-Health applications.[50]

Cambodia established it first ever Health Information System Strategic Plan (HISSP) in 2008. 2008-2015 HISSP covers five main HIS components include: i) HIS policy and resource, ii) data management and use, iii) health and disease records including surveillance, iv) census, civil registration, and population based surveys, v) health service administration and support system.[51] Application of ICTs into health sector is a big challenge in Cambodia. The national e-Health strategy and e-Health system does not exist, except HISSP 2008-2015.[52] The most important barriers hindering the implementation of e-Health services in Cambodia are governance and policy, infrastructure, human resources, and financial.[53]

Cambodia does not include e-Health as an approach to support women and children's health. Moreover, infrastructure is not yet adequate, accessible, or cost-effective to support desired services. Cambodia also lacks of experienced and suitably qualified human resource that can develop and implement e-Health project and promote their use. There is no ICT training for student of health science or education in ICT for health professionals. Besides, the approaches to ensure quality of the health-related content on the Internet, child protection in the online environment, legislation to secure privacy and security of personal and health-related data does note exist. Social media are popular in this country, however not many of active social media

---

[49] WHO, eHealth: The health data ecosystem and big data. Available at: http://www.who.int/ehealth/en/ (10.01.2017)
[50] Ibid.
[51] MoH, Health Information System Strategy Plan 2008-2015, 2008, p 5. Available at: http://www.hiscambodia.org/public/fileupload/HISSP_ENG.pdf (20.01.2017)
[52] WHO, eHealth Country Context Indicators: Cambodia, 2016. Available at: http://www.who.int/goe/publications/atlas/2015/khm.pdf?ua=1 (20.01.2017)
[53] WHO, Survey on eHealth and Innovation in Women's and Children's health: Cambodia, 2013. p 22-23. Available at: http://www.who.int/goe/publications/atlas/2013/khm.pdf (20.01.2017)

users use it health education or awareness.[54]

1.1.2. Define Cybersecurity

The term "Cybersecurity" was first used by computer scientist in the early 1990s to underline the series of insecurities related to networked computers. The term become widely used beyond a mere technical conception of computer security when threats arising from digital technology in the cyberspace.[55] Cybersecurity has been defined by ITU as *"the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, action, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets"*. [56] Or as "*the prevention of damage to, unauthorized use of, exploitation of, and the restoration of electronic information and communication systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems*".[57]

Technologies development originates the new trend of crime in cyberspace. Cybercrime keeps rising, and the amount of economy loss is even bigger than the black market of the global drug trafficking. The global cybercrime is known as the biggest underworld industry that cause US$1 trillion loss worldwide annually.[58] There is a huge gap between law and technology in the twenty-first centuries. According to McDowell, law and ethic are both normative systems prescribing guideline on how people ought to live their lives. And people are not always legal or ethical in their behavior. Therefore, people need more responsible sense of their action. They have to consider whether what benefits them also benefits other people or cause possible harms. How big is the harm could be?[59]

There are different understandings on the concept of cybercrime and define differently depending on the purpose of using that term. Cybercrime can be defined as *"any illegal behavior directed by means of electronic operations that target the security of computer systems and the*

---

[54] Ibid
[55] Hansen, L. Digital Disaster: Cyber Security, and the Copenhagen School. International Study Quarterly 2009, 53, pp 1155-1175, p 1155. Doi:10.1111/j.1468-2478.2009.00572.x (20.10.2016)
[56] ITU, Overview of Cybersecurity. Recommendation ITU-T X. 1205. 2008. p 2. Available at: https://www.itu.int/rec/T-REC-X.1205-200804-I (20.10.2016)
[57] ITU, Report on best practice for a national approach to cybersecurity: A management framework for organizing national cybersecurity efforts. ITU-D secretariat draft, 2008. p 5. Available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf (20.10.2016)
[58] Gruodyte, E., Bilus, M. Investigating Cybercrimes: Theoretical and Practical Issues. Regulating eTechnologies in the European Union. Kerikmäe, T. (Ed.). Springer 2014, p 218.
[59] McDowell, B. Ethic and Excuses: The Crisis in Professional Responsibility. United States, Quorum Books 2000, p 13-16.

data processed by them".[60] On the other hand, the term can be described as "computer-related acts for personal or financial gain or harm, including forms of identity-related crime and computer content-related acts".[61] There are number of questions has been asked concerning the relationship between law and technology development. The purposes of law are to maintain the public order security, morality and respect the fundamental principle safeguarding the dignity and integrity of a person. However, traditional legal system failed to keep pace with new technology and ITCs that have made all kind of things possible that were impossible, or unimaginable in an earlier age[62] such as new trend of crime 'cybercrime'.

The evolution of computers and information systems have given rise to novel controversies regarding boundaries and obligations, intellectual property rights, privacy rights, diplomatic relations and military affairs, critical infrastructure, and the public welfare. It is true or whether the technology reaches advance level, the ethical issue goes down? Ethical issue is not only concern how individual should treat one another, but also the about how to regulate the regulation that fits with swift technology development today.[63] Cybercrime is one of the most serious threats to economic and national security around the world. The volume of data breaches, mostly consisting of hacking and malware, is at the highest level ever. Highly confidential information is stolen and leaked causing significant legal and ethical concerns.[64]

1.1.3. How Cambodia Defines Cybercrime?

As we are simply understood that cybercrime refers to a computer-related crime because cybercrime is commit through a computer network.[65] In order to secure the cyberspace from any threats, the specific regulations and mechanisms dealing with cybercrime is needed. There are variations of names for Cybercrime law in different legal systems. For example, Cybercrime law is being called "Computer Misuse Act"[66] in Singapore. On the other, in China cybercrime law is being called "Cybersecurity Law" after The Standing Committee of China's legislature passes

[60] Gruodyte (2014), *supra note* 58, p 226-227.
[61] Ibid.
[62] Brownsword, R., Goodwin, M. Law and the Technology of the Twenty-first Centur. Cambridge University Press, 2012. p 8.
[63] Harrington, S. Professional Ethics in the Digital Forensics Expert: Ultimate Tag-Team or Disastrous Duo? William Mitchell L. Rev. 2011, 38 (1), pp 353-396, p 2. Available at: http://open.mitchellhamline.edu/wmlr/vol38/iss1/8 (15.11.2016)
[64] Ibid.
[65] Hassan, A. et al. Cybercrime in Nigeria: Causes, Effects and the Way out. ARPN Journal of Science and Technology 2012, 2 (7), pp 626-631, p 626. Available at: http://www.ejournalofscience.org/archive/vol2no7/vol2no7_11.pdf (20.10.2016)
[66] Tan (2016), *supra note* 23.

this law on November 07, 2016, and the law is effective from June 01, 2017.[67]

Cybercrime is not a new issue in Cambodia, since 2002 Government websites have been vulnerable to technical violence in the form of cyber attacks.[68] Several of Government websites targets in 2012 and 2013 included Ministry of Foreign Affair, National Election Committee, National Police, Military and Supreme Court. Thousands of government documents including official personnel expense records, details of lost Cambodian passports, and law enforcement exchange with Cambodian-based embassies and consulates leaked online by the hacktivist collective Anonymous.[69] However, not many Cambodian including the netizens in the country understand what cybercrime really is.[70]

For the last few years more Cambodian gaining access to the Internet and now the current the Cybercrime Law is in the drafting process by RGC in order to control the Internet activities. The computer related offences were introduced for the time in the Cambodian Criminal Code 2009 from Article 317-320 and 427-432. The Criminal Code of the kingdom of Cambodia introduces very general terms on computer related crime as "Offences in information technology sector".[71] There is no specific definition on the terms in the cyber offense or specific categories of cybercrime and mechanism found in this legislation. Criminal Code alone cannot secure the nation from cyber threats and impose appropriate punishment on cyber criminal.

The main challenge in Cambodian traditional legal system is the denial of potential abuses of new technologies and necessary amendments to the national criminal law. This challenge remains as relevant and topical as ever as the speed of network innovation accelerates. Some other legal systems do not criminalize the access itself, but only when perpetrator has harmful intentions to obtain, modify, and damage accessed data.[72] Opponents to criminalization of illegal access refer to situations where no dangers were created by mere intrusion, or where acts of "hacking" have led to the detection of loopholes and weakness in the security of targeted computer systems.

In order to keep pace with technology trend, the RGC puts more effort on the legal framework for the ICTs safeguard. As a result, the government announced in 2012 that it was in the drafting

[67] Ron Cheng. "China Passes Long-Awaited Cyber Security Law", 2016, *supra note* 21.
[68] Freedom House, Freedom on the Net: Cambodia 2013, *supra note* 7. p 10.
[69] Ibid
[70] ITU, Global Cybersecurity Index & Cyberwellness Profiles. 2015, *supra note* 15.
[71] Criminal Code of the Kingdom of Cambodia, No.NS/RKM/1109/09, September 30, 2009.
[72] ITU, Understanding Cybercrime: Phenomena, Challenges and Legal Response. 2012, s*upra note* 18, p 179.

process. Unfortunately, the leak of Cambodia' draft law on Cybercrime became the controversial topic between government and civil society concerning the development of Cambodian online community. The drafted law on Cybercrime turns Free Speech into Cybercrime under the Article 28.[73] The controversies Article has no input from civil society lack of transparency and secrecy, which has strict limits on the content. The government uses existing criminal defamation and incitement laws to limit freedom of expression, which allows the government to have free reign to stifle speech online and lock down any political dissenters integrated into Article 28 of the draft law.[74]

1.2. What perceived as threats in cyberspace?

1.2.1. Cybersecurity Actors

There are multi-cyber actors who perceived as threats in the cyberspace with different behavior and motivation behind their attack. According to Alexander Klimburg, cybersecurity actors divided into three major groups includes: State Actors, Organized Non-State Actors, and Non-Organized Non-State Actors.[75] Hacking without permission and authorization is considered illegal.

Cybercrimes and attacks are not new in Cambodia, but the level of understanding of this issue is still low among Internet users. As mentioned earlier, hacker groups have targeted several government websites since 2002. There were several reports on malicious viruses, and scam and fraud mail from the Internet users, and also the efforts of ambitious local hackers showing their strength, but mostly they have gone unnoticed and unpunished. Internet cafes have been major source of virus spread in Cambodia, due to limitation of cybersecurity measure.[76]

People usually have misconception about the term hacker, whether we describe them as a malicious or a skilled expert pushing technology. According to Gross, *"Hacker is anybody looking to manipulate technology to do something other than its original purpose".*[77] Given the number of high profile data theft, sever compromises, and stolen passwords, it is easy to see how

[73] Article 19, *supra note* 13, Art. 28.
[74] Kimberly Carlson, "Cambodia's Draft Law turns Free Speech into Cybercrime", Internet Frontier Foundation, 27.05.2014. Available at: https://www.eff.org/deeplinks/2014/05/cambodian-cybercrime-draft-law-threatens-freedom-expression-online (25.11.2016)
[75] Klimburg, A., Healey, J. Strategic Goals & Stakeholders. National Cyber Security Framework Manual. Klimburg, A. (Ed.). NATO CCDCOE, 2012. p 68-70.
[76] Cheang (2009), *supra note* 6.
[77] Doug Gross, "Mafiaboy breaks silences, paints portrait of a hacker", CNN, 15.08.2011. Available at: http://edition.cnn.com/2011/TECH/web/08/15/mafiaboy.hacker/index.html?iref=obnetwork (28.11.2016)

the public forms the negative opinion concerning malicious intent. Nevertheless, there are some people who view hacks as highly skilled computer experts. They manipulate systems and expose vulnerabilities to point out the flaws before others can exploit them. Their actions inspire computer programmers to more securely code their software to protect against vulnerabilities.[78]

1.2.1.1. Script Kiddie

Script Kiddie is a less experienced intruder who depends on more knowledgeable crackers to automate attacks by using tools written by others to automate the process for them. Script Kiddie does not cause much damage due to their low level of skill if compare to other categories.[79] They are general young teenagers that have little knowledge of the mechanics of the Internet, such as routing and switching, and have only rudimentary knowledge of how Internet protocol such as FTP, SMTP and Telnet work. Usually, Script Kiddie uses the Internet chat room to swap information about hacking tools and pass on the stories.[80]

In this case, they break into a computer system for fun or disruption, or to install malware code in order to steal information, to launch or propagate viruses or to facilitate denial-of-service attacks (DoS) on website. This mean that these young category of hackers use computer "script" to carry their actions. Even though it does not cause serious damage, but it results in harm to moral patients who own, use or rely upon the systems that are violated or brought to a halt by the deployment of the script.[81] This kind of virus reportedly caused around 10 billion in lost productivity and digital damage.[82]

1.2.1.2. Hacktivist (Non-organized Non-State Actors)

Hacktivist describes as who draw on their computer skills to make political statements and actions. For the current time, social justice campaigners can deploy a range of hacktivist

[78] Long, L. Profiling Hackers. SANS Institute InfoSec Reading Room 2012. p 2-3. Available at: https://www.sans.org/reading-room/whitepapers/hackers/profiling-hackers-33864 (28.11.2016)
[79] Arbaugh, W. et al. Window of vulnerability: a case study analysis. IEEE 2000, 33 (12), pp 52-59, p 52. DOI: 10.1109/2.889093 (28.11.2016)
[80] Barber, R. Hackers Profiled: Who are they and what are their motivations? Computer Fraud & Security 2001, p 15. Available at: http://130.18.86.27/faculty/warkentin/SecurityPapers/Robert/Others/Barber2001_CF&S_Hackers.pdf (25.11.2016)
[81] Jonhson, D., Powers, T. Computer system and responsibility: A normative look at technological complexity. Ethics and Information Technology, Springer 2005, 7 (2), p 99-107, p 101-102. DOI: 10.1007/s10676-005-4585-0 (25.11.2016)
[82] Tech advisor, 4 different types of hackers. 28.04.2016. Available at: http://www.techadvisory.org/2016/04/4-different-types-of-hackers/ (25.11.2016)

strategies to further their cause.[83] Hacktivist refers to a collective of hackers group that made up of talented computer level, for example Anonymous, LulzSec or AntiSec. Their attitude is very often connected with the radical-punk idea of self-management, DIY and independent production. Number of the hacker and activist utopias spread in 1980s and in 1990s by took shape through collective experiences in social centers and promoted the idea of building up self-organized and economically independent spaces of networking and interactions.[84]

Hacktivist group are commonly politically motivated or to cause damage in order to make an ecological, political and ethical reason. They aim to embarrass their targets or disrupt their operations, most common practice they attack their target by stealing sensitive information and exposing or DoS where sever is overloaded till it finally crashes.[85] Government websites are commonly targets including Cambodia. Such attack has tarnished the government image in the world of cyber community.

Hacker group called NullCrew launched its campaign named Operation The Pirate Bay (OpTPB) to attack Cambodian websites. OpTPB targeted several websites of Cambodian businesses and government organization, including the armed forces. As result, OpTPB leaked highly confidential information and posted a number of passwords for other hacktivist groups to use. Hacktivist collective, Anonymous, also waged a cyber war against Cambodia in protest of the arrest of Warg. Over 5,000 documents were successfully stolen and leaked from Cambodia's Ministry of Foreign Affairs in 2012.[86]

1.2.1.3 Cybercriminals

Cybercriminals use technology to facilitate a crime primarily for chasing after money and personal benefit. Their targets run the gamut, including everyone from individuals to small business to large enterprise and banks. Cybercriminals attack by using social engineering to trick users into providing sensitive information, steal individual banking credentials, infecting an organizations, health care records, credit card and others with ransom ware or another form or

[83] Pierce, M. The Internet and the Seattle WTO Protests. Peace Review 2001, 13 (3), pp 331-337, p 334. DOI: 10.1080/13668800120079027 (25.11.2016)
[84] Bazzichelli, T. On Hacktivist Pornography and Networked Porn. GNU 2010, p 1. Availale at: http://www.tatianabazzichelli.com/PDF_files/Bazzichelli_Hacktivist_Pornography.pdf (25.11.2016)
[85] Barber (2001), *supra note* 80, p 16.
[86] YMAC (2016), *supra note* 9.

malware, or exploiting weakness in the network.[87]

1.2.1.4. Insiders

Insider theft is considered as the dangerous type that steals data and cause more damaging than other malicious attack carried out by external hackers. Insiders refer to a type of hacker who is an employee, a former employee or a contractor who try to steal sensitive documents or try to disrupt the organization operation. Edward Snowden is a prime example of an insider who hacked his own organization. Since they are the employees to the organization they know exactly the category of precious information and the place where those information stored.[88]

1.2.1.5. State Sponsored

State sponsored is known as advanced persistent threats.[89] They comprises of talented cyber attackers, rich of resources, well-organized group with advanced cyber attack tool. They are considered as the state sponsored group that works for the government in order to disrupt or compromise target governments, organizations or individuals to gain access to valuable data or intelligence, and can create incidents that have international significance.[90]

1.2.2. Categories of cybercrime

There are many different categories of cybercrimes being committed daily on the Internet such as financial crimes, unauthorized access, theft, virus/worm, DoS, Trojan attacks, web jacking, cyber terrorist, cyber pornography, online gambling, IP crime, email spoofing, cyber defamation, cyber stalking, etc. There are several reports on malicious viruses, scam and fraud mail from the Internet users in Cambodia, while we had noticed that internet café have been a major source of virus spread due limitation of cyber security measure.[91] However, cybercrime is not a serious threats to Cambodia yet if compare to other countries.

Government is likely the target of the cyber attack if compare to private sector and individual. Most of the common cases happen in Cambodia are web defacement, phishing, hacking, email

[87] Chicone, R. A Layman's Guide to Cyber Threats, Threat Actors, Attacks, and Intelligence. Kaplan University 2015, p 2. http://alliance.kaplan.edu/uploadedFiles/_Global_Content/Generic/Promotional_contents/Laymans%20Guide%20to%20Cyber%20Threats%20Article.pdf (25.11.2016)
[88] Tan (2016), *supra note* 23.
[89] Chicone (2015), *supra note* 87.
[90] Klimburg (2012), *supra note* 75. p 68-69.
[91] Cheang (2009), *suppra note* 6.

hijack, telecom fraud, and fraudulent money transfer.[92] Hacking happens very often in Cambodia and most targets are government websites such ministries, government agencies, and other high-ranking government officials through SQL injection and Distributed Denial of Service (DDoS). Cambodian government experienced several attack from different hacker groups includes: Black Hats Team from Iran, Anonymous, Young Geek, Brothers Team, and NullCrew who launched its campaign named OpTPB to attack Cambodian government websites. Thousands of highly confidential documents were stolen and leaked online and number of passwords also published for other hackers as well.[93]

Very few official reports on cyber attack that targets private companies offering online service, such as banks and telecommunication operators. Private sector and ISPs usually have better equipment and technician to monitor the network traffic, filter the spam and some malicious actions on the cyberspace. Most of cybercrimes and attacks have gone unnoticed and most victims of the cyber incidents were reluctant to report. Absent of incident report might be due to the impact of the incidents was not yet severe and the absent of legal procedure and the limit capability if the enforcement.[94]

1.3. Threat Responses

According to the transnational dimension of cybercrime, a significant weakness in the current system in combating against computer misuse is the inconsistency of legislatives among individual states and effective investigation and prosecution measures.[95] The strategic goals of the ITU Global Cybersecurity Agenda (GCA) calls for the elaboration of strategies for the development of cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures, as well as addressing the approach to organizing national cybersecurity efforts. The adoption by all countries of appropriate legislation against the misuse of ICTs for criminal or other purposes, including activities intended to affect the integrity of national critical information infrastructures, is central to achieving global cybersecurity.[96]

Since threats can originate anywhere around the globe, the challenges are inherently

---

[92] Ou, P. Status of Cybercrime in Cambodia. Presentation at Octopus Cooperation against Cybercrime in Stasbourg, France,November 2016. Avaiable at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806bdc39

[93] Cheang (2009), *suppra note* 6.

[94] Ibid.

[95] The transnational dimension of cybercrime and terrorism. Ed. Sofaer, A., Goodman, S. California, Hoover Institution Press, 2001, p 15-16.

[96] ITU (2012), *supra note* 18

international in scope and require international cooperation, investigative assistance, and common substantive and procedural provisions. Thus, it is important that countries harmonize their legal frameworks to combat cybercrime and facilitate international cooperation. However, it takes time to update national criminal law to prosecute new forms of online cybercrime. Indeed, some countries have not yet finished with this adjustment process.[97]

Cambodia does not have any specific legislation dealing with cybercrimes, while the Cybercrime Law is in the drafting process, Criminal Code 2009 take the arms over the cybercrime issues in Kingdom. Before 24 October 2013, there were government agencies, MPTC and NiDa, in charge of national cybersecurity framework and played leading role in designing and improving cybersecurity policy in Cambodia. MPTC is the regulator and policymaker on ICT industry, responsible for licensing all the ICT businesses, and solving the conflict of interest among the telecom operators.[98]

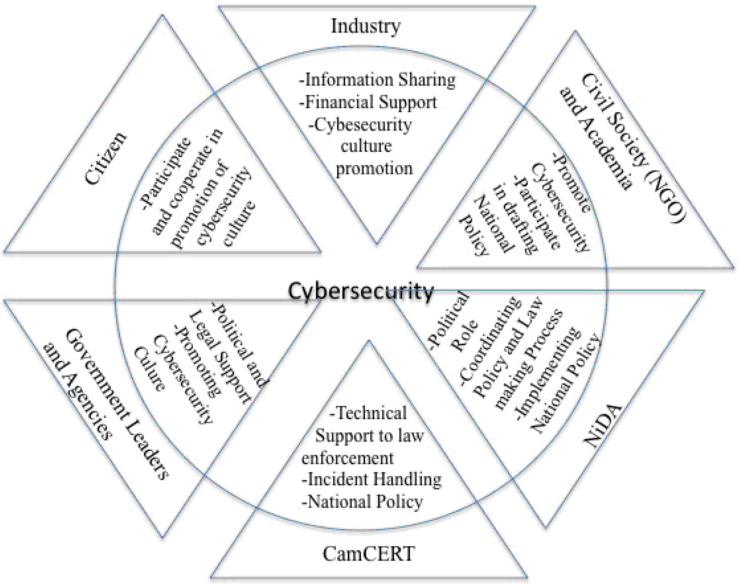

Figure 4: National framework to establish cybersecurity.[99]

NiDA was established in 2000 chaired by the Prime Minister and consists of a secretariat of around 40 people. NiDA's task is to map out an ICT Master Plan for Cambodia. NiDA has developed as short, medium and long-term strategy to pursue the goal of using computer technology in order to move government closer to the citizen. NiDA also helps organize an IT

[97] Ibid.
[98] Cheang (2009), *suppra note* 6. p 655.
[99] Ibid.

and security awareness. After 24 October 2013, NiDA has been integrated into MPTC's structure and divided into two department called General Department of Information Communication Technology (GD-ICT) and National Institute of Post Telecommunication and Information Communication Technology (NIPTICT). [100]

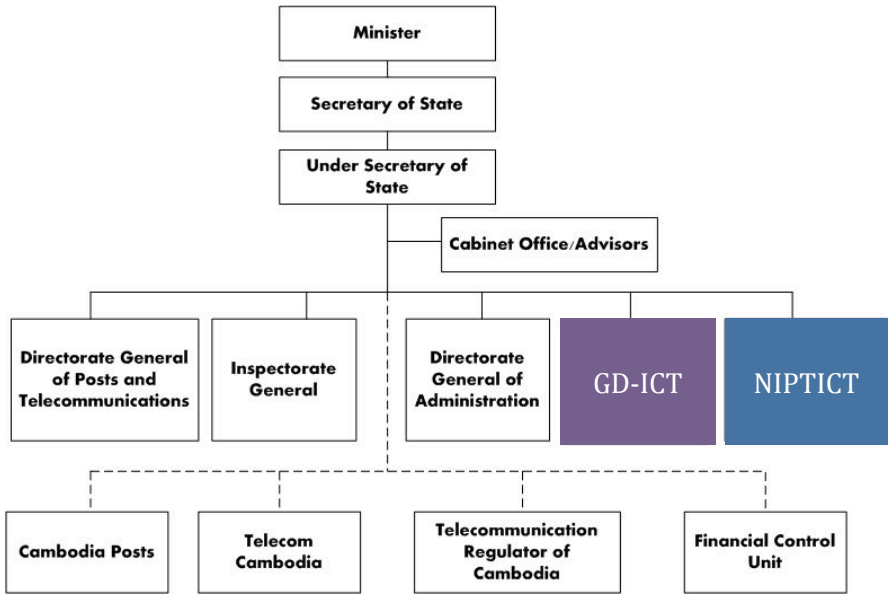

Figure 5: New MPTC's Structure after 24 October 2013.[101]

The potential and actual challenges confronting Cambodia in Cyberspace are expected to grow in as the cyber space expends to envelop larger area of social, economic and political activities. The government is aware and concern over the invasion of cyber threats through the Internet and the need to enhance cyber security at the government, private sectors, organization and individual levels. In December 2007, CamCERT, a non-profit team of IT security professional was established. CamCERT provides computer information security advice and cooperate with the Cambodian government, ISPs, local/international CSIRTs, as well as the Cambodian public including ICT venders, National Security Communities, and corporate/individuals users.[102]

[100] Tan, S. Security is everyone business: Don't become the healing. Presentation in Cambodia-Korea Information Session workshop, Phnom Penh, 23 June 2015.
[101] Ibid.
[102] CamCERT, Who we are? Available at: https://www.camcert.gov.kh/who-we-are/

1.4. Conclusion

The technologies and new innovation keep growing and become the backbone of the global economy, yet it also generated a new trend of crime and provides greater opportunity for criminals to conduct criminal activities via computer system and network. Cybersecurity is a concerned global issue and costs an estimated 1 trillion economic loss annually. Moreover, the lack of proper legal framework and mechanisms to deal with cybersecurity issue is the main challenges for securing cyberspace,[103] particularly for less developed and low-tech countries.[104]

Cambodia is a latecomer of Internet with the first commercial service launched in 1997. Number of Internet penetration increased from 0.07% in 2001 to around 48% in 2016. Cybercrime is not a serious threat to this country, yet it is not a new issue. The RGC launched its first e-government project in 2002, and noticed that some of government websites were vulnerable to cyber attack since then. The number of cyber attacks remarkably increased between 2012 and 2015 after RGC announced it is in the drafting process of its fist ever Cybercrime Law. The draft of controversial Cybercrime Law leaked in early 2015, which netizens fear that their freedom of expression on Internet will turn into crime. Civil societies also voice their concern that broad terms used, particularly Article 19 and 28 that have limit on content behavior, could become a serious threat to privacy and freedom on the Internet.

Since 68% of the total population are under 30-year old and are actively online, the potential and actual challenges confronting Cambodia in Cyberspace are expected to grow as the cyber space expends to develop larger area of social, economic and political activities. Cambodia has significantly achieved some key efforts on cybersecurity and policy implication through promoting cybersecurity culture, established e-government service, e-commerce, and focus on raising awareness and capacity building to the citizens and agencies. Cambodia also established CamCERT in 2007 in order handle Information Security. Last but not least, Cambodia also works hard on structural reform in order to improve the development of ICT sector. As a result NiDA has been integrated into MPCT's structure in 2013.

---

[103] Jahankhani, H., Al-Nemrat, A. Examination of Cyber-criminal Behavior. International Journal of Information Science and Management, 2015, p 41. Available at: https://www.researchgate.net/profile/A_Al-Nemrat/publication/228684366_Examination_of_Cyber-criminal_Behaviour/links/55643e3208ae8c0cab37167f.pdf (last accessed on 20.12.2016)

[104] Schmitt, M. The Law of Cyber Targeting. NATO CCDCOE, 2015. p 1. Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/TP_07_2015.pdf (last access on 25.10.2016)

2. Current Legal Framework

2.1. Legislating Cyberspace

The potential trend toward e-government, e-commerce, e-education, including e-health sector and others is growing in this nation; Cambodia tries to make a magnificent effort on both legal framework and structural reform. In order to keep pace with other member states in the region in the areas of social, economical development in order to attract more foreign investors to Cambodia, proper legislation and mechanism concerning the ICT sector is needed. In the first chapter have mentioned about the regulators and agencies that in charge of cybersecurity issue in Cambodia. In chapter two will look at the current legal framework and accessing Cambodia's effort on cybersecurity and policy implication.

2.1.1. Criminal Code of the Kingdom of Cambodia (2009)

The term "Cybercrime" does not exist in anytime specific legislation in the Kingdom yet. While the controversial Cybercrime Law being drafted, Cambodian Criminal Code 2009 have jurisdiction over the current cybercrime issue. The computer related offences were introduced for the time being in the Cambodian Criminal Code 2009 from Article 317-320 and 427-432, the crimes being called *"Infringement on the secrecy of the correspondence and telecommunication"* and *"Offences in information technology sector"*. Moreover, *"Defamation and Insult"* has been categorized into types of cybercrime as well once it is committed via computer network. The terms being introduced in this law are very general.[105]

2.1.1.1. Infringement on the secrecy of the correspondence and telecommunication

Right to correspondence is an international fundamental right to private life recognized under international human rights law and it is also applied to the secrecy of telecommunication. This right protects parties from any active interference; any censorship or other kind of active limitation on the free flow of communication is considered as an interference and violation to above rights.[106] According to the Cambodian Criminal Code, any act of opening, disappearing, delay or diverting the correspondence addressed to third party, in bad faith is an infringement on correspondence.[107]

---

[105] Cambodia Criminal Code 2009, *supra note* 71.
[106] Ruiz, B. Privacy in Telecommunications: A European and an American Approach. Netherland, Kluwer Law International 1997, p 134-135.
[107] Cambodia Criminal Code 2009, *supra note* 71, Art.317-320.

In addition, fraudulently acquiring knowledge of the content of the correspondences addressed to a third party is categorized in the same group as above acts and are punishable by an imprisonment of between one and five years. Moreover, it is capable of fine between one hundred thousand and two million Riels. According section 5 of this law, the act of listening or jamming the telephone conversation, in bad faith will receive the same punishment mentioned above.[108] There are other additional penalties as well regarding with the categories and duration of act such confiscation of materials, prohibition against pursuing a profession, posting and broadcasting the decision of the sentence, etc.[109]

2.1.1.2. Offenses in information technology sector

The offenses in IT sector seem too vague under chapter two of the Cambodian Criminal Code. According to Article 427, the offence of accessing or maintaining access to automated data processing systems provides, *"the acts of having access to automated data processing or maintaining access to it is punishable by an imprisonment from 1 (one) month to 1 (one) year and a fine from 100,000 (one hundred thousand) Riels to 2,000,000 (two million) Riels*.[110] Moreover, the same article also provides that, *"when the act has resulted in either deletion or modification of the data contained in the system…, is punishable by an imprisonment from 1 (one) year to 1 (one) years and a fine from 2,00,000 (two million) Riels to 4,000,000 (four million) Riels"*.[111]

Beside, the act of obstruction the operation of automated data processing system, fraudulent introduction, deletion or modification of data, participation in a group or a agreement to prepare for the commission of offences are considered as offenses in information technology sector and received similar punishment as above. [112] Criminal law failed to provide clear explanation of the terms used in each offense listed in above articles. The term *"having access to automated data processing or maintaining access"* is being used in the current law without instruction whether having access here refer illegal access, access to unauthorized data or intentional access to unauthorized data. The law failed to explain as well the level of technical access, usage or obtain of data via technical means.

The broad term being used leads to confusion when it comes to the implementation and

[108] Ibid.
[109] Ibid.
[110] Ibid. Art. 427.
[111] Ibid.
[112] Ibid. Art. 428-432.

interpretation of the article. The clearer term of offences are being introduced in the current draft law on Cybercrime such as illegal access, data espionage, illegal interception, unauthorized data transfer, and system interference. The access without right to a computer system, obtains without authorization against unauthorized access, interception without right made by technical means, alteration, deletion or deterioration of computer data or restriction to such data without right, unauthorized data transfer from computer system or by means of a computer data storage medium, or the act of causing serious hindering without right of the functioning of a computer system shall be sentenced between six months and fifteen years and fined from one million Riel to twenty four million Riel.[113] Even the term getting clear in the draft law, but it seems focus more on the sanction and the amount of fine of each offense.

2.1.1.3. Defamation and insult

Defamation and Insult has been categorized into a type of cybercrimes as well once it is committed via computer network. Defamation is one of concerning issue on the Internet, it is defined as *"an intentionally false communication, either published or publicly spoken, that injures another's reputation or good name, or holds a person up to ridicule, scorn, or contempt in a respectable and considerable part of the community"*.[114]

Civil societies claim RGC uses the defamation and insult provision of the Cambodian Criminal Code 2009 as a tool to crack down on the exercise of free speech by journalists, the political opposition and human rights defenders and activists.[115] Until now the RGC continue to use these provisions in order to threaten and prosecute those who criticize on the high ranking official or government institutions. The criminalization of defamation is continues as the repression of right to freedom of expression in Cambodia including freedom of expression on Internet.[116]

Article 305 of the Criminal Code defines defamation as *"any allegation or slanderous charge that undermines the honor or the reputation of a person or an institution"*.[117] Defamation of institution as well as individuals could result in criminal charge and punishable by a fine of between one hundred thousand to ten million Riels ($25-$2500) when the defamation was

[113] Cybercrime Law, Draft V.1, *supra note* 13, Art 21-26.
[114] Black, S. Telecommunications Law in the Internet Age. San Francisco, Academic Press 2002, p 418.
[115] CCHR, The criminalization of defamation of expression in Cambodia. CCHR Briefing note 2014, p 1. Available at: http://cchrcambodia.org/admin/media/analysis/analysis/english/2014_05_27_CCHR_Briefing_Note_Defamation_in_Cambodia_(ENG).pdf (20.12.2016)
[116] Ibid.
[117] Cambodia Criminal Code 2009, *supra note* 71, Art. 305.

committed by the following means: by speeches, by any whatsoever, announced in a public place or in public meeting; in writing or sketches by any means whatsoever, circulated in public or exposed to sight of the public; or by any means of audio-visual communication intended for the public.[118]

In addition to defamation under Article 305, public insulting under Article 307 of the Criminal Code further infringements on freedom of expression in Cambodia. Article 307 states that, *"any insulting expression, any scorning term or any other verbal abuses which does not affect the slanderous charges constitute an insult is punishable by a fine of between 100,000 (one hundred thousand) and 10,000,000 (tem million) Riels*".[119] The same article further explain that insult can be committed by speeches, by any whatsoever, announced in a public place or in public meeting; in writing or sketches by any means whatsoever, circulated in public or exposed to sight of the public; or by any means of audio-visual communication intended for the public could result in criminal charge.[120]

Last but not least, the term defamation and insult seem widely use in Cambodian laws including the questioning of a judicial decision under Article 523, insult of a public official under Article 502 of Criminal Code 2009 including articles under Press Law.[121]

2.1.2. Press Law 1995

Defamation and insult offenses under Criminal Code are using as pair with Press Law 1995. According to Article 306 and 308 of the Criminal Code, the defamation and insult committed by means of media is subject to the provision of the press law.[122]

The 1993 Constitution of Cambodia guarantees personal freedom to any individual under Article 31 and guarantees the right of freedom of expression, press, publication, and assembly under Article 41.[123] The Press Law 1995 also aim to provides protection and guarantees freedom of expression for the press provides under Article 1, *"This law determines the regime of the press and assures freedom of the press of the publication in conformity with articles 31, and 41 of the Constitution"*.[124] Moreover, this law further to maintain the independence of the press and

[118] Ibid.
[119] Ibid. Art. 307.
[120] Ibid.
[121] CCHR, Briefing note 2014, *supra note* 115, p 2.
[122] Cambodia Criminal Code 2009, *supra note* 71, Art. 306,308.
[123] Constitution of the Kingdom of Cambodia 1993, Art. 31, 41.
[124] Law on the Press No.NS/RKM/36/95, Art 1.

provide the right to freedom from pre-publication censorship under Article 3. Article 4 also states that public of official information may not be penalized if such publication is fully true and accurate summary of the truth.[125]

However, Press Law also restricts journalists from publishing information that harms someone's honor and dignity and it is used to punish journalists who criticize public figures[126] and imposes content restriction that *"may affect the public order by inciting directly one or more persons to commit violence"*[127] or which *"may affect national security and political stability"*[128] or which affects *"the good custom of society"*.[129] The terms being used provide more than vague interpretation of the laws in Cambodian judicial system. Undefined terms under Press Law and Criminal Code have been continual confusion as to which law should be used to prosecute journalists charged with defamation and insult. There are many vague provisions under Press Law that actively threaten to the right to freedom of expression in Cambodia, which need reviewing and amending.[130]

2.1.3. The Law on Telecommunications 2015

The Law on Telecommunication is promulgated by the Royal Decree No.NS/RKM/1215/017 dated 17 December 2015, a most comprehensive legal instrument for supervising the telecom sector in Cambodia. The objectives of this law are to defines the authorities of the Ministry of Post and Telecommunication, to establishes and sets duties of the Telecom Regulator Cambodia, classifies different types of authorization, certificate and licenses, sets the supervision on the use of infrastructure and network, the fees, the fair competition and the protection of the consumers.[131]

Report of the Special Rapporteur on the situation of human rights in Cambodia submitted during the 33rd regular session of the United Human Right council highlighted the concern over the adoption of the Law on Telecommunication 2015. The report from the UN Special Rapporteur Rhona Smith noted that, *"the law requires telecommunications companies to turn over certain*

[125] Ibid, Art. 3-4.
[126] Yasuda, Y. Rules, Norms and NGO Advocacy Strategies: Hydropower development on the Mekong River. New York, Routledge 2015.
[127] Law on the Press, *supra note* 123, Art 11.
[128] Ibid, Art 12.
[129] Ibid, Art 14.
[130] CCHR, Briefing note 2014, *supra note* 115, p 2-3.
[131] The Law on Telecommunications, No.NS/RKM/1215/017 dated 17 December 2015, Art 2.

data to the government upon request".[132] Moreover, the report also highlighted the degree of compliance with international human rights law lies in the interpretation and application of the law by law enforcement and judicial official. Therefore, clear guidelines reflecting prevailing international human rights should be carefully drafted and disseminated in order to ensure that the law is applied in a manner that regulates without unnecessarily restriction the activities.[133]

According to Article 6, MPTC shall have competence to control telecommunications and ICT service data, where all telecommunication operators shall provide to MPTC data on their service users.[134] This article seem to requires companies to provide data without the requirement of a judicial warrant or other safeguards protecting the right to privacy guarantees under Article 31 of the Constitution and Article 17 of the International Covenant on the Civil and Political Rights.[135] In addition to Article 6, Article 97 allows secret surveillance of communications where it is conducted with the approval of the "legitimate authority".[136] While there is no clear interpretation of the term legitimate authority under Article 97 of the Law on Telecommunications, the private communications can be monitored. Therefore, any private speech via telecommunication can no longer be considered truly private.[137]

Beside privacy issue, under the same law also provides criminalization of expression and restriction of rights. Article 80 states that, "*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*."[138] In addition seven to fifteen years imprisonment, person who commits offenses as stated in Article 80 shall be fined from 140 million Riels to 300 million Riels.[139] This mean that any communications conducted by any electronic could be criminalized if it is deemed to create "national insecurity". The broad term being used give too much power of the law interpretation to law enforcement and judicial official and its vagueness may politically exploitable.[140] Article 66 also provides general prohibition of any acts in communication sectors that may "*affect public order and lead to*

[132] UN, Report of the Special Rapporteur on the situation of human rights in Cambodia, A/HRC/33/62, p 10.
[133] Ibid.
[134] The Law on Telecommunications, *supra note* 131, Art. 6.
[135] Licadho, Cambodia's Law on Telecommunications a Legal Analysis, Briefing Paper 2016, p 1-2. Available at: http://www.licadho-cambodia.org/reports/files/214LICADHOTelecomsLawLegalAnalysis_March2016ENG.pdf (10.01.2017)
[136] The Law on Telecommunications, *supra note* 131, Art. 97.
[137] Licadho 2016, *Supra note* 135.
[138] The Law on Telecommunications, *supra note* 131, Art. 80.
[139] Ibid, Art 81.
[140] Licadho 2016, *Supra note* 135, p 2.

national insecurity". [141] Without clear instruction, individuals could not identify the consequences that could subsequently be deemed to have been violated to this law and incur penalties.[142]

Telecom Law 2015 also provides specific powers for the destruction of evidence. Article 76 stated that, "*in case the evidence of this offense is prohibited products or dangerous, telecommunication inspection officials have the rights to request the prosecutors' s ruling to destroy in line with applicable procedures*".[143] It unclear what does this law mean by "applicable procedures" and "prohibited or dangerous products". Destruction of evidence under this article could affect right to fair trial for those charged under this law. When a defendant is deprived of material evidence, he is deprived of the fundamental right to a fair trial because he cannot present a complete defense.[144]

The constitutionality duty to preserve evidence standard should apply and constitutionality materiality test should take place; police must preserve physical evidence of a type that they reasonably should know has the potential in order to reveal immutable characteristics of the criminal.[145] Whether or not the prosecutor act in the good faith or bad faith, evidence could be destroyed at a pre-trial stage under Article 76 of the this law.[146]

2.1.4. Case Study

2.1.4.1. Anonymous Cambodia

Two member if Anonymous Cambodia, a part of the global hacking group, were arrested on April 2014 on charges of infiltrating government website and stealing sensitive data, following an eight-month operation by local authorities and the U.S, Federal Bureau of Investigation (FBI). Bun Khing Mugkul Panha, 21, and Chou Dongheng, 21, were arrested on April 07 for hacking a total of 30 government websites, including those of the National Election Committee (NEC), Ministry of Foreign Affairs, Ministry of Defense, Anti-Corruption Unit and Phnom Penh

---

141 The Law on Telecommunications, *supra note* 131, Art. 66.

142 Licadho 2016, *Supra note* 135, p 2.

143 The Law on Telecommunications, *supra note* 131, Art. 76.

144 Bernstein, S. Fourteenth Amendment—Police Failure to preserve Evidence and Erosion fo the Due Process Right to a Fair Trial. J. Crim. L. & Criminology, 1990, 80 (4), pp 1256-1280, p 1274. Available at: http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=6649&context=jclc (20.02.2017)

145 Ibid, p 1273.

146 Licadho 2016, *Supra note* 135, p 4.

Municipality, as well as some other private sector sites.[147]

Mr. Panha confessed to hacking the site, while Mr. Songheng said he was only Mr. Panha's student. The attacks on government websites were Distributed Denial of Service (DDoS) attacks, in which the sites were taken offline and data was stolen from them. Both of them were third-year student at SETEC Institute in Phnom Penh. Since Cambodia does not have specific cybercrime, young hackers charged under Article 427, 428, 424 of the Cambodian Criminal Code 2009, which relate to the offenses in information technology sector. The offenses each carry a fine between $500 and $1,000 along with a jail term of between one and two years.[148]

The Phnom Penh Municipal Court found Mr. Panha and Mr. Songheng guilty of four charges including unauthorized access to or remaining in an automated data-processing system and obstructing the functioning of an automated data-processing system. The Municipal Court sentenced both of them to two years in prison. However, the judge suspended their sentences, prescribed their release from pretrial detention and ordered them to work for the Ministry of Interior instead. [149]

2.1.4.2. Phel Phearun accused of defamation over a Facebook post[150]

Teacher Phel Phearun accused of defamation over his Facebook post about his motorbike incident. Phel Phearun was stopped by two police officers on 24 January 2014 and asked him to prove that he legally owned the new motorbike without number license plate. Police brought him and his motorbike to the police station, but after he proved that he is the legal owner of the motorbike, police refused, saying: "This motorbike will be returned, you just wait until tomorrow". Phearun agreed to return the next day, but insisted police to give him the confirmation letter as evidence that his bike had been impounded.

Teacher Phel Phearun posted a description of these events on his Facebook account, expressing concern about his treatment. His post was asking readers whether they thought police procedures could be improved in such cases, in order to make the situation simpler for law-abiding citizens.

---

[147] Sinary, S. Wilwohl, J, "Hackers Arrested in Joint Operation with FBI", The Cambodia Daily April 32, 2014. Available at: https://www.cambodiadaily.com/archives/hackers-arrested-in-joint-operation-with-fbi-57065/ (10.01.2017)
[148] Ibid.
[149] Pisey, H. Wilwohl, J, "Hackers Ordered to Work for Government, The Cambodia Daily", October 1, 2014. Available at: https://www.cambodiadaily.com/archives/hackers-found-guilty-freed-ordered-to-work-for-government-68722/ (10.01.2017)
[150] CCHR, Case Study Series on Phel Phearun case, Factsheet 2013. Available at: http://cchrcambodia.org/index_old.php?url=media/media.php&p=factsheet_detail.php&fsid=54&id=5 (10.01.2017)

He also posted a scanned image of the confirmation letter. On 26 January, new website Sabay published an article about Phel Phearum's case, including the Facebook post. A month later, on 23 February 201, he received a letter from the police requesting that he attend the police station on 25 February 2013 to answer questions in relation to a defamation case over his Facebook post.

According to Article 305 of the Cambodian Criminal Code 2009 defines defamation as any allegation or slanderous charge that undermines the honor or the reputation of a person or an institution constitutes defamation is punishable by a fine of between 100,000 (one hundred thousand) and 10,000,000 (ten million) Riels (equal 25 to 2,500 USD). Phearun posted a question asking ideas for improving the situation; it was not carried out "in bad faith". He did not publish false information, and did not set out to injure the reputation of the police but merely exercised his right to freedom of expression in order to share his experience and to generate legitimate awareness and debate.[151] The police dropped charge against Phel Phearun after social societies issued number statements and factsheets calling it was a serious threat to freedom of expression in the Kingdom.[152]

[151] Ibid.
[152] CCIM, "Charges on Defamation Cases Against Facebook User Dropped", 19 March 2013. Available at: http://www.ccimcambodia.org/what-we-do/internet-freedom/36-charges-on-defamation-case-against-facebook-user-dropped (20.01.2017)

2.2. National Policy

2.2.1. Rectangular Strategy Phase III – Side 4: Development of Information and Communication Technology

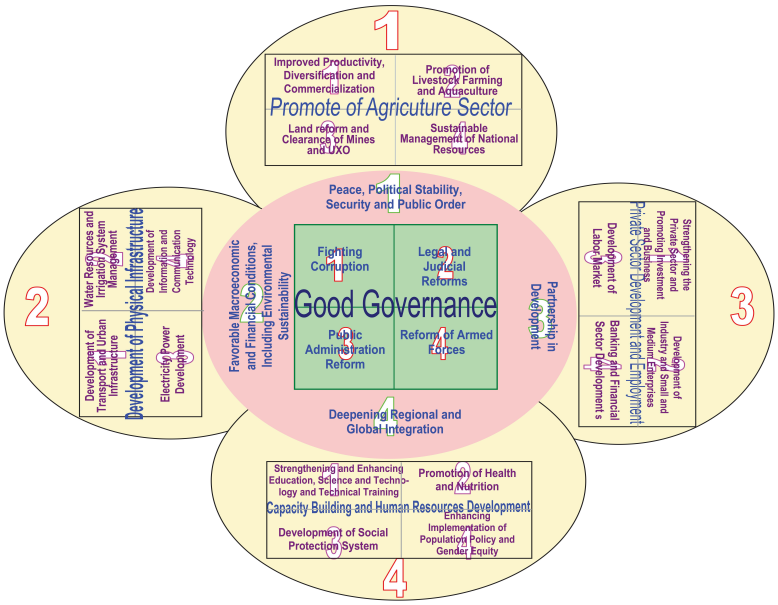

Figure 6. Rectangular Strategy Phase III.[153]

The Rectangular Strategy is the part of the political platform of the Legislature with its central theme of Growth, Employment, Equity and Efficiency. The four strategic rectangles will be maintained with extended scope, developed and reprioritized sides, and enriched effective policy and mechanisms. The RGC has been implemented Rectangular Strategy Phases I and II in the previous decade and the Rectangular Strategy Phase III is used to reaffirms the RGC's mission and its commitment to sustainable development and poverty reduction in its Political Platform of the Fifth Legislator in 2013-2018. Rectangular Strategy Phase III is a scheme to guide the activities of all stakeholders to further pursue and strengthen long-term sustainable development aimed at promoting economic growth, creating jobs, equitable distribution, and ensuring efficiency of the public institutions and management of resources.[154] The RGC put out the commitment toward the development of ICTs in to the national strategic plan, where we can find in Rectangular Strategy Phase III, Side 4.

[153] RGC, National Strategic Development Plan 2013-2018, 17 July 2014, p 3. Available at: http://cdc-crdb.gov.kh/cdc/documents/NSDP_2014-2018.pdf (20.11.2016)
[154] RGC, Rectangular Strategy for Growth, Employment, Equity and Efficiency Phase III, September 2013, p 2. Available at: http://www.ilo.org/wcmsp5/groups/public/---asia/---ro-bangkok/---sro-bangkok/documents/genericdocument/wcms_237910.pdf (20.11.2016)

2.2.1.1. Objective and Strategy

Rectangular Strategy Phase III – Side 4 aim at improving ICT sector in Cambodia by solidifying legal framework, strengthening governmental institutions capabilities and public services, and upgrading technologies to assist other technical undertaking. Moreover, the RGC also have objectives to boost up the market competition among the service providers in order to ensure the efficiency in this sector, promote e-application in both public and private sectors such as e-government, e-commerce and other information infrastructure development. [155]

In order to achieve above objectives, the Telecommunication Regulator of Cambodia was established in order to regulate the policy and legal framework in telecommunication and ICT sector and monitor the practice of service providers in the Kingdom. In addition to this, in order reach international standard the RGC transformed Cambodia Post into state-owned enterprise and create a data management center.[156]

2.2.1.2. Development Priorities

In order to achieve the objectives set under Rectangular Strategy Phase III – Side 4, the RGC has prioritize particular activities including establishing "National Telecom/ICT Development Policy", which based on the social and economic dimensions. RGC also focus on the legislation development though adoption of the Law on Telecommunications, the Law on E-Commerce and other necessary law for the effective management in this area. Capacity building of the relevant institutions and enhancing institutional collaboration to develop and manage telecom and ICT sector with transparency and efficiency is also one among other development priorities.[157]

Last but not least, preparing and implementing the "National Broadband Plan" in order to develop human resource, encourage the technology innovation, and boost up the economic productivity through broader participation from the public and private sector is another important priorities for ICT development in this nation. RGC plan to enlarge the coverage and bolstering the efficiency of Telecom/ICT, particularly by encouraging greater use of this infrastructure and continue to expand to areas with high economic and tourism potential as well as remote areas without or with limited telecommunication services.

[155] Ibid, Phase III Side 4, p 26.
[156] Ibid.
[157] Ibid. p 27.

Promoting human resource development in ICT sector is the key to success by strengthening all levels of education curricula, training of government officials and encouraging the private sector to participate in enhancing public's literacy in ICTs. RGC also plan for further developing e-Government and encouraging the private sector to invest in the modern and innovation of technology including broadband Internet, Cloud computing and software development to enhance the quality and efficiency of telecom and ICTs in Cambodia. [158]

2.2.1.3. Assessment on 2013 Rectangular Strategy Phase III – Side 4

Based on the development priorities listed in 2013 Rectangular Strategy Phase III above, we are going to access on the RGC's effort on the ICT development. What the RGC have achieved from 2013 to 2016?

Legal and Policy Framework – Cambodia officially launched the "ICT Master Plan 2020", the final product of two million US dollars grant aid from the government of the Republic of South Korea, on 20 August 2014. Cambodian ICT Master Plan 2020 is made in the line with international Telecom/ICT development Framework such as ASEAN ICT Master Plan 2020 and ITU Connect 2020 Agenda. The "Law on Telecommunications" adopted in 2015 for regulating telecommunications industry, role of MPTC and Telecommunication Regulator of Cambodia (TRC) and foundation and principles for establishing regulation on numbering plan, licensing regime, spectrum, numbering plan, IP and domain name, quality of service, etc. [159]

In 2016, RGC also adopted "Telecom/ICT Development Policy 2020" to provide roadmap for telecommunication and ICT development including guideline and principle for Broadband policy in Cambodia. There are some other laws and policies are being drafted includes: draft law on Cybercrime, draft law on E-commerce, and draft of Spectrum regulation.[160]

Institutional Framework – NiDA has been integrated into the structure of the ministry of MPTC in 2013. TRC was established by the Royal Decree dated on 17 December 2015, which declared the Law on Telecommunications, and Sub Decree dated on 16 March 2016 regarding the organization and operation of the Telecommunication Regulator of Cambodia. The main of objective of TRC is to formulate the regulations, relating to the operation and provision of

[158] Ibid.
[159] Kothara, H. Presentation on Economic Aspect of Spectrum Management, November 2016. Available at: http://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2016/Nov-SM-Economics/Presentations/Day%202%20-%20Session%204%20(Cambodia).pdf (10.01.2017)
[160] Ibid.

telecommunication in the line with the RGC's policy on the telecommunication sector.[161]

Mobile cellular subscriptions – the number of mobile phone subscription increased from around 10 million in 2010 to around 20 million in 2016.[162]

Internet subscriptions – the number of Internet subscription increased from 6% in 2013 to around 46% by June 2016.[163]

Quality and network – the quality of telecommunication network and service was steadily enhanced, along with gradual development of the fixed-line telephone service. Moreover, network and service coverage of the optical cables was continuously expanded by connecting from Phnom Penh to all districts and communes across the country as well as neighboring countries in the region.[164]

2.2.2. Cambodia's ICT Master Plan 2020

2.2.2.1. Objectives

ICT Master Plan aims to build an "ICTopia" that support the country push toward intelligence. It has 5 priority actions have been identified by the government, including development of an e-government framework, strengthening of cyber-security, e-education, e-commerce and e-tourism. The National Institute of Posts Telecommunications and ICT was also established in early 2014, which aims to leverage ICT to strengthen the education system, improving government efficiency and enhancing ICT literacy in the private sector.

[161] TRC, History of Telecommunication Regulator of Cambodia. Available at: https://www.trc.gov.kh/about-us/background/ (10.01.2017)
[162] TRC, Mobile Phone Subscription. Available at: https://www.trc.gov.kh/mobile-phone-subcribers/ (10.01.2017)
[163] MPTC, Fact Sheet on Telecommunication Sectors. June 2016. *supra note* 11.
[164] RGG, Phase III Side 4. *Supra note* 154.

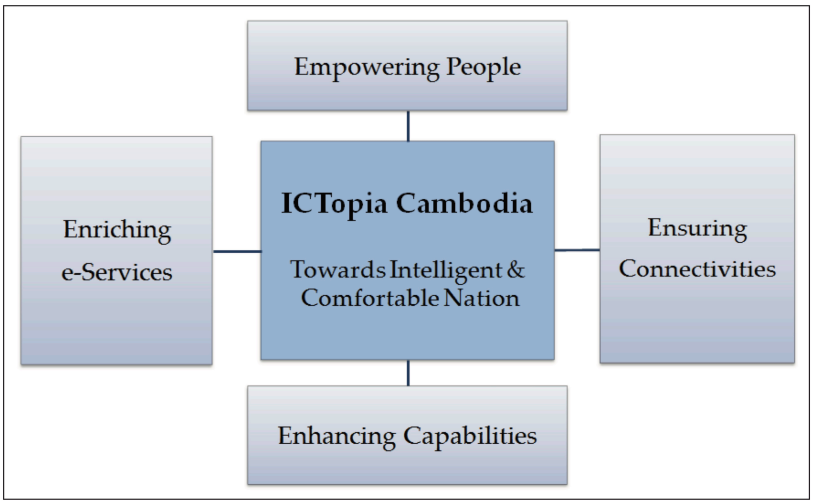

Figure 7. Cambodia's ICT Master Plan 2020 sets objectives.[165]

Cambodia's ICT Master Plan 2020 sets objectives as following:

Part 1. Empowering People: Focus on human resources development an awareness, to become Top-tier country of ICT Human Resource Development in Southeast Asia and 70% of Cambodian people are able to access the Internet by 2020.

Part 2. Ensuring Connectivity: Focus on infrastructure development, legal framework, institutional framework, and cybersecurity. Improve service accessibility of telecom and broadcasting for all the people; expand ICT infrastructure through government assistance and activating private investment and set base environment for diverse ICT convergence such as voice & data, wire & wireless, and telecom & broadcasting.

Part 3. Enhancing Capabilities: Focus on industry promotion, standardization, research and development. Cambodian's own ICT ecosystem have to be integrated into the global ICT ecosystem; Standardization is top priority; need to Increasing the number of participation; Enhancing ICT technological capacity through R&D and to help reinforce national competitiveness.

Part 4. Enriching e-Services: has 5 priority actions including development of an e-government

[165] KOICA, Summary on Cambodia ICT Masterplan 2020, 2014, p 5. Available at: https://data.opendevelopmentmekong.net/dataset/summary-on-cambodian-ict-masterplan-2020/resource/bf12527f-255e-4f2a-bb14-3ba433408e52?type=library_record (20.01.2017)

framework, strengthening of cybersecurity, e-education, e-commerce and e-tourism.[166]

2.2.2.2. Cybersecurity development plan

Cybersecurity becomes equal important with issue for ICTs development in Cambodia. Cybersecurity development plan have been listed in part two of the Cambodian ICT Master Plan 2020. Cambodia has tried to establish national cybersecurity base through CamCERT organization, there are some limitations such as lack of comprehensive cybersecurity system to ensure ICT service reliability, absence of relevant laws, regulations, policy, standard & norm, low level of knowledge and know-how skill on cyber security, and outdated infrastructure for cyber security for example, Information systems, ICT devices.[167]

To overcome these limitations and enhance the nationwide cybersecurity, it is needed to enhance cybersecurity system in Cambodia such as enactment completion of relevant legislations and establishment of government-wide leadership and organization. Moreover, it is necessary to expand cybersecurity activities through enhancing CERT system, protecting major infrastructure and distributing the standard. It is also crucial to build health culture for cybersecurity through making measures for unhealthy information distribution prevention, implementing illegal spam mail prevention system and executing awareness education & promotion for cybersecurity.[168]

The main objectives in cybersecurity development plan are: safeguarding the cyber space and provide basis for ICT progress by improving reliability of ICT service. In order to achieve objectives, RGC plan to establish basis for national cybersecurity system, spread cybersecurity system for the public sector to major private sector, and setup a system for continuous operation and development architecture for cybersecurity. Last but not least, RGC will also decide direction of improvement in consideration of the worldwide cybersecurity trends.[169]

2.2.2.3. Bolstering Cybersecurity

Bolstering Cybersecurity program means the enhancement plans of information security as applied to administrative, technological and physical areas in order to provide reliable and stable ICT services.

---

[166] Tan, S. Presentation on Cambodian Master Plan 2020 and Draft T-ICT Development Policy. Cambodian-Korean Information Security Workshop on 23 June 2015. Available at: http://www.mptc.gov.kh/files/2015/06/275/Session2-T-ICT-Policy.pdf (10.01.2017)
[167] KOICA (2014), *supra note* 165.
[168] Ibid.
[169] Ibid.

RGC can successfully implement the program by establish cybersecurity base like policy, organization and law. To do this, the RGC will compose relevant government organization, complete enacting cyber security laws and enhance internal & external cooperative network including government and private sector. Moreover, the RGC will expand activity coverage and targets of cyber security by enhance CERT system, protect major ICT infrastructure and establish & distribute cyber security standard.[170]

In addition to above strategy, the RGC will establish privacy protection system for dealing with infringement of personal information by establishing foundation for protecting personal information and set up plans for implementing and expanding the personal information protection system. Finally, the RGC will improve awareness on cyber security at the national level for improving cyber security culture continuously. This can be achieved by establish measures for harmful and indecent information, build an illegal spam mail prevention system and execute cyber security awareness education & promotion.[171]

2.2.3. Telecom/ICT Development Policy 2020

2.2.3.1. Objective

Telecom/ICT Development Policy 2020 adopted by the RGC in April 2016 with the vision toward ICT connectedness and readiness. The main goals of Telecom/ICT Development Policy 2020 are to provide vision, policy framework, coordination framework and institutional arrangement from telecommunication and ICT development in Cambodia. Moreover, it helps to address structural challenges and enhance business and investment environment in Telecommunication and ICT sectors. And to provide interlock measure and specific interventions as needed between 2015 and 2020.[172]

Telecom/ICT Development Policy 2020 has three main objectives as following:

Objective 1 – Improve and expand telecommunication infrastructure and usage.

Objective 2 – Develop ICT human capacity.

[170] Ibid.
[171] Ibid.
[172] Mok, K. Presentation on e-Government Status in Cambodia. Available at: https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2015/August-eGov2015/Session-2/S2B_Khemera_Mok.pdf (10.01.2017)

Objective 3 – Diversify ICT industry and promote the application of ICT.[173]

2.2.3.2. Strategic framework and measures

In order to achieve the three objective above, RGC set up thee strategy as following:

Firstly, strengthen the Telecom/ICT development foundation by providing a trusty and clear legal and regulatory frameworks, further developing Telecom/ICT infrastructure, bringing digital divide and enhancing the level of ICT literacy.[174]

Secondly, enhance ICT security and development the ICT industry by raising awareness about cybersecurity to all level stakeholders, organized and encourage the implementation of cybersecurity technique, prepare national technical standard on cybersecurity, strengthen the CamCERT's capacities. Moreover, the working team have to pay more attention on the sustainability and safeguard of all government website at all level from cyber attack, diversify Telecom/ICT industry and identify critical information infrastructure.[175]

Lastly, promote the application of ICT by developing and promoting e-government, e-commerce, and promoting the use of ICT for environmental protection, climate change adaption and mitigation, and disaster management.

Monitoring and evaluation: target based evaluation. The biannual reports on the progress and challenges in implementing Telecom/ICT development policy will submit to the office of the Council of Minsters. Midterm review will be in 2018 on the progress of Telecom/ICT development policy implementation or suggested revisions. [176]

2.3. Draft law on Cybercrime

2.3.1. Purpose, Objective and Scope

English-language version of the draft law on Cybercrime in Cambodia were obtained and released by Article 19, the London-based freedom-of expression advocacy group in 2012 seeks to criminalize online content.[177] According to Council of Ministers spokesman Ek Tha, the draft

[173] RGC, Telecom/ICT Development Policy 2020, April 2016, p 17. Available at: http://www.mptc.gov.kh/site/detail/546 (20.12.2016)
[174] Ibid. at p 20.
[175] Ibid.
[176] Ibid.
[177] Kevin Ponniah, "Cyber bill raises concerns", The Phnom Penh Post 09.04.2014. Available at: http://www.phnompenhpost.com/national/cyber-bill-raises-concerns (10.02.2017)

of the Cybercrime Law is designed to "*prevent any ill-willed people or bad-mood people from spreading false information and groundless information*".[178] Article 1 of the draft law states that, "*This law has a purpose to determine education, prevention measures and combat all kind of offense commit by computer system*".[179] Moreover, this law has objectives to "*ensure the implementation of law, anti-cybercrime and combating all kinds of offense commit by computer system*" and "*ensure safety and prevent all legitimate interest in using and developing technology*". [180]

2.3.2. Structure

Draft Cybercrime Law divided into six main chapters. Chapter 1 is the general provision that covers the purpose, objective, scope, and terms and definition of this law. Chapter 2 cover the establishment of National Anti-Cybercrime Committee (NACC), composition of NACC, duties, officials, budget and other concerning NACC. Chapter 3 provides the procedure dealing with cybercrime offence including other investigation power. Chapter 4 covers specific type of offence such as illegal access, data espionage, illegal interception, data interference, etc. Chapter 5 cover the mutual legal assistance, international cooperation and extradition, final chapter 6 is the final provision.

Interestingly, there is an establishment provision of institute to deal with cybercrime specific called NACC that will be chaired by prime minister and deputy prime minister will be the deputy chairman. Other composition of members includes five secretaries of state from Ministry of Interior, Ministry of Foreign Affair, Ministry of Information, Ministry of Post and Telecommunications, and Ministry of Justice. There will be one general commissioner from National Police as well will be served as member. Other six members are the representative from Anti-terrorism, Council of Justice, Ecosoc, Chamber of Commerce, NiDA and NACC.[181]

NACC has duties to devises strategies, action plans, and related programs in securing cyber and information grid for RGC, advises and recommend course of actions to the General Secretariat of the National Anti-Cybercrime Committee, supervises workflows and course of action-plans implementations of the General Secretariat of the National Anti-Cybercrime Committee. Moreover, NACC also issues findings and appropriate recommendations for ministries and

[178] Ibid.
[179] Cybercrime Law, Draft V.1, *supra note* 13, Art.1.
[180] Ibid, Art. 2.
[181] Ibid, Art.6.

departments to ensure the security of cyber and information grid of the RGC, provides cyber and information grid security report for the nation to the RGC bi-semester and annually and performs duties directed by the Royal Government of Cambodia.[182]

In democratic society, the powers shall be separated between the legislative power, the executive power and the judicial power. Each branch must function independent from each other's interference, but must have powers to check and balance against each other.[183] Establishment of NACC chaired by Prime Minister, deputy prime minister and other compositions from ministries under Article 6 of this draft law provide legislative power to the members of executive body. Interference of power and lack of independent among the three branches remains as major concerns in Cambodia. The absence of checks and balances is resulting in unaccountability of the government and the political leadership.[184]

2.3.3. Offenses

According to discussion in section 2.1.1, Cambodian Criminal Code 2009 have jurisdiction over the current cybercrime issues. The computer related offences under the Cambodian Criminal Code 2009 is being called *"Infringement on the secrecy of the correspondence and telecommunication"* and *"Offences in information technology sector".*[185] More specific cyber offences are being introduced in the current draft law on Cybercrime such as illegal access, data espionage, illegal interception, unauthorized data transfer, and system interference.[186]The access without right to a computer system, obtains without authorization against unauthorized access, interception without right made by technical means, alteration, deletion or deterioration of computer data shall be sentenced between six months and fifteen years imprisonment and fined from one million Riels to twenty four million Riels.[187]

Article 23 of the draft law introducing offence "illegal interception" of computer data, which resembles Article 3 of the Convention on Cybercrime, however the draft law failed to provide discretion of the criminalization base on "*dishonest intent*" or "*in relation to a computer system*

[182] Ibid, Art.7.
[183] Constitution 1993, *supra note* 123, Art. 51.
[184] Bhagat, R. Separation of power without checks and balance in Cambodia. Journal of Alternative Perspectives in the Social Sciences 2015, 6 (4), pp 389-401, p 390. Available at: http://www.japss.org/upload/3.%20Bhagat.pdf (10.02.2017)
[185] Cambodia Criminal Code 2009, *supra note* 71.
[186] Cybercrime Law, Draft V.1, *supra note* 13, Art 21-26.
[187] Ibid.

that is connected to another computer system".[188] The same issues remain the same in the rest of offenses under the draft law. The offences against computers are drafted in broad terms and failing to make reference to malicious or fraudulent intent, where honest mistakes over the Internet are likely to be caught and penalized.[189] Moreover, Article 19's Executive Director, Thomas Hughes said, "*With a version of the Draft Law released, the authorities can no longer deflect the legitimate concerns of the national and international human rights community*". [190] Cambodia's draft Cybercrime Law falls well below international standards on the rights tor freedom of expression, information and privacy.[191]

Article 28 of the draft law cover the content and websites, which seeks to criminalize online activities that are deemed to "*hinder the sovereignty and integrity of the Kingdom of Cambodia*", "*incite or instigate anarchism*", "*generate insecurity, instability and political cohesiveness*", "*slander or undermine the integrity of any government agencies, ministries*", or "*damage moral and culture values*".[192] Offences commits under the meaning of Article 28 are punishable from one year to three years imprisonment and fined from two million Riels up to six million Riels ($500-$1500).[193] Civil societies concern these offenses extremely vague and open for political abuse, while the sanctions are unreasonable to create another serious threat to freedom of expression. There is no clear explanation of what could cause 'political cohesiveness' or maybe used to silence those who disagree with the decision made by the government. [194]

2.3.4. Investigating Cybercrimes and Collecting Digital Evidence

Gathering of evidence as one of the main challenges in fighting against cybercrime.[195] Cybercrime is different from physical crime in the forms of motive, intent, and outcome of the crime, especially the form of evidence. Investigation of cybercrime is a complicated task because evidence arising out of the electronic discovery process, therefore it is very important for the investigator to understand the level of supplication of the cybercriminal suspects.[196] Digital

---

[188] Convention on Cybercrime, ETS 185, 23.11.2001, Art. 3.
[189] Article 19, Cambodia: Secret Draft Cybercrime Law seeks to undermine free speech online, Article 19, Press release 09. 04. 2014. Available at: https://www.article19.org/resources.php/resource/37516/en/cambodia:-secret-draft-cybercrime-law-seeks-to-undermine-free-speech-online (10.02.2017)
[190] Ibid.
[191] Ibid.
[192] Cybercrime Law, Draft V.1, *supra note* 13, Art. 28.
[193] Ibid.
[194] *Supra note* 177.
[195] Gruodyte, *supra note* 58, p 241.
[196] Worl, O. Computer crime: Factors of Cybercriminal Activities. Int'l J. IJACSIT ISSN 2320-0235, Cloud Publications 2014, 3 (1), pp 51-67, p 53-54.

evidence is breakable, typically it comprise of binary data inscribed on a mass storage device and can contain of something from executable code objects, image or other encrypted electronic content that can be destroyed by inappropriate discovery process. Therefore, only investigators who are computer forensic expert should undertake investigation.[197]

Article 17 of the daft law states that "*for the purpose of gathering evidence, the expeditious preservation of the computer data or the data referring to data traffic, subject to the danger of the destruction or alteration, can be ordered by the prosecutor*".[198] The law required the service providers to make available of users data to competent authority under confidentiality conditions.[199] Prosecutors received huge powers to order the reservation of computer data or traffic data under the draft law and it cause concerns when prosecutor is under political influence or lack the independence necessary for the proper balancing of the diverse interests involved, especially the protection of the right to privacy.[200]

Moreover, the Law on Telecommunications 2015 and draft Law on Cybercrime can further control freedom of expression, information and privacy if they are deemed threaten to national security, national unity, cultures, moral or custom of Cambodian. Defamation and incitement offences under Cambodian law have expanded its jurisdiction over fundamental freedom beyond what is permitted under ICCPR, which Cambodia is a party to, according to statement made by the Special Rapporteur on Human Rights in Cambodia to the Human Rights Council in October 2009.[201]

Collecting of digital evidence is extremely important process in investigating cybercrime. At the same time, various aspects are involved such as balancing between fundamental rights and security. Therefore, applying "Principle of Proportionality" and "Reasonable data management" during cybercrime investigation is a must in order to guarantee that there is no violation of fundamental rights involved in this aspect.[202] Furthermore, it is extremely important for cybercrime investigator to understanding the purposes, personalities, and behaviors of the cybercriminal, and applies different analytical technique on different type of digital evidence in

[197] Ibid.
[198] Cybercrime Law, Draft V.1, *supra note* 13, Art. 17.
[199] Ibid.
[200] Article 19, *supra note* 189.
[201] UN, Report of the special rapporteur on the situation of human right in Cambodia, A/HRC/12/46.
[202] Kasper, A., Laurits, E. Challenges in Collecting Digital Evidence: A Legal Perspective. The Future of Law and eTechnologies. Kerikmäe, T. Rull, A. (Eds.). Springer 2016, p 201.

each particular case for more effective result.[203] To balance the security in privacy, policymakers and citizens must jointly consider the continuum as decomposable into two aspects such as 'identity' and 'behavior', which can be regulate separately to moderate overall balance of privacy and security.[204] The real danger to citizens and security is when individuals or organization have extensive information on both 'Behavior' and 'Action'. The data collection efforts should respect the division between 'identity' and 'behavior' by allowing the government to collect information on behavior, but must place identity knowledge behind.[205]

In European Union, the right to private life is found under Article 8 of the European Convention of Human Right (ECHR). The public authorities must act in accordance with it, and legislation passed by government must compliant with the ECHR.[206] Moreover, under Article 1 of Directive 95/46/EC of the European Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the freedom of movement of such data provides protection to the fundamental right and freedom of natural person, and in particular their right to privacy with regard to the processing of personal data.[207] According to Article 17 of Directive 95/46/EC, "*member states shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing to ensure a level of security appropriate of such measures*".[208]

In addition to Directive 95/46/EC of 24 October 1995, Directive 2002/58/EC of 12 July 2002 also provides protection concerning the processing of personal data and the protection of privacy in the electronic communication sector and was amended by Directive 2009/136/EC of 25 November 2009. According to Article 1, equivalent level of protection of fundamental rights and freedom regarding processing personal data in the electronic communication sectors shall be guaranteed by member states.[209] It is also provides under Article 4 that, the service providers

[203] Cross, M. Scense of the Cybercrime. 2nd ed. United State, Elsevier 2008, p 118.
[204] Demchak, C., Frenstermacher, K. Balancing Security and Privacy in the 21st Century. Intelligence and Security Informatics. Chen, H., *et al*. (Eds.). Second Symposium on Intelligence and Security Informatics, ISI 2004. p 327.
[205] Ibid, p 328.
[206] Edwards, L., Waelde, C. Law and the Internet. 3rd ed. United States, Hart Publishing 2009, p 445.
[207] OJ L 281, 23.11.1995, Art.1.
[208] Ibid, Art. 17.
[209] OJ L 201, 31.07.2002, Art. 1.

must take appropriate technical and organizational measures to safeguard security of its services and shall ensure a level of security appropriate to the risk presented of data.[210]

Member states have obligation to ensure the confidential of communication and the related traffic data by means of a publication communications network and publicly available electronic communication service through national legislation. For the legitimate purpose of this Directive, the member states shall prohibit listening, tapping, storage or other kind of interception or surveillance of communications and the related traffic data by persons other than users.[211] Last but not least, Article 15 of the Directive 2002/58/EC allow member states to adopt legislation measures to restrict the scope of the rights and obligation regarding confidentiality of the communication, traffic data, presentation and restriction of calling and connected line identification, and location data, however such restrict must constitute a necessary, appropriate, and proportionate measure within democratic society to safeguard of national security.[212]

The High Court of Ireland and Constitutional Court of Austria were asking the Court of justice to examine the validity of the directive, in particular in the light of two fundamental rights under the Charter of Fundamental Rights of the EU in respect for private life and the fundamental right to the protection of personal data. The court provided that "even though the retention of data required by directive 2006/24 constitutes a particular serious interferences with those rights, it is not such as to adversely affect the essence of those rights, the directive does not permit the acquisition of knowledge of the content of the electronic communication as such."[213]

Moreover, the competent national authorities to have possible access to those data shall genuinely satisfies an objective in general interest as required by Directive 2006/24. This means that the proportionality of the interference in those circumstances should be existed to be appropriate for attaining the 'legitimate objective' and do not exceed the limits of what is 'appropriate and necessary' in order to achieve those objective.[214] In the case, Directive 95/46 does not require any provision to be adopted, which imposes an obligation on the personal data protection and only 'processing operations carried out'.[215]

[210] Ibid, Art. 4.
[211] Ibid, Art. 5.
[212] Ibid, Art. 15. See also OJ L 105, 13.04.2006, Preamble, Recital 4.
[213] EIKo 08.04.2014, Joined cases C-293/12 and C-594/12, para 39.
[214] Ibid, para 44-46. See also case C-343/09, Afton Chemical, C-581/10 and C-343/09 Nelson.
[215] EIKo 09.11.2010, Joined cases C-92/09, *Volker und Markus Schecke GbR* and C-93/09, *Hartmut Eifert*, § 99.

In the same case the court also point out that, "option of specifying in greater detail of the Directive in to national legislation may pose specific risks to the right and freedom of data subjects, Directive 95/46 provides, as is evidence from recital 54 in its preamble, the number of such operations should be very limited."[216] Investigating cybercrime and collecting of digital evidence need appropriate technical measures and proper legislation and policy that in par with international standard that could balance between fundamental rights and security in cyberspace.[217] The terms being used under Cambodian Telecom Law 2015 and draft law Cybercrime are too vague, which comprise of Internet censorship behavior and impose a severe threat to fundamental freedom guarantee under international human rights law.[218]

[216] Ibid, para 105.
[217] Agnes (2016), *supra note* 202.
[218] Article 19, *supra note* 189.

2.4. Conclusion

Cambodia has significant achievements in the past few years in the field of legal and policy framework, institutional framework, awareness and coverage and service for ICTs development. As result, RGC adopted ICT Master Plan 2020 in 2014 in the line with ASEAN ICT Master Plan 2020 and ITU Connect 2020 Agenda. The Law on Telecommunications also adopted in 2015 for regulating telecommunications industry, role of MPTC and Telecommunication Regulator of Cambodia (TRC) and foundation and principles for establishing regulation on numbering plan, licensing regime, spectrum, etc.

RGC also adopted Telecom/ICT Development Policy 2020 in April 2016. There are some other laws and policies are being drafted includes: draft law on Cybercrime, draft law on E-commerce, and draft of Spectrum regulation. Last but not least, RGC has been integrated NiDA into the MPTC's structure in 2013 and established TRC in 2015 in order to formulate the regulations, relating to the operation and provision of telecommunication in the line with the RGC's policy on the telecommunication sector. However, achievements come along with number of challenges.

Cambodia lacks of adequate and comprehensive strategy, policy and regulation frameworks, which constrain the effective oversight of this sector. If compare to other nations in the region, Cambodia and Lao are the slowest in term of establishment the legal framework concerning ICT sector. Cambodia also needs to strengthen and coordinate institutional mechanisms ineffective response of human resources and level of IT literacy to cope with the fast growth of modern Technology.

Last but not least, Cambodia also needs more competitiveness of Cambodia's mobile cellular and Internet services compared o the neighboring countries. Strengthen cooperation and coordination among operators and between the operators and supervisory authority, enhance the effectiveness of investment and utilization of physical infrastructure and to expand the coverage and enhance efficiency of backbone infrastructure is needed in order to reach connectedness and readiness for the sustainable development in the ICT sector.

3. International Human Rights Aspects in Cyberspace

3.1. Freedom on the Internet

The expansion of the Internet over the last few years have a huge contribution to social and economical develop and has change the way people live and communicated on a global scale. The Internet now serves as a primary source of information and increasingly recognized as having a potentially positive influence on activism in the developing countries. Growing of Internet penetration and ICT development become another motivation for youth to get involvement in social, political and economic activism.[219] Due to the expansion of Internet network and modern ICT tools, cyberspace is become even more convenient to conduct criminal activities 'cybercrime' and the risks is much more greater than the traditional crime ever. Therefore, specific regulations and mechanisms are very important to ensure the safeguard in cyberspace.

Cambodia known as the home for largest adolescent in the region, while 68% of the total population is under 30-year old and active online. [220]

Total Population	**15,827,241 (68% Under 30)**	
Active Internet Users	7,157,409	
Active Social Media Users	4,900,00	
	Facebook Users	Other
	4,800,000	
Active Mobile Social Users	4,400,000	

Figure 8. Internet penetration and social media statistic in Cambodia, 2016.[221]

New medias and increasing of Internet access transform information environment in Cambodia and change opinion expression behavior. Through the use of new medias and digital tools, young activists of both genders are able to circulate views on important social and political issues. However, the government has made sporadic attempts to control Internet usage. Authorities have

[219] Chak, S. New Information and Communication Technologies' Influence on Activism in Cambodia. SUR Int'l J. on Hum Rts 2014, 20, p 437. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2553249 (13.10.2016)
[220] Sokha, C. Presentation on ICT Development in Cambodia. CICC Forum, Tokyo, December 2015. Available at: http://www.cicc.or.jp/japanese/kouenkai/pdf_ppt/pastfile/h27/151013-2kh.pdf (10.01.2016)
[221] Joseph Soh, "Cambodia's 2017 Social Media and Digital Statistics", *supra note* 12.

begun to interfere with ICT access by blocking at least three blogs hosted overseas on multiple ISPs for content that criticized the government since 2011. Compared to traditional media in Cambodia, new media, including online news, social networks and personal blog, enjoy more freedom and government censorship and restriction. In 2012 the authorities continued to threat the Internet users of its draft Cambodia Cybercrime Law in order to control online behavior. [222]

ICTs has the potential contribution social development by improve transparency and accountability as well as provide a wide range of opportunities to advocate for democracy and human rights in Cambodia. Individual can access information more easily and able to distribute the information about human rights violation and method of resistance, express their concerns, and access wider international audience. The draft of Cybercrime law was the most concerning development for Cambodian online community. The draft law use of existing criminal defamation and incitement offence from the 2009 Criminal Code to limit freedom of expression by legislate them into Cybercrime law and impose more serious sanctions.[223]

On of Cambodia's well-known young bloggers, OU Ritthy has been hosting "Politikoffee" since 2011. Politikoffee is a group of young, enthusiastic and social media savvy Cambodian who love discussing socioeconomic, political developments and democratization in Cambodia and the region. They create platforms for youth debate and discussion on political and other important sector. Politikoffee members actively participate in debate and discussion via Politikoffee media such as website and Facebook group. Moreover, this group also meet up weekly to discuss and debate on most pressing issues through series guest speaker including members form different political parties in Cambodia.[224] Ritthy expressed his concerns that "if the is law is passed, my peers and I will be more cautious with our political expression despite the fact that we have never defamed or abused any ruling official."[225]

Another 29-year old, Lack Vannak, co-founder of Politikoffee and former program officer of ICTs for Human Rights at Diakonia international organization, said the project was focus on developing ICT tool to promote human rights and freedom of expression in Cambodia. He said, "If the government passes this law, without amendment of some articles and proper

[222] CCHR, Cyber Laws: Tools for Protection or Restriction Freedom of Expression? CCHR Briefing note February 2014, p 2-3. Available at: https://www.ifex.org/cambodia/2014/03/03/cambodia_cyber_crimes_legislation_cchr.pdf (15.10.2016)
[223] Chak (2014), *supra note* 219, p 440.
[224] About Politikoffee. Available at: http://politikoffee.com/about-us/ (10.01.2017)
[225] Peter, Z. "Cambodia's bloggerati fear new Internet law", 04.05.2014. Available at: http://www.aljazeera.com/indepth/features/2014/05/cambodia-bloggerati-fear-new-internet-law-201454115127157534.html (10.01.2017)

implementation, cybercrime law will become a serious threats to freedom of expression and privacy in this country."[226]

Cambodia Cybercrime law has been drafted behind the close door, with the government so far refusing any input from civil societies.[227] In addition to this, in late 2014, the Council of Ministers' Press and Quick Reaction Unit announced the creation of a "Cyber War Team" with the stated aim of monitoring all online activity to "protect the government's stance and prestige", while the ministry of Interior announced that it would install surveillance equipment in all Cambodia's mobile phone network and ISPs.[228]

Civil societies concerns that the drafting without any consultation will is widely expected to contain restrictive provision for freedom of expression and privacy right in the Internet users. The Cambodian's Cybercrime law might be drafted with two main objectives. First is to ensure the implementation of law, anti-cybercrime and combating the all kinds of offenses commit by computer system. Second is to ensure safety and prevent all legitimate interests in using and developing technology. However, legal experts, human right activists, and technical experts on ICT viewed the draft law in its current form as broad, vague, and restriction on the freedom of expression rather than cybercrime.[229]

According to the compilation of the report submitted CSOs to the United Nations Human Rights Council during the 18th session of Universal Periodic Review (UPR) of the Kingdom of Cambodia, CSOs seek civil society input on the Cyber Crimes Law and ensure that the law complies with international human rights standards and does not contain any vague or restrictive provisions that could jeopardize online freedom. Moreover, refrain from blocking websites, which should always be considered a disproportionate measure because of associated risks of over blocking. In addition, and in any event, any such order should be made, if at all, only by a court or other independent adjudicatory bodies. [230]

---

[226] Interview with Mr. Lach Vannak on 24.02.2017.
[227] Carmichael, R., "Cambodia's Draft Cybercrime Law Worrying, Say Critics", VOA News, 25 April 2014. Available at: http://www.voanews.com/a/cambodias-draft-cybercrime-law-worrying-say-critics/1900884.html (10.01.2017)
[228] Blomberg, M. Naren, K., "Cyber War Team' to Monitor Web. The Cambodia Daily", 20 November 2014. Available at: https://www.cambodiadaily.com/archives/cyber-war-team-to-monitor-web-72677/ (10.01.2017)
[229] CCC, Minute of Consultative Meeting on the draft of Cybercrime Law, 05 June 2014. Available at: https://www.ccc-cambodia.org/downloads/events-archive/2014/cybercrime-draftlaw/Cybercrime%20Law_Minute_Meeting.pdf (10.01.2017)
[230] CHRAC, Compilation of the reports submitted by CSOs to UNHRC during 18th session of UPR of the Kingdom of Cambodia, July 2013, p 20. Available at: http://sithi.org/upr/docs/Compilation_of_Reports_CHRAC.pdf (25.11.2016)

3.2. Cambodia's legal obligation

There are a number of legal number of cases study last few years where the courts used to curtail the freedom of expression in the country, namely through charges of defamation, disinformation and incitement. According to the leaked draft cybercrime law, the most distressing of the cybercrime law's provisions is Article 28, which allows to be imposed for any electronic communication deemed to "hinder the sovereignty and integrity of the Kingdom of Cambodia...[or] incite or instigate the general population." Article 28 also allows those same penalties to be imposed for any publication or republication "deemed to generate insecurity, instability, and political cohesiveness...[or that] slanders or undermined the integrity of any governmental agencies, ministries...[or is] damaging to the moral and cultural values."[231]

This language in this draft law is exceedingly vague and exposed a dangerous drift away from international human rights standards regarding freedom of expression, access to information and right to privacy on the Internet. Author will go through Cambodia's legal obligation concerning human rights, particular link to cyberspace in the following sections.

3.2.1. National's legal obligation

Constitution of the Kingdom of Cambodia adopted in 1993, the supreme law, was a result from the agreement of Paris Peace Accord in 1991.[232] According to Article 150 (new)[233], the present Constitution is the supreme law, all laws and decisions of all the state institutions must be absolutely in conformity with the Constitution.[234] The highest law of provides in its Article 31 (1) that Cambodia recognizes and respects human rights as enshrined in the United Nations Charter, the Universal Declaration of Human Rights and all the treaties and conventions related to human rights, women's rights and children's rights.[235] Therefore, all legal frameworks shall guarantee the human rights of the Cambodian.

Freedom of express, access to information, and privacy are the fundamental human rights guaranteed under the highest law in the Kingdom. Khmer citizens shall have the freedom to express their personal opinions, the freedom of press, of publication and of assembly. No one

---

[231] Cybercrime Law, Draft V.1, *supra note* 13, Art.28.
[232] CCIM, Report on Challenges for Independent Media Development in Cambodia, March 2013, p 3. Available at: http://www.ccimcambodia.org/report/CCIM_report_indepedent_media_promotion.pdf (20.12.2016)
[233] The 1993 Constitution of the Kingdom of Cambodia last revisions and amendments in 2008 on some article. Article 150 on the effect, the revision and the amendment of the Constitution was former Article 131.
[234] Cambodian Constitution 1993, Art.150.
[235] Ibid. Art. 31.

can take abusively advantage of these rights to impinge on dignity of others, to affect the good mores and custom of society, public order and national security.[236] The right to freedom of expression is enshrined in Article 41 of the Cambodia's Constitution, however Cambodia has a poor record of honoring the human right in practice and in several substantial laws in the Kingdom, the government and ruling party CPP maintain strong control over the media and do not support freedom of the press in Cambodia.[237]

During the national elections last July 2013, 55 of 123 seats at the National Assembly were taken away from ruling party CPP. The opposition party CNRP won 55 seats was the historic change of democratic process in Cambodia and people believe that social media was the main factor for this historical election result in July 2013. [238] The fundamental rights guaranteed under Constitution are threatened by the Criminal Code due to the government increasing using criminal defamation and incitement law to intimidate critics. Individual can be arrested for disturbing public order or affecting the dignity, at least 12 persons imprisonment under such law for peaceful expression of view since 2010, according to human right watch.[239]

While draft of Cybercrime law is in the controversial discussion, the National Assembly passed a Telecommunication Law in November 2015, which significantly undermined the body's stated goal of reducing centralized state control.[240] Article 6 of the Telecommunication Law obliges the telecommunications service provider to provide data on their users to government authorities, even if they are not presented with judicial warrant. Article 97 allows secret surveillance of any and all telecommunications where it is conduct with the approval of a legitimate authority. The Special Rapporteur Rhona Smith highlighted that the Telecom law is vague, clear implementation guidelines reflecting prevailing international human rights should be carefully drafted and disseminated in order to ensure that the law is applied in a manner that regulates without unnecessarily restricting the activities of civil society bodies, trade unions and human

[236] Ibid. Art. 41.
[237] CCIM (2013), *supra note* 152, p 19.
[238] Kennedy, V. Pineros, E., " Opposition rejects Cambodia electon results, call for investigation", CNN, 29 July 2013. Available at: http://edition.cnn.com/2013/07/29/world/asia/cambodia-elections/ (10.01.2017)
[239] Human Rights Watch, Word Report 2012: Cambodia, HRW 2011. Available at: https://www.hrw.org/world-report/2012/country-chapters/cambodia (20.12.2016)
[240] Freedom House, Freedom in the Net: Cambodia. 2016. Available at: https://freedomhouse.org/sites/default/files/FOTN%202016%20Cambodia.pdf (10.01.2017)

rights defenders. She urged that particular care should be taken to ensure respect for freedom of expression when arresting, detaining and prosecuting those posting materials on social media.[241]

According to the statement released by LICADHO, the new telecoms law that it labeled a severe threat to freedom of expression and private communication that hid behind the facade of technical intent.[242] Also a legal analysis conducted by LICADHO provides that the telecoms law "allow the government to secretly intrude into the private lives of individuals, destroy evidence before criminal trials, and seize control of the entire telecoms industry if arbitrarily deemed warranted. Its excessive measures, particularly those creating new criminal offenses, reveal the true intent of the law: to intimidate individuals, punish the exercise of fundamental rights and freedoms and quash individual and group dissent."[243]

3.2.2. Regional's legal obligation

ASEAN was established in August 1967 in Bangkok, Thailand. The primarily purpose of the ASEAN was to accelerate the economic growth, social progress and culture and development in the region. Moreover, it aimed at promoting regional peace and stability through abiding respect for justice and the rule of law in the relationship among countries of the region.[244] Cambodia become the last member of ASEAN in 1999 and party to "Bangkok Declaration"[245]. ASEAN established the ASEAN Intergovernmental Commission on Human Rights to promote human rights in 2009. The Commission drafted the ASEAN Declaration of Human Rights, which was unanimously adopted by all member states in November 2012. The Declaration provides a provision to guarantee all the civil and political rights in the UDHR in order to fit the international human rights standard to all ASEAN member states.[246]

Article 21 of the ASEAN Declaration on Human Rights provides that "every person has the right to be free from arbitrary interference with his or her privacy, family, home or correspondence

---

[241] Telecom Asia, UNHR blasts Cambodian Telecoms, cybercrime laws, October 03, 2016. Available at: http://www.telecomasia.net/blog/content/unhr-blasts-cambodian-telecoms-cybercrime-laws (10.01.2017)
[242] LICADO, New Law on Telecommunications: A Legislative Attack on Individuals' Rights and Freedoms. Available at: https://www.licadho-cambodia.org/pressrelease.php?perm=401 (10.01.2017)
[243] LICADO. Cambodia's Law on Telecommunications A Legal Analysis. March 2016. p 1. Available at: https://www.licadho-cambodia.org/reports/files/214LICADHOTelecomsLawLegalAnalysis_March2016ENG.pdf (10.01.2017)
[244] About ASEAN. Available at: http://asean.org/asean/about-asean/history/ (15.01.2017)
[245] ASEAN Declaration is the founding document of Association of Southeast Asian Nation of 08.08.1967, hereby refer to "Bangkok Declaration". Available at: http://asean.org/the-asean-declaration-bangkok-declaration-bangkok-8-august-1967/ (15.01.2017)
[246] ASEAN Declaration on Human Rights, 09.11.2012. Available at: aichr.org/?dl_name=ASEAN-Human-Rights-Declaration.pdf (15.01.2017)

including personal data, or to attack upon that person's honor and reputation. Every person has the right to the protection of the law against such interference or attacks."[247] We can see the intents of this article clearly that the right of individual in guaranteed in the line of UDHR, however there no specific guideline for the implementation of this instrument. As result, ASEAN cannot reach its legitimate purposes of the convention among member states.

In addition to above article, Article 5 of the 2000 e-ASEAN Framework Agreement signed at 4th ASEAN International Summit provides that member state shall adopt electronic commerce regulatory and legislation frameworks that create trust and confidence for consumers and facilitate the transformation of business toward the development of e-ASEAN. It further provides that member states shall expeditiously put in place national laws and policies relating to electronic commerce transaction based on International Norms; … [5] take measures to promote personal data protection and consumer privacy.[248] Another fundamental right, particularly data protection and privacy were found in ASEAN Agreement for establishing e-ASEAN. However, 17 years after signed this agreement, Cambodia show its slowness since many regulations concerning the field still in the drafting process includes cybercrime law, e-Commerce while other nice member state already enacted those laws.

Article 23 of the ASEAN Declaration on Human Right focus on freedom of expression. This article provides that "every person has the right to freedom of opinion and expression, including freedom to hold opinions without interference and to seek, receive and impart information, whether orally, in writing or through any other medium of that person's choice."[249] Cambodia is bound to ASEAN's legal obligation that it is party to as described above. But unfortunately, the current draft law on Cybercrime Law of Cambodia seems to provide vague provision that can be a serious infringement to above rights.

3.2.3. International's legal obligation

Freedom of expression, information and privacy are fundamental human rights protected under international human rights conventions and other regional human rights treaties such as American Convention on Human Rights, European Convention on Human Rights, African Charter on Human and Peoples' Rights including ASEAN Declaration of Human Rights. The

[247] Ibid. Article 21.
[248] 2000 e-ASEAN Framework Agreement, 24.11.2000. Available at: https://cil.nus.edu.sg/rp/pdf/2000%20e-ASEAN%20Framework%20Agreement-pdf.pdf (15.01.2017)
[249] ASEAN Declaration on Human Rights. *Supra note* 246, Art.23.

rights above are equally important, however they are not absolute. Certain rights may be restricted for the protection of other rights and national security.[250]

Members of the UN and of the signatories to international treaties are assuming obligation under international laws to respect, to protect and to fulfill human rights. UDHR provides a set of basic human rights standard that at least all member state should achieve at the minimum level. Preamble of the UDHR recognizes that "*the equal and inalienable rights of all members of the human family are the fundamental of freedom, justice and peace in the world*".[251] Unfortunately, the fundamental rights standards are not being achieved in the online context until UNHRC adopted a resolution affirming the application of human right in cyber aspect in 2012, especially freedom of expression.

During the 20th session, the Human Rights Council recalling all relevant resolution of the commission on Human Rights and Human Rights Council on the right to freedom of opinion and expression, particular Council resolution 12/16 of 02 October 2009, and also recalling General Assembly resolution 66/184 of 22 December 2011 and affirms that *" the same rights that people have offline must also be protected online, particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with article 19 of the UDHR and ICCPR."* The resolution based on the exercise of human rights; in particular the freedom of expression, on the Internet is an issue of increasing interest and importance due to the rapid grow of technology.[252]

3.2.3.1. International Covenant on Civil and Political Rights (ICCPR)

Cambodia ratified the ICCPR on 25 May 1992, therefore Cambodia have obligation to "respect and ensure" individual right within its territory.[253] Moreover legislative or other measures adopt by individual state party must be in accordance with its constitutional processes and with the provisions of the Covenant.[254] The state also undertakes to submit periodic reports on the measure they have adopted (reporting system)[255] as well as establish the competence of the

[250] Mendel, T., Salomon, E. Freedom of Expression and Broadcasting Regulation. A Debates series, UNESCO 2011, 8, p 9-10. Available at: http://unesdoc.unesco.org/images/0019/001916/191623e.pdf (15.03.2017)
[251] UDHR, GA/RES/3/217A of 10 December 1948.
[252] UNHRC Resolution on the promotion, protection and enjoyment of human rights on the Internet. A/HRC/20/L.13, 29.06.2012.
[253] International Covenant on Civil and Political Rights, GA/RES/21/2200A, 23.03.1976, Art.2.
[254] Ibid.
[255] Ibid, Art.40.

committee to received and consider communications (inter-state)[256] and individual complaint system.[257] Implementation of the Covenant is the state responsibility and an international obligation requiring the achievement of a certain result for the protection and promotion of human rights. The state must responsible for the treaty breach and the breach of customary international law.[258]

Article 17 of the ICCPR provides that "no one shall be subjected to arbitrary or unlawful inference with his privacy … correspondence" and "everyone shall have the right to the protection of the law against such interference or attack."[259] According to general comment No.16 adopted by UN Human Rights Committee, rights provides under Article 17 is required to be guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal person.[260] For certain circumstances interference may be permitted, however it must be very limited and must be made only by authority designated under the law. Surveillance, including electronic, telephonic, telegraphic, and other forms of communications is prohibited.[261]

Data privacy law aimed at safeguarding certain interest and right of individuals. There are several core principles for the better protection of data privacy such as principle of fair and lawful processing, principle of minimality, principle of purpose limitation, principle of data quality, principle of data security and data subject influence.[262] Moreover, other several principle adopted by OECD apply to personal data in both public or private sectors, which should be protected by security safeguards against such risk as loss or unauthorized access, destruction, use or modification or disclosure of data[263] regardless whether those acts emanate from State authorities or from natural or legal person.[264] OECD issued important guideline on privacy and

[256] Ibid, Art.41.
[257] Fobr, A. Domestic Implementation of the International Covenant on Civil and Political Rights Pursuant to its article 2, para.2. Max Planck UNYB 2001, 5, p 400. Available at: http://www.mpil.de/files/pdf1/mpunyb_seibert_fohr_5.pdf (18.02.2017) see also First Optional Protocol to ICCPR for establishing individual complaint mechanism for ICCPR adopted by UN General Assembly on 16.12.1966 and entry into force on 23.03.1976.
[258] Tams, C. Enforcing Obligations *Erga Omnes* in International Law. New York, Cambridge University Press 2005, p 252.
[259] *Supra note* 253, Art. 17.
[260] UNHRC, CCPR General Comment No.16: Article 17 on Right to Privacy, HRI/GEN/l/Rev.9 (Vol. I), 1988, para.1.
[261] Ibid, para.8.
[262] Bygrave, L. Data Privacy Law: An International Perspective. Oxford, Oxford University Press 2014, p 1-2.
[263] OECD, Recommendation of the Council concerning Guideline Governing the Protection of Privacy and Transborder Flows of Personal Data, 2013, p 13-15. Available at: https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (18.02.2017)
[264] *Supra note* 260.

data protection in 1980, although it do not form binding internal law, it may seem highly influential and were used together with CoE Data Protection Convention 1981 as template for the introduction of national legislation in many countries in Europe.[265]

Article 8 of CoE Data Protect Convention also guarantee the right to respect for his private and correspondence.[266] According European Court of Human Right, private life includes the privacy of communication, which covers the security and privacy of mail, telephone, e-mail and other forms of communication including information derived from the monitoring of the personal Internet usage.[267] Moreover, monitoring via technological means and the processing and use of data obtain without consent, systematic collection and storing of data by security services on particular individuals, even without the use of covert surveillance methods, thereby amounted to an interference if private life protected under Article 8.[268] Interference by law is permitted under section two, however it must be for necessity in a democratic society and proportionate to the legitimate aims pursued under this article.[269]

In addition to privacy protection, ICCPR also guarantee the freedom of expression under Article 19. Article 19 (2) provides that "Everyone shall have right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, … any other media of his choice."[270] Paragraph two of this article requires state parties to guarantee the right to freedom of expression in all forms includes political discourse, commentary on one's own and on public affairs, discussion of human rights, cultural and artistic expression, teaching and religious discourse.[271] The Committee reiterates that the right to freedom of expression in Article 19 (2) includes the right of individuals to criticize or openly and publicly evaluate their Governments without fear of interference or punishment.[272]

According to Council resolution 12/16 of 02 October 2009 and General Assembly resolution 66/184 of 22 December 2011, freedom of expression is protected equally both offline and online

[265] Casagran, C. Global Data Protection in the Field of Law Enforcement. New York, Routledge 2017, p 227-229.
[266] Council of Europe (CoE), Convention for the Protection of Individual with regard to Automatic Processing of Personal Data, ETS 108, 28.1.1981, Art.8.
[267] EIKo 03.04.2011, 62617/00, *Copland vs. the United Kingdom*, § 41, 44.
[268] EIKo 02.09.2010, 35623/05, *Uzun vs. Germany*, § 44-46.
[269] Ibid, § 78.
[270] *Supra note* 253, Art. 19, § 2.
[271] UNHRC, General Comment No.34: Article 19 on Freedom of Opinion and Expression, CCPR/C/GC/34, 2011, § 11-12.
[272] U.N. Doc. CCPR/C/83/1128/2002, *Rafael Marques de Morais vs. Angola*, § 6.7.

under Article 19 of the UDHR and ICCPR.[273] Therefore, everyone shall be freed from censorship and unconstrained of press or other media to ensure the enjoyment of the rights provides by this covenant.[274] Moreover, state parties should undertake particular measure to protect the rights of media use and encourage an independent and diverse media for citizens to receive a wide range of information and exchange of ideas via Internet and mobile-based electronic information dissemination system.[275]

Freedom of expression may be restricted for the purpose of protection for the right or reputation of others, national security, public order or morals.[276] Everyone shall enjoy the freedom of expression, any restriction must be providing by law and pursuant with paragraph 3 of Article 19 and they must conform to the strict tests of necessity and proportionality.[277] States parties should put in place measures to protect against attacks aimed at silencing those exercising their right to freedom of expression such as arbitrary arrest, torture, threat to life and killing. [278]

A Cambodian university student imprisoned for calling for a "color revolution" in his Facebook post. Kong Raya, a 25-year-old student, was convicted of incitement to commit a felony for making a posting on his Facebook page asking if anyone would "dare to make a color revolution with me?" Phnom Penh Municipal Court sentenced him to 18 months in March 2016. Am Sam Ath, monitoring manager for rights group Licadho said, " it is a strategy and an example to hinder or threaten the expression of other youth."[279] Raya's lawyer, Sam Sokong said, it is an absurd punishment for a young man guilty 18 months for expressing himself online. He continued that the freedom of expression was violated in Cambodia and the sentence itself is serious based on the law while Incitement receive maximum penalty of 2 years under Criminal Code 2009.[280]

[273] *Supra note* 252.
[274] *Supra note* 271, § 13.
[275] Ibid, § 14-15.
[276] *Supra note* 253, Art. 19, § 3.
[277] *Supra note* 271, § 22. See also U.N. Doc. CCPR/C/89/D/1353/2005, *Njaru vs. Cameroon*, 03.04.2007, § 6.4.
[278] *Supra note* 271, § 23.
[279] Khy Sovuthy, "Supreme Court Hears 'Color Revolution' Facebook Case", The Cambodia Daily, 24.12.2016. Available at: https://www.cambodiadaily.com/news/supreme-court-hears-color-revolution-facebook-case-122430/ (10.01.2017)
[280] Ouch Sony, "Taylor O'Connell, Student gets 18 month for call for 'Color Revolution'", The Cambodia Daily, 16.03.2016. Available at: https://www.cambodiadaily.com/news/student-gets-18-months-for-call-for-color-revolution-109944/ (10.01.2017)

3.2.3.2.International Covenant on Economic Social and Cultural Rights (ICESCR)

Under Article 1, paragraph 1 of ICESCR guarantee the right of self-determination, everyone can enjoy freely determine their political status and freely pursue their economic, social and cultural development.[281] Cambodia ratified ICESCR on 26 May 1992, this mean the Cambodia have responsibility for administration of non-self-government and Trust Territories, shall promote the realization of the right of self-determination, and shall respect that right provide by this Covenant and the Charter of the United Nation.[282]

Article 15 (1) (a) guarantee the rights to "take part in cultural life"[283], to "enjoy the benefit of scientific progress and its application"[284] and to "benefit from the protection of the moral and material interests resulting from any scientific, literary or artistic production or which he is the author."[285] The rights to take part in cultural life can be characterized as a freedom and integral part of human rights the same as other rights.[286] The Covenant imposes on State parties the immediate obligation to guarantee that the right set out in Article 15 paragraph 1 (a) is exercise without discrimination, to recognize cultural practice and to refrain from interfering in their enjoyment and development.[287]

The CESCR adopts in general comment a broad concept of culture, which includes all manifestation of human existence and is conceived as a living process historical, dynamic and evolving.[288] Everyone have right to participate in cultural life alone or in association with other or as a community. Moreover, they can act freely in choosing their own identity, to be identified or change their choice, to take part in political life of society, and to engage in one's own cultural practice. Everyone also has the right to seek and develop cultural knowledge and expression and to share them with other, as well as to act creatively and take part in creative activity.[289] Therefore, states parties have a duty to implement their obligation under this article and other

[281] International Covenant on Economic Social and Cultural Rights, GA/RES/21/2200, 16.12.1966, Art. 1. § 1.
[282] Ibid, Art. 1. § 3.
[283] Ibid, Article 15, § 1 (a).
[284] Ibid, Article 15, § 1 (b).
[285] Ibid, Article 15, § 1 (c).
[286] CESCR General comment No.21 on Right of everyone to take part in cultural life Art.15, para. 1 (a), E/C.12/GC/21, 20.11.2009, § 1, 6.
[287] Ibid, § 44.
[288] Odello, M. The Right to Take Part to Cultural life: General Comment No.21 of the United Nations Committee on Economic, Social and Cultural Rights. Anuario Español De Derecho Internacional 2011, 27, pp 493-521, p 500. Available at: https://www.unav.edu/publicaciones/revistas/index.php/anuario-esp-dcho-internacional/article/viewFile/2563/2436 (21.02.2017)
[289] *Supra note* 286, § 15 (a)

provision of Covenant and international instruments, in order to promote and protect the entire range of humans guaranteed under international law.[290]

3.2.3.3. UN Convention on the Rights of the Child – the optional protocol on the sale of children, child prostitution and child pornography

Cambodia ratified the Convention on the Rights of the Child (CRC) on 15 October 1992 and party to its Optional Protocol on the Convention on the Right of the Child on the sale of children, child prostitution and child pornography in 30 May 2002. The CRC is the main international instrument of the protection of children's rights, including from all forms of abuse, violence, neglect and exploitation.[291] Article 34 of the Convention provides that States Parties undertake to protect the child from all forms of sexual exploitation and sexual abuse [292] and shall prohibit the sale of children, child prostitution and child pornography.[293] Moreover, states shall undertake all appropriate national, bilateral and multilateral measures to ensure at least a minimum standard of child protection.[294]

Article 2 (c) of the Optional Protocol provides that "child pornography means any representation, by whatever mean, of child engaged in real or simulated explicit activities or any representation of the sexual parts of a child for primarily sexual purpose."[295]According to observation report submitted by Committee on the Right of the Child 2015, Cambodia adopted National Plan of Action against Trafficking and Sexual Exploitation of Children (2011-2013) and new action plan for the period of 2014-2018. However, the committee viewed that measures undertaken by the State Party in areas covered by Optional Protocol have no been sufficient enough due to delays in its adoption and implementation.[296]

[290] Ibid, § 17.
[291] UNICEF, Handbook on the Optional Protocol on the Sale of Children, Child Prostitution, and Child Pornography. Florence, UNICEF 2009, p 1. Available at: https://www.unicef-irc.org/publications/pdf/optional_protocol_eng.pdf (20.02.2017)
[292] Convention on the Right of the Child, GA/RES/44/25, 20.11.1989, Art.34.
[293] Optional Protocol to the Convention on the Right of the Child on the sale of children, child prostitution and child pornography, GA/RES/54/263, 25.05.2000, Art.1.
[294] *Supra note* 292, Art.34-35. See also *supra note* 293, Art.1.
[295] *supra note* 293, Art.2 (C).
[296] UNCRC, Concluding observations on the report submitted by Cambodia under article 12, paragraph 1, of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, CRC/C/OPSC/KHM/CO/1, 26.02.2015. Available at: http://www.refworld.org/publisher,CRC,,KHM,566e85009,0.html (20.02.2017)

3.2.3.4. The Convention on Cybercrime of the Council of Europe

The Convention on Cybercrime of the Council of Europe entered into force on 01 July 2004 and it the only binding international instrument on Cybercrime. The Convention aims at harmonizing the domestic criminal substantive law elements of offences and connected provision in the area of cyber-crime.[297] It is also providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form.[298] Last but not least, the Convention setting up a fast and effective regime of international cooperation.[299]

Cambodia is not a signatory to the Convention on Cybercrime while many non-European states have signed this convention including countries from Asia Pacific such as Philippines, Japan, and Sri Lanka.[300] According to the current draft law on Cybercrime of Cambodia, many articles resembled CoE Convention on Cybercrime, however some of concrete terms were taken out. For example, Article 23 of the draft law introducing offence "illegal interception" of computer data, which resembles Article 3 of the Convention on Cybercrime, however the draft law failed to provide discretion of the criminalization base on "*dishonest intent*" or "*in relation to a computer system that is connected to another computer system*".[301] The same issues remain the same in the rest of offenses under the draft law. The offences against computers are drafted in broad terms and failing to make reference to malicious or fraudulent intent, where honest mistakes over the Internet are likely to be caught and penalized. [302]

3.3. Amending draft law for Cambodia to comply with human rights standards

Cybercrime law has been drafted in secrecy behind closed door by Cambodian government without any initiatives from civil societies. Cybercrime law could be a dangerous instrument if it is enacted, because it could easily be used to infringe fundamental rights and freedom or target activists and those who criticize against the government.[303] The draft law itself fails to address

[297] CoE, Explanatory Report to the Convention on Cybercrime, ETS 185, 21.11.2001, § 16. Available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b (28.02.2017)
[298] Ibid.
[299] Ibid.
[300] CoE, Chart of signatory and ratification of Treaty 185, The Convention on Cybercrime. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures (28.03.2017)
[301] *Supra note* 188.
[302] *Supra note* 189.
[303] Gerry QC, F., Moore, C. A slippery and inconsistent slope: How Cambodia's draft cybercrime law exposed the dangerous drift away from international human right standards. Computer Law & Security Review, Elsevier 2015, 31, pp 628-650, p 639. Available at: https://doi.org/10.1016/j.clsr.2015.05.008 (25.11.2016)

the cybersecutiy issues, but tend to impose sanction against those who seeks to exercise their fundamental rights and freedom instead. As mentioned earlier, special rapporteur to Cambodia and Article 19 said the current draft law is well bellow the international standard, the government needs to amend the draft law to reflect its international obligation.[304]

According to Mačák, states have shown reluctance behavior to contribute toward the development of cyber-specific customary international rules. In addition, the states practice in the area is being certainly hidden in secrecy and has been reluctant to offer clear expression on matters related to cyber security.[305] General applicable rules of international law apply to state's conduct in cyberspace as accepted by states. Therefore, if customary international law is to be an efficient government structure; it must be adaptable new phenomena without the need of to reinvent an entire regulation framework on each occasion.[306]

In general, various cyber regulations often do not use consistent terminology and it tends to focus on domestic cyber issues that are viewed as being detached from broader global trends. Moreover, provisions of the regulation are vague and may not be well positioned to keep pace with rapidly advancing technology.[307] The draft law on Cybercrime must be redrafted in order to reflect the necessity for the balance of fundamental rights and regulation concerning security in cyberspace. The definition of each offences of the draft law should be more specific in the narrow scene to avoid inconsistent interpretation and giving too much power to law enforcement officers.[308]

Article 28 concerning the content on website of the draft law should be removed, because the definition are too vague and overlapping with the provisions provides under Criminal Code 2009 and Press Law 1995. According to the legal principles, Article 28 should be useless and cannot be used to punish anyone, but too weak and easy to be politically influence. In Cambodia this article can be interpreted to punish anyone who criticize the government or any high ranked or powerful person. Furthermore, defamation and incitement under this article can be used to infringe the freedom of expression guaranteed under Article 19 of the UDHR and ICCPR. The

[304] Ibid, p 642.
[305] Mačák, K. Is the International Law of Cyber Security in Crisis? 2016 8th International Conference on Cyber Conflict: Cyber Power. Pissanidis, N., *et al* (Eds.). NATO CCD COE Publications 2016, p 130.
[306] Ibid, p 131-132.
[307] Shackelford, S., Kastelic, A. Toward a state-centric cyber peace?: Analyzing the role of national cybersecurity strategies in enhancing global cybersecurity. N.Y.U.J. Legis. & Pub. Pol'y 2015, 18, pp 895-984, p 932.
[308] *Supra note* 189

punishment and fines of defamation and incitement offences commits online are excessively serious if compare to punishment impose in the current Criminal Code.

In addition to above issues, cybercrime investigating procedure and collecting of evidence under chapter 3 of the draft law fails to provide appropriate measure and higher legal standard that could protect the right to privacy and data protection of individuals.[309] Specific explanation on the investigation measures and proportionality test is needed to ensure rights on private life and data protection is guaranteed under the national legislation.

Last but not least, the draft law also gives legislative power to Prime Minister on behalf of chairman of NACC and other executive members. Cambodia should not establish NACC, because it could have political influence to the implementation of this law. Composition of cybercrime investigation team should be independent and are cyber technical experts; therefore Cambodia should focus more on capacity building, international cooperation and raising awareness.

Finally, government should open for public opinion and it is better to have drafting working group, which consist of representative from various stakeholders. RGC should commit to common human rights standard though balancing the cyber law and procedures to combat cybercrime and improve cybersecurity, without compromising human rights. Cambodia should sign and ratify the existing Convention on Cybercrime and implement it in the harmonized way[310] and achieve the standard and aim of guideline adopted by OECD 30 years ago.

[309] Agnes (2016), *supra note* 202.
[310] *supra note 303, p 643.*

3.4. Conclusion

Internet has created a wide variety of new opportunities for human being and makes life easier in many possible ways. While we are enjoying our freedom on Internet, we could not know whether our rights have been violated on the other side of this complex system.[311] Cambodia is a latecomer of Internet, but it has contributes a lot to social development in this country during the last few years. More Cambodians are using Internet for various purposes including expressing opinion on social and political issues. Freedom of expression, information and privacy in Cambodia are limited under Cambodia Criminal Code 2009 and Telecom Law 2015.

According to the language used under the current draft law on Cybercrime of Cambodia, the draft law itself fails to address the cybersecurity issues, but seeks to criminalize free speech of those who criticize of the government, high ranked officials or harm to the national security. Moreover, the draft law also tends to violate the right privacy of individuals through retention of private data without consent from the owner. Fundamental human rights are protected under the Constitution, the supreme law of the Kingdom of Cambodia. Moreover, Cambodia also signed and ratified many regional and international human rights covenants and treaties; therefore it is obliged to guarantee that those rights are respected and achieved at least minimum standard of human rights protection purposes pursued under these instruments.

The current draft law is fails bellow the international standard and constitutes serious threats to freedom exercise on the Internet. The draft law on Cybercrime must be redrafted in order to reflect the necessity for the balance of fundamental rights and regulation concerning security in cyberspace. Those specific provisions that violate human right must be removed, more specific definitions should be added to avoid inconsistent interpretation, and avoid giving too much power to law enforcement officials to interpret the provision of the law. Government should provide more promotion of independent media, press, and protection freedom of expression, right to access to information and privacy.

[311] Akhgar, B., et al. Application of Big Data for National Security: A Practitioner's Guide to Emerging Technologies. (Eds.). Oxford, Elsevier, 2015, p 155.

4. Comparative analysis: state practice from China, Japan and Singapore

The development of cyberspace and ICT became the integral part of socioeconomic growth in the Asia-Pacific region during the last few years. Online environment is also growing more important for the political and social expression, however there are big gaps of technological development among countries in the region.[312] The terms ICT and cybersecurity are being used to achieve different purposes by different states. Author will compare the practice for China, Japan, and Singapore in this chapter.

Why China, Japan and Singapore?

Politically, China is a dominant player in Cambodia and one of the closest allies. Economically, China is Cambodia's top foreign investor, a major donor, and major trading partner. As China continues to be a major player in Cambodia's socioeconomic development, the development of policies and other regulations more or less influence Cambodia's environment.[313] Japan has signed the Convention on Cybersecurity and also play important role in Cybersecurity Cooperation between ASEAN and Japan. Japan is the second closest allies to Cambodia under the framework of "peace and happiness through economic prosperity and democracy".[314]

Japan supports Cambodia in many fields including conflict resolution, peace building, national reconstruction and rule of law development. Cambodia also received support from Japan in drafting the Civil Code and Civil Procedure Code with 21 million USD fund via Japan International Cooperation Agency (JICA).[315] Therefore, understanding Japan's cybersecurity practice could possibly benefit Cambodia in the area of cybersecurity development. Last but not least, the author is going to do the analysis on Singapore practice as well because it is the first ASEAN member state that transforms itself into a smart nation.[316] Author will do the comparative analysis base on the three major aspects that must be taking in to consideration when adopting national policies, includes Governance, Economy and Social.

---

[312] ASPI, Cyber Maturity in the Asia-Pacific Region, ASPI 2014, p 5. Available at: http://kipis.sfc.keio.ac.jp/wp-content/uploads/2014/04/ASPI_cyber_maturity_2014.pdf (25.02.2017)
[313] Heng, P. Cambodia-China Relations: A Perspective-Sum game? Journal of Current Southeast Asian Affairs, GIGA 2012, 31 (2), pp 57-85, p 57. Available at: https://journals.sub.uni-hamburg.de/giga/jsaa/article/viewFile/545/543 (25.02.2017)
[314] Chheang, V. Cambodia: Between China and Japan. CICO Working Paper, Cambodian Institute for Cooperation and Peace 2009, 31, p 10. Available at: http://www.cicp.org.kh/userfiles/file/Working%20Paper/CICP%20Working%20Paper%20No%2031_Cambodia_Between%20China%20and%20Japan%20by%20Cheang%20Vannarith.pdf (25.02.2017)
[315] Ibid, p 13.
[316] *Supra note* 23, p 1.

4.1. Governance

The national decision-making body for cyber governance in China is the 'Central Leading Group for Cyber Affairs', constituted by high-ranking officials and headed by the president. China has further strengthened its centralized government control of cyberspace through legislative framework that reflect China's strong belief of 'cyber sovereignty' and content control.[317] Last year China launched new 13th five years plan (2016-2020) outlining investment to support innovation in cybersecurity, quantum communication and big data application. China also actively participated in international cyber discussion, promoting the concept of cyber sovereignty and has successfully established new bilateral cybersecurity agreement with US, UK, India and Russia covering issues including intellectual property theft, cybercrime and norm.[318]

On 07 November 2016, the Standing Committee of the National People's Congress approved new Cybersecurity Law. The law is set to take effect in 01 June 2017 and has wide-ranging implication on how company in China handle personal data, data localization, and content control. The law requires critical information infrastructure operators to store personal and business data gathered or produced during operations in China on servers within main land China. Moreover, Company operating in China will required to undergo security reviews and provide investigators full access to data in criminal cases.[319]

Japan launched it new Cybersecurity Strategy Plan in September 2015. The Cybersecurity Strategic Headquarters functions as the command and control body to promote cyber strategy plan, and National Information Security Center (NISC) takes leading roles to promote cybersecurity policies set forth in this strategy. New Cybersecurity Strategy Plan highlights the role of industry and civil society in maintaining Japan's cybersecurity and the centrality of two-way information sharing. Moreover, it allows NISC to monitor government-affiliated agencies for the first time.[320] The Japanese government adopted the Cybersecurity Basic Act in November 2014 and was amended in April 2016 in response to the Japan Pension Service hack to give

[317] Raud, M. (Ed.). China and Cyber: Attitudes, Strategies, Organization. Tallinn, CCD COE Publications 2016, p 7. Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016.pdf (11.12.2016)
[318] ASPI, Cyber Maturity in the Asia-Pacific Region, ASPI 2014, p 31. Available at: http://www.spain-australia.org/files/documentos/62_ASPI-Cyber-Maturity-2016.pdf (25.02.2017)
[319] *Supra note* 22.
[320] The Government of Japan, Cybersecurity Strategy, 04.09.2015, p 52. Available at: https://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf (25.02.2017)

NICS new power to monitor and audit the security of entities created by direct government approval or laws.[321]

Japan is a member of the Global Forum on Cyber Expertise and has been a member of two UNGGEs. Japan actively involve in cyber discussion at high-level international political dialogues and has a strong Asia-Pacific engagement program, working closely with ASEAN countries. JPCERT/CC is Japan's national CERT establish in 1996 in order to work with government agencies, critical infrastructure operators, security vendors and civil society. JPCERT/CC actively promote collaboration-monitoring system across Asia-Pacific and enhances the sharing of threat information. It is also undertake extensive capacity building across and outside Asia-Pacific and working with global partners on a Cyber Green Initiative.[322]

Singaporean Government's created new Cybersecurity Strategy Plan 2018 with the aims to establish a resilient cyber environment for the country. The new strategy will focus on building a resilient infrastructure, creating a safer cyberspace, developing a vibrant cybersecurity ecosystem and strengthening international partnership.[323] Moreover, Communication and Information minister has committed to spending up to 10% of Singapore' IT budget on boosting cybersecurity.[324] In addition to this, the change to the existing Computer Misuse and Cybersecurity Act were passed in Parliament on 03 April 2017. The new amended Cybersecurity Act will institute standards for incident reporting, audits and risk assessment such as dealing in personal information obtained via cybercrime such as a trading in hacked credit cared details.[325]

Singapore engages in strong international program to establish itself as one of the region's leading central government cybersecurity bodies. It has signed several MoU with other cyber and coordinating ministries inside and outside the region. Singapore is also active in forums such as the East Asia Summit, ASEAN cybercrime meetings and the ASEAN Regional Forum. SingCERT was established in 1997 and works to detect, to resolve and prevent security-related

[321] *Supra note* 318, p 43.
[322] Ibid.
[323] Singapore's Cybersecurity Strategy, Cyber Security Agency of Singapore 2016. Available at: https://ccdcoe.org/sites/default/files/documents/SingaporeCybersecurityStrategy.pdf (25.02.2017)
[324] *Supra note* 318, p 70.
[325] Kevin Kwang, "Changes to Singapore's cybercrime law passed", Channel NewsAsia, 03.04.2017. Available at: http://www.channelnewsasia.com/news/singapore/changes-to-singapore-s-cybercrime-law-passed-8712368 (15.04.2017)

incidents on the Internet affecting Singaporean companies and users. SingCERT signed MoU with CERT-In to enable information sharing and incident response collaboration.[326]

Cambodia has made steady move in the area of cyber policy and security. In order to strengthen the area of national telecommunication legislation, Cambodia government adopted the Law on Telecommunications in 2015 and launched its Telecom/ICT Development Policy in 2016. Other legislation such as e-commerce and cybercrime is in drafting process. Cambodia's international cyber engagement is limited to engagement with ASEAN's cyber discussion and some bilateral engagement with Japan, South Korea and US. The engagement is focused more on technical capacity building and legislative and policy development assistant.[327]

4.2. Economy

The Cyber Security Association of China was established in May 2016 to engage the private sector, academia and government in the development of China's cyber policy. This Industry led by Chinese Communist Party and features Chinese Tech giants Alibaba, Baidu, and other with a positive development.[328] The Cybersecurity law will be effect from 01 June 2017, may has huge influence to business in China.

Japan's Cybersecurity Strategy has made strong move in bolstering digital economy. The new strategy allows NISC to monitor government-affiliated agencies for the first time to ensure the safeguard of cybersecurity in this area. The Japanese Business Federation has also established a cybersecurity working group of more than 30 of Japan's most important companies.[329] Japan has prepared several strategies for digital economy development, including the ICT Growth Strategy II (2014), ICTs for Inclusive Social and Economic Development in Japan, the Revitalization Strategy, the 2013 Declaration to be the World's Most Advanced IT Nation etc.[330]

Singapore has a very high level of substantive two-way dialogue between it public and private sectors. These relationships are encouraged by high-level policy documents. The Singaporean government also include Cybersecurity Association and Technologists Program, Capabilities Development Grant, Cybersecurity Awareness Alliance, International Advisory Program and other important industrial and economy development program in to its national Cybersecurity

[326] *Supra note* 318, p 70.
[327] Ibid, p 28.
[328] Ibid, p 32.
[329] Ibid, p. 44.
[330] Ibid.

Strategy plan.[331] Singapore's digital economy is a good model practice for the countries in the region and the other because of the strong culture of consultation among state and private sector when forming any key national document and strategies. Government also include new member into the Committee on the Future Economy that consist of government member and industrial leaders, to help solidify Singaporean's position a best practice and embrace the new technologies and opportunities for economic growth.[332]

ICT Federation of Cambodia (ICTF) was launched again with a new Board of Director, represented by industrial leaders, and with a new vision to set forth: "Empowering Cambodia's Digital Economy."[333] Elimination of political appointees to the ICT Federation's board is a positive step for public and private dialogue on digital business in Cambodia. The e-commerce activity is significantly increased in Cambodia. However, to ensure the safeguard of business conduct online, further support from government is needed, particularly by providing an effective legal framework.[334] As mentioned earlier, the e-commerce regulation still in the drafting process.

4.3. Social

China now has the largest online population, which is highly engaged in social networks such as WeChat and RenRen. More than half of China's population is online. Its more than 688 million Internet users make up the world's largest online population. The recent legislative changes sparked some public debate over the social and economic implications.[335] Unfortunately, strong government censorship, including tougher restrictions on news content providers and limit the discussion of cyber issues in China. Chinese government has sought to control its content and to sensor information it deemed detrimental or sensitive.[336] Self-censorship also continues to inhibit open public discussion.

Japan has a well-developed culture of academic research into cyber issues, and many universities also partner with government and the private sector to develop skills programs to help fill the country's growing skills gap. Media reporting on new government policies, organizational

[331] Ibid, p 71.
[332] Ibid.
[333] About ICT Federation. Available at: http://www.ictfederation.org/about
[334] *Supra note* 318, p 29.
[335] Ibid, p 32.
[336] Amnesty International, Undertnading Freedom of Expression in China. Amnesty International 2006, p 16. Available at: http://www.agsm.edu.au/bobm/teaching/BE/AmnestyReportonYahooMicrosoftGoogleinChina.pdf (12.04.2017)

changes, cyber threats and infiltrations remains plentiful. The number of mobile data connections in Japan is equal to 126% of the population, while 30% have a fixed broadband connection. [337] However, media have been viewed as "Bias", according to UN special rapporteur.[338] Japanese politician have been engaged in fights to maintain control over the media.[339]

The Infocomm Development Authority of Singapore conducts an impressive suite of awareness-raising events, training workshops and programs and delivers many educational IT scholarship opportunities. Singapore's media and public commentary on cybersecurity issues is at a very developed level, and the public's understanding of IT issues is among the most developed in the region. Singapore's mobile Internet connectivity sits at 142%, the largest number in this year's maturity metric and reflective of Singapore's highly networked society. Fixed-line broadband connectivity is comparatively low: only 26% of the population uses it to get online. [340]

There is only few medias that coverage the cyber issues in Cambodia. Citizen can access to cybersecurity alert information through CamCERT website and MPTC. Some other private media websites also cover come cyber related issues, but not focus much on raising public awareness. Social media become very popular as 68% of Cambodian population is under 30-year old and 46% of the total of population have access to Internet.[341] Citizen can access to Internet easier via mobile phone Internet or Internet café. However, there are on going debate and discussion of the violation on freedom of expression and privacy through the legislation in Cambodia.

4.4. Discussion and Good Practice

Governance, Economy and Social are important factors that must be taking into consideration when legislating cyberspace. In the area of governance, in 2013, the United Nations Working Group of Government Expert, concluded that the UN Charter and international law are fully applicable to the state behavior in cyberspace, which has also been taken by NATO countries.[342] However, China does not fully agree that international law should have jurisdiction on regulating

[337] *Supra note* 318, p 44.
[338] Shusuke Murai, "U.N. rapporteur on freedom of expression slams Japan's 'press club' system, government pressure", Japan Time, 16.04.2016. Available at: http://nottspolitics.org/2016/07/11/controlling-the-media-in-japan/ (12.04.2017)
[339] Kirsch, G. Controlling the Media in Japan. Available at: http://nottspolitics.org/2016/07/11/controlling-the-media-in-japan/ (12.04.2017)
[340] *Supra note* 318, p 71.
[341] *Supra note* 220.
[342] *Supra note* 317.

cyberspace. China views that state should have such jurisdiction to set up it own rule. With the strong belief that state should have cyber sovereignty, China together with Russia and some other Asian countries, has introduced its alternative position through the Shanghai Corporation Organization (SCO) in the UN General Assembly.[343]

China has been actively participated in high-level cyber dialogue and signed several agreements for the purpose of protection and improvement cybersecurity. Yet, several national policies adopted gave extensive arm jurisdiction to Chinese Government to control cyberspace in the area of social and economy as well. New Chinese Cybersecurity Law continues self-censorship on the content and control over the personal and business data. Therefore, the principle of international law covering cyberspace and fundamental human rights has not been fulfilled based on Chinese government's cyber attitude. The similar issues have been found in the current Cambodia's legislations where the citizens can exercise very limited fundamental rights.

Freedom of expression, access to information, and privacy are also in the limited manner in Japan, however it very success and open term when addressing the cybersecurity issue. Japan and Singapore are good role models in addressing cybersecurity issue, public-private partnership in digital economy, effective international cooperation for cybersecurity development. It is impossible to transforms Cambodia to reach the level above due to political, social and economic barriers. However, there are some concrete steps that RGC could follow in order improve the cybersecurity, combat against cybercrime and serve the best interest of its citizens.

Bellow are some concrete suggest that RCG should take into consideration:

a) Amendment overlapping provisions in the current laws and other provisions that provide unnecessary restriction and violation on human rights;
b) Draft law on Cybercrime should address cybersecurity issues and follow the minimum international cybersecurity standard norm;
c) Cambodia does not have to establish NACC;
d) Capacity building is very important for the effective implementation in the area of cybercrime investigation. It is not only for the cybercrime investigators, but also for other law enforcement officials and those who are working in other government institutions;
e) Cyber awareness program should be implemented in all level to help citizen aware the possible risks and threats on the Internet. Government should integrate cyber awareness

[343] Ibid.

in school program because numbers of young Cambodian are using Internet for various purposes without acknowledge that those activities could constitute harms;

f) Open discussion among government, public, private and civil societies when adopting any national legislations and policies;
g) Cambodia should consider about signing and ratify the current Cybercrime Convention;
h) Increase regional and international cooperation and partnership;

There are many other good recommendations proposed by stakeholders and international partners. RGC should take those suggestions and international good practice into consideration in order to improve cyber wellness in Cambodia.

Conclusion

The technologies and new innovation keep growing and become the backbone of the global economy, yet it also generated a new trend of crime and provides greater opportunity for criminals to conduct criminal activities via computer system and network. Cybersecurity is the global issue; the national effort of individual states alone cannot address this issue properly. The United Nations Working Group of Government Expert in 2013 concluded that the UN Charter and international law are fully applicable to the state behavior in cyberspace. For globalization and regional integration, Cambodia does need cybercrime law to ensure cybersecurity and international cooperation. It has shown clear that Cambodia should be well prepared for the upcoming opportunities for economic growths and self-development.

Cambodia has significantly achieved some key efforts on cybersecurity and policy implication through promoting cybersecurity culture, established e-government service, e-commerce, and focus on raising awareness and capacity building to the citizens and agencies. RGC adopted ICT Master Plan 2020 in 2014 in the line with ASEAN ICT Master Plan 2020 and ITU Connect 2020 Agenda and the Law on Telecommunications also adopted in 2015. Cambodia also established CamCERT in 2007 in order handle Information Security. Last but not least, Cambodia also works hard on structural reform in order to improve the development of ICT sector. Telecom/ICT Development Policy drafted by MPCT working team finally approved by the RGC on 11 April 2016.

There are some other laws and policies are being drafted includes draft law on Cybercrime, draft law on E-commerce, and draft of Spectrum regulation. Last but not least, RGC has been integrated NiDA into the MPTC's structure in 2013 and established TRC in 2015 in order to formulate the regulations, relating to the operation and provision of telecommunication in the line with the RGC's policy on the telecommunication sector.

However, achievements come along with number of challenges. Cambodia lacks of adequate and comprehensive strategy, policy and regulation frameworks, which constrain the effective oversight of this sector. If compare to other nations in the region, Cambodia and Lao are the slowest in term of establishment the legal framework concerning ICT sector. Cambodia also needs to strengthen and coordinate institutional mechanisms ineffective response of human resources and level of IT literacy to cope with the fast growth of modern Technology.

UDHR provides a set of basic human rights standard that at least all member state should achieve at the minimum level. Unfortunately, the fundamental rights standards are not being achieved in the online context until UNHRC adopted a resolution affirming the application of human right in cyber aspect in 2012, especially freedom of expression. The resolution provides that, *" the same rights that people have offline must also be protected online, particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with article 19 of the UDHR and ICCPR."*[344]

According to international legal norm, members to the United Nations and of the signatories to international treaties are assuming obligation under international laws to respect, to protect and to fulfill human rights. Cambodia ratified ICCPR, ICESCR, CRC and other major international covenants and treaties, therefore Cambodia has binding obligation to guarantee at least minimum purposes pursued under those legal instruments. This language in current draft law is exceedingly vague and exposed a dangerous drift away from international human rights standards regarding freedom of expression, access to information and right to privacy on the Internet. The draft law fails to address cybersecurity issue properly, but focus on the punishment on those who seek to exercise their freedom instead.

This law cannot ensure better improvement in safeguarding cyberspace and it needs the creative initiation from all stakeholders to help establish a proper Cybercrime law that can address cybersecurity issue in Cambodia without compromising human rights. Consequently, Cambodia needs support almost in every sector, due to the rapid development of network technologies and their complex structures it will be difficult to implement Cybercrime Law without international cooperation.

Cybercrime could be a major role in addressing cybersecurity in various sectors in Cambodia, however it has to be qualified with the international cybersecurity standard, and compliance with Cambodia's legal oblations at all level. Cybercrime law is important to Cambodia in the context of political, social and economic development. The future of Cybercrime Law of Cambodia should integrate international good practice from other developed countries based on positive experiences and best practices as suggested above. There are many other good recommendations proposed by stakeholders and international partners. RGC should take those suggestions and international good practice into consideration in order to improve cyber wellness in Cambodia

[344] *Supra note* 252.

List of References

Books

1. Schwabe, W. Need and Prospect for Crime-fighting Technology: The Federal Role in Assisting State and Local Law Enforcement. Washington, D.C. Rand 1999.
2. Weippl, E.R. Security E-Learning. New York, Springer 2005.
3. McDowell, B. Ethic and Excuses: The Crisis in Professional Responsibility. United States, Quorum Books 2000.
4. Brownsword, R., Goodwin, M. Law and the Technology of the Twenty-first Century. Cambridge University Press, 2012.
5. The transnational dimension of cybercrime and terrorism. Ed. Sofaer, A., Goodman, S. California, Hoover Institution Press, 2001.
6. Ruiz, B. Privacy in Telecommunications: A European and an American Approach. Netherland, Kluwer Law International 1997.
7. Yasuda, Y. Rules, Norms and NGO Advocacy Strategies: Hydropower development on the Mekong River. New York, Routledge 2015.
8. Black, S. Telecommunications Law in the Internet Age. San Francisco, Academic Press 2002.
9. Cross, M. Sense of the Cybercrime. 2nd ed. United State, Elsevier 2008.
10. Edwards, L., Waelde, C. Law and the Internet. 3rd ed. United States, Hart Publishing 2009.
11. Tams, C. Enforcing Obligations *Erga Omnes* in International Law. New York, Cambridge University Press 2005.
12. Bygrave, L. Data Privacy Law: An International Perspective. Oxford, Oxford University Press 2014.
13. Casagran, C. Global Data Protection in the Field of Law Enforcement. New York, Routledge 2017.
14. Akhgar, B., et al. Application of Big Data for National Security: A Practitioner's Guide to Emerging Technologies. (Eds.). Oxford, Elsevier, 2015.

Journal articles and collected volumes

1. Marsoof, A. Online Social Networking and the Right to Privacy: The Conflicting Rights of Privacy and Expression. Int'l J. Info Tech, Oxford University Press 2011, 19 (2), pp 110-132.
2. Kong, P. Overview of the Cambodian Legal and Judicial System. Introduction to Cambodian Law. Hor, P., *et al* (Eds.). Phnom Penh, Konrad-Adenauer-Stiftung 2012.
3. Cheang, S., Sang, S. Sate of Cybersecurity and the Roadmap to Secure Cyber Community in Cambodia. International conference on availability, reliability and security, IEEE, 2009. pp 652-657. doi: 10.1109/ARES.2009.144
4. Dalei, P., Brahme, T. Cyber Crime and Cyber Law in India: An Analysis. IJHAS 2013, 2(4), ISSN 2277-4386, pp 106-109.
5. Chowbe, V. An Introduction to Cyber Crime: General Considerations. SSRN 2011. Available at: https://ssrn.com/abstract=1766234
6. Kaper, A. The Fragmented Securitization of Cyber Threats. Regulating eTechnologies in the European Union. Kerikmäe, T. (Ed.). Springer 2014.
7. Kerikmäe, T. Särav, S. E-Residency: A Cyberdream Embodied in a digital Identity Card? The Future of Law and eTechnologies. Kerikmäe, T. Rull, A. (Eds.). Springer 2016.
8. Nyman-Metcalf, K. e-Government in Law and by Law: The Legal Framework of e-Government. Regulating eTechnologies in the European Union. Kerikmäe, T. (Ed.). Springer 2014.
9. Sang, S. et al. E-government adoption in Cambodia: a partial least squares approach. Transforming Government: People, Process and Policy 2010, 4 (2), pp 138-157. DOI 10.1108/17506161011047370
10. Zissis, D. Lekkas, D. Securing e-Government and e-Voting with an open cloud computing architecture. Government Information Quarterly 2011, 28 (2), pp 239-251. Doi:10.1016/j.giq.2010.05.010
11. Zwass, V. Electronic Commerce and Organizational Innovation: Aspects and Opportunities. International Journal of Electronic Commerce 2003, 7 (3), pp 7-37. Available at: http://www.jpedia.org/ijecnew/zwass-20031.pdf
12. Richardson, J. ICT in Education reform in Cambodia: Problems, Politics, and Policies Impacting implementation. The MIT Press 2008, 4 (4), pp 67-82. Available at: http://itidjournal.org/itid/article/viewFile/311/143

13. Hansen, L. Digital Disaster: Cyber Security, and the Copenhagen School. International Study Quarterly 2009, 53, pp 1155-1175. Doi:10.1111/j.1468-2478.2009.00572.x
14. Gruodyte, E., Bilus, M. Investigating Cybercrimes: Theoretical and Practical Issues. Regulating eTechnologies in the European Union. Kerikmäe, T. (Ed.). Springer 2014.
15. Harrington, S. Professional Ethics in the Digital Forensics Expert: Ultimate Tag-Team or Disastrous Duo? William Mitchell L. Rev. 2011, 38 (1), pp 353-396. Available at: http://open.mitchellhamline.edu/wmlr/vol38/iss1/8
16. Hassan, A. et al. Cybercrime in Nigeria: Causes, Effects and the Way out. ARPN Journal of Science and Technology 2012, 2 (7), pp 626-631. Available at: http://www.ejournalofscience.org/archive/vol2no7/vol2no7_11.pdf
17. Klimburg, A., Healey, J. Strategic Goals & Stakeholders. National Cyber Security Framework Manual. Klimburg, A. (Ed.). NATO CCDCOE, 2012.
18. Arbaugh, W. et al. Window of vulnerability: a case study analysis. IEEE 2000, 33 (12), pp 52-59. DOI: 10.1109/2.889093
19. Jonhson, D., Powers, T. Computer system and responsibility: A normative look at technological complexity. Ethics and Information Technology, Springer 2005, 7 (2), p 99-107. DOI: 10.1007/s10676-005-4585-0
20. Pierce, M. The Internet and the Seattle WTO Protests. Peace Review 2001, 13 (3), pp 331-337. DOI: 10.1080/13668800120079027
21. Jahankhani, H., Al-Nemrat, A. Examination of Cyber-criminal Behavior. International Journal of Information Science and Management, 2015. Available at: https://www.researchgate.net/profile/A_AlNemrat/publication/228684366_Examination_of_Cybercriminal_Behaviour/links/55643e3208ae8c0cab37167f.pdf
22. Schmitt, M. The Law of Cyber Targeting. NATO CCDCOE, 2015. Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/TP_07_2015.pdf
23. Bernstein, S. Fourteenth Amendment—Police Failure to preserve Evidence and Erosion fo the Due Process Right to a Fair Trial. J. Crim. L. & Criminology, 1990, 80 (4), pp 1256-1280. Available at: http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=6649&context=jclc

24. Bhagat, R. Separation of power without checks and balance in Cambodia. Journal of Alternative Perspectives in the Social Sciences 2015, 6 (4), pp 389-401. Available at: http://www.japss.org/upload/3.%20Bhagat.pdf

25. Worl, O. Computer crime: Factors of Cybercriminal Activities. Int'l J. IJACSIT ISSN 2320-0235, Cloud Publications 2014, 3 (1), pp 51-67.

26. Kasper, A., Laurits, E. Challenges in Collecting Digital Evidence: A Legal Perspective. The Future of Law and eTechnologies. Kerikmäe, T. Rull, A. (Eds.). Springer 2016.

27. Demchak, C., Frenstermacher, K. Balancing Security and Privacy in the 21st Century. Intelligence and Security Informatics. Chen, H., et al. (Eds.). Second Symposium on Intelligence and Security Informatics, ISI 2004.

28. Chak, S. New Information and Communication Technologies' Influence on Activism in Cambodia. SUR Int'l J. on Hum Rts 2014, 20, p 437. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2553249

29. Mendel, T., Salomon, E. Freedom of Expression and Broadcasting Regulation. A Debates series, UNESCO 2011, 8, p 9-10. Available at: http://unesdoc.unesco.org/images/0019/001916/191623e.pdf

30. Fobr, A. Domestic Implementation of the International Covenant on Civil and Political Rights Pursuant to its article 2, para.2. Max Planck UNYB 2001, 5. Available at: http://www.mpil.de/files/pdf1/mpunyb_seibert_fohr_5.pdf

31. Odello, M. The Right to Take Part to Cultural life: General Comment No.21 of the United Nations Committee on Economic, Social and Cultural Rights. Anuario Español De Derecho Internacional 2011, 27, pp 493-521.

32. Shackelford, S., Kastelic, A. Toward a state-centric cyber peace?: Analyzing the role of national cybersecurity strategies in enhancing global cybersecurity. N.Y.U.J. Legis. & Pub. Pol'y 2015, 18, pp 895-984.

33. Mačák, K. Is the International Law of Cyber Security in Crisis? 2016 8th International Conference on Cyber Conflict: Cyber Power. Pissanidis, N., *et al* (Eds.). NATO CCD COE Publications 2016.

34. Gerry QC, F., Moore, C. A slippery and inconsistent slope: How Cambodia's draft cybercrime law exposed the dangerous drift away from international human right

standards. Computer Law & Security Review, Elsevier 2015, 31, pp 628-650. Available at: https://doi.org/10.1016/j.clsr.2015.05.008

35. Heng, P. Cambodia-China Relations: A Perspective-Sum game? Journal of Current Southeast Asian Affairs, GIGA 2012, 31 (2), pp 57-85. Available at: https://journals.sub.uni-hamburg.de/giga/jsaa/article/viewFile/545/543
36. Chheang, V. Cambodia: Between China and Japan. CICO Working Paper, Cambodian Institute for Cooperation and Peace 2009, 31. Available at: http://www.cicp.org.kh/userfiles/file/Working%20Paper/CICP%20Working%20Paper%20No%2031_Cambodia_Between%20China%20and%20Japan%20by%20Cheang%20Vannarith.pdf
37. Raud, M. (Ed.). China and Cyber: Attitudes, Strategies, Organization. Tallinn, CCD COE Publications 2016. Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016.pdf

Case laws

1. EIKo 08.04.2014, Joined cases C-293/12 and C-594/12
2. EIKo 09.11.2010, Joined cases C-92/09, *Volker und Markus Schecke GbR* and C-93/09, *Hartmut Eifert*.
3. EIKo 03.04.2011, 62617/00, *Copland vs. the United Kingdom.*
4. EIKo 02.09.2010, 35623/05, *Uzun vs. Germany*.
5. U.N. Doc. CCPR/C/83/1128/2002, *Rafael Marques de Morais vs. Angola.*
6. U.N. Doc. CCPR/C/89/D/1353/2005, *Njaru vs. Cameroon.*

Legislative Acts

Cambodia

1. 1993 Constitution of the Kingdom of Cambodia, additional Constitutional law is promulgated by Kram No.NS/RKM/0704/001 of 13 July 2004.
2. Criminal Code of the Kingdom of Cambodia, No.NS/RKM/1109/09 dated 30 November 2009.
3. Law on the Press No.NS/RKM/36/95 dated 18 July 1995.
4. The Law on Telecommunications, No.NS/RKM/1215/017 dated 17 December 2015.

Council of Europe

1. Convention on Cybercrime, ETS 185, 23.11.2001.
2. Council of Europe (CoE), Convention for the Protection of Individual with regard to Automatic Processing of Personal Data, ETS 108, 28.1.1981.
3. Commission Regulation (EC) No 95/46 of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the freedom of movement of such data, OJ L 281, 23.11.1995.
4. Commission Regulation (EC) No 2002/58/EC of 12 July 2002 concerning of the processing of personal data and the protection in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.07.2002.
5. Commission Regulation (EC) 2006/25/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications service or of public communications network and amending Directive 2002/58/EC, OJ L105, 13.04.2006.

National Policies

1. RGC, National Strategic Development Plan 2013-2018, 17 July 2014.
2. RGC, Rectangular Strategy for Growth, Employment, Equity and Efficiency Phase III, September 2013.
3. RGC. Telecom/ICT Development Policy 2020, April 2016.
4. The Government of Japan, Cybersecurity Strategy, 04.09.2015.
5. Singapore's Cybersecurity Strategy, Cyber Security Agency of Singapore 2016

Regional Legal Instruments

1. Bangkok Declaration founding of Association of Southeast Asian Nation of 08.08.1967.
2. ASEAN Declaration on Human Rights, 19.11.2012.
3. 2000 e-ASEAN Framework Agreement, 24.11.2000.

United Nations legal instruments

1. Universal Declaration on Human Rights, GA/RES/3/217A, 10.12.1948.
2. International Covenant on Civil and Political Rights, GA/RES/21/2200A, 23.03.1976.
3. International Covenant on Economic Social and Cultural Rights, GA/RES/21/2200, 16.12.1966.

4. Convention on the Right of the Child, GA/RES/44/25, 20.11.1989.
5. Optional Protocol to the Convention on the Right of the Child on the sale of children, child prostitution and child pornography, GA/RES/54/263, 25.05.2000.
6. UNHRC Resolution on the promotion, protection and enjoyment of human rights on the Internet. A/HRC/20/L.13, 29.06.2012.
7. UNHRC, CCPR General Comment No.16: Article 17 on Right to Privacy, HRI/GEN/l/Rev.9 (Vol. I), 1988.
8. UNHRC, General Comment No.34: Article 19 on Freedom of Opinion and Expression, CCPR/C/GC/34, 2011.
9. CESCR General comment No.21 on Right of everyone to take part in cultural life Art.15, para. 1 (a), E/C.12/GC/21, 20.11.2009

Research Papers

1. YMAC. Security: How can we enhance cybersecurity in ASEAN? Youth Model ASEAN Conference 2016. Available at: http://www.sp.edu.sg/ymac/documents/securitycybersecurity.pdf
2. Long, L. Profiling Hackers. SANS Institute InfoSec Reading Room, 2012. Available at: https://www.sans.org/reading-room/whitepapers/hackers/profiling-hackers-33864
3. Barber, R. Hackers Profiled: Who are they and what are their motivations? Computer Fraud & Security 2001. Available at: http://130.18.86.27/faculty/warkentin/SecurityPapers/Robert/Others/Barber2001_CF&S_Hackers.pdf
4. Bazzichelli, T. On Hacktivist Pornography and Networked Porn. GNU 2010. Availale at: http://www.tatianabazzichelli.com/PDF_files/Bazzichelli_Hacktivist_Pornography.pdf
5. Chicone, R. A Layman's Guide to Cyber Threats, Threat Actors, Attacks, and Intelligence. Kaplan University 2015. http://alliance.kaplan.edu/uploadedFiles/_Global_Content/Generic/Promotional_contents/Laymans%20Guide%20to%20Cyber%20Threats%20Article.pdf

News article and commentaries

1. McDowell, M. Householder, A. Good Security Habits. What is Cyber Security? Blimline, B. (Ed.). Today's Insurance Professionals 2016, 73 (1). Available at:

http://c.ymcdn.com/sites/www.internationalinsuranceprofessionals.org/resource/resmgr/Today_s_Insurance_Professionals_magazine/Spring2016_Mag_FINALWEB.pdf

2. Mong Palatino, "Cambodia: Mandatory Internet Surveillance Cameras", Global Voice, 09.12.2012. Available at: https://globalvoices.org/2012/09/09/cambodia-mandatory-internet-surveillance-cameras/
3. Joseph Soh, "Cambodia's 2017 Social Media and Digital Statistics", Geeks 09.02.17. Available at: http://geeksincambodia.com/cambodias-2017-social-media-digital-statistics/
4. Ron Cheng, "China Passes Long-Awaited Cyber Security Law", Forbes, 09.11.2016. Available at: http://www.forbes.com/sites/roncheng/2016/11/09/china-passes-long-awaited-cyber-security-law/#2653934b6868
5. Tan, T. B. We, Cittizens of Smart Signapore: Data Protection in Hyper-connected Age. RSIS Commentaries, No. 036, 2016. Available at: http://hdl.handle.net/10220/40253
6. Tian Shoahui, "Cambodia drafts E-commerce as online sale grow", Xinhua 06.11.2016. Available at: http://news.xinhuanet.com/english/2016-11/06/c_135809717.htm
7. KOICA, "The First e-Learning Center Appears in Cambodia", KOICA 04.05.2012. Available at: http://www.koicacambodia.org/the-first-e-learning-center-appears-in-cambodia/
8. Kimberly Carlson, "Cambodia's Draft Law turns Free Speech into Cybercrime", Internet Frontier Foundation, 27.05.2014. Available at: https://www.eff.org/deeplinks/2014/05/cambodian-cybercrime-draft-law-threatens-freedom-expression-online
9. Doug Gross, "Mafiaboy breaks silences, paints portrait of a hacker", CNN, 15.08.2011. Available at: http://edition.cnn.com/2011/TECH/web/08/15/mafiaboy.hacker/index.html?iref=obnetwork
10. Licadho, Cambodia's Law on Telecommunications a Legal Analysis, Briefing Paper 2016. Available at: http://www.licadho-cambodia.org/reports/files/214LICADHOTelecomsLawLegalAnalysis_March2016ENG.pdf
11. Sinary, S. Wilwohl, J, "Hackers Arrested in Joint Operation with FBI", The Cambodia Daily April 32, 2014. Available at: https://www.cambodiadaily.com/archives/hackers-arrested-in-joint-operation-with-fbi-57065/

12. Pisey, H. Wilwohl, J, “Hackers Ordered to Work for Government”, The Cambodia Daily, October 1, 2014. Available at: https://www.cambodiadaily.com/archives/hackers-found-guilty-freed-ordered-to-work-for-government-68722/
13. Kevin Ponniah, “Cyber bill raises concerns”, The Phnom Penh Post 09.04.2014. Available at: http://www.phnompenhpost.com/national/cyber-bill-raises-concerns
14. Carmichael, R., “Cambodia’s Draft Cybercrime Law Worrying, Say Critics”, VOA News, 25 April 2014. Available at: http://www.voanews.com/a/cambodias-draft-cybercrime-law-worrying-say-critics/1900884.html
15. Blomberg, M. Naren, K., “Cyber War Team’ to Monitor Web. The Cambodia Daily”, 20 November 2014. Available at: https://www.cambodiadaily.com/archives/cyber-war-team-to-monitor-web-72677/
16. Kennedy, V. Pineros, E., “ Opposition rejects Cambodia electon results, call for investigation”, CNN, 29 July 2013. Available at: http://edition.cnn.com/2013/07/29/world/asia/cambodia-elections/
17. Telecom Asia, UNHR blasts Cambodian Telecoms, cybercrime laws, October 03, 2016. Available at: http://www.telecomasia.net/blog/content/unhr-blasts-cambodian-telecoms-cybercrime-laws
18. LICADO, New Law on Telecommunications: A Legislative Attack on Individuals’ Rights and Freedoms. Available at: https://www.licadho-cambodia.org/pressrelease.php?perm=401
19. Khy Sovuthy, “Supreme Court Hears ‘Color Revolution’ Facebook Case”, The Cambodia Daily, 24.12.2016. Available at: https://www.cambodiadaily.com/news/supreme-court-hears-color-revolution-facebook-case-122430/
20. Ouch Sony, “Taylor O’Connell, Student gets 18 month for call for ‘Color Revolution’”, The Cambodia Daily, 16.03.2016. Available at: https://www.cambodiadaily.com/news/student-gets-18-months-for-call-for-color-revolution-109944/
21. Kevin Kwang, “Changes to Singapore’s cybercrime law passed”, Channel NewsAsia, 03.04.2017. Available at: http://www.channelnewsasia.com/news/singapore/changes-to-singapore-s-cybercrime-law-passed-8712368
22. Shusuke Murai, “U.N. rapporteur on freedom of expression slams Japan’s ‘press club’ system, government pressure”, Japan Time, 16.04.2016. Available at: http://nottspolitics.org/2016/07/11/controlling-the-media-in-japan/

International organizations reports and policy documents

1. Freedom House, Freedom on the Net: Cambodia. Report 2013. Available at: https://freedomhouse.org/sites/default/files/resources/FOTN%202013_Cambodia.pdf

2. Article 19, Cybercrime Law, Draft V.1, unofficial translation to English. Available at: https://www.article19.org/data/files/medialibrary/37516/Draft-Law-On-CyberCrime_Englishv1.pdf

3. ITU, Information Society Statistical Profile Asia and the Pacific, 2009. Available at: http://www.itu.int/ITU-D/ict/material/ISSP09-AP_final.pdf
4. ITU, Global Cybersecurity Index & Cyberwellness Profiles. 2015. Available at: http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf
5. ITU, Understanding Cybercrime: Phenomena, Challenges and Legal Response. 2012. Available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf
6. ITU, Khmer Internet: Cambodia Case Study. 2002. Available at: http://www.itu.int/itudoc/gs/promo/bdt/cast_int/79475.pdf
7. UNCTAD, Review of e-commerce legislation harmonization in the Association of Southeast Asian Nations, 2013. Available at: http://unctad.org/en/publicationslibrary/dtlstict2013d1_en.pdf
8. WHO, Survey on eHealth and Innovation in Women's and Children's health: Cambodia, 2013. Available at: http://www.who.int/goe/publications/atlas/2013/khm.pdf
9. ITU, Overview of Cybersecurity. Recommendation ITU-T X. 1205. 2008. Available at: https://www.itu.int/rec/T-REC-X.1205-200804-I
10. ITU, Report on best practice for a national approach to cybersecurity: A management framework for organizing national cybersecurity efforts. ITU-D secretariat draft, 2008. Available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf
11. KOICA, Summary on Cambodia ICT Masterplan 2020, 2014. Available at: https://data.opendevelopmentmekong.net/dataset/summary-on-cambodian-ict-masterplan-2020/resource/bf12527f-255e-4f2a-bb14-3ba433408e52?type=library_record
12. UN, Report of the Special Rapporteur on the situation of human rights in Cambodia, A/HRC/33/62.

13. UN, Report of the special rapporteur on the situation of human right in Cambodia. A/HRC/12/46.
14. Human Rights Watch, Word Report 2012: Cambodia, HRW 2011. Available at: https://www.hrw.org/world-report/2012/country-chapters/cambodia
15. Freedom House, Freedom in the Net: Cambodia. 2016. Available at: https://freedomhouse.org/sites/default/files/FOTN%202016%20Cambodia.pdf
16. OECD, Recommendation of the Council concerning Guideline Governing the Protection of Privacy and Transborder Flows of Personal Data, 2013. Available at: https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf
17. UNICEF, Handbook on the Optional Protocol on the Sale of Children, Child Prostitution, and Child Pornography. Florence, UNICEF 2009, p 1. Available at: https://www.unicef-irc.org/publications/pdf/optional_protocol_eng.pdf
18. UNCRC, Concluding observations on the report submitted by Cambodia under article 12, paragraph 1, of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, CRC/C/OPSC/KHM/CO/1, 26.02.2015. Available at: http://www.refworld.org/publisher,CRC,,KHM,566e85009,0.html
19. CoE, Explanatory Report to the Convention on Cybercrime, ETS 185, 21.11.2001, § 16. Available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b
20. ASPI, Cyber Maturity in the Asia-Pacific Region, ASPI 2014. Available at: http://kipis.sfc.keio.ac.jp/wp-content/uploads/2014/04/ASPI_cyber_maturity_2014.pdf
21. ASPI, Cyber Maturity in the Asia-Pacific Region, ASPI 2014, p 31. Available at: http://www.spain-australia.org/files/documentos/62_ASPI-Cyber-Maturity-2016.pdf
22. Amnesty International, Undertnading Freedom of Expression in China. Amnesty International 2006. Available at: http://www.agsm.edu.au/bobm/teaching/BE/AmnestyReportonYahooMicrosoftGoogleinChina.pdf

Other electronic materials

1. UN, World Statistics Pocketbook: Cambodia. Available at: http://data.un.org/CountryProfile.aspx?crName=Cambodia

2. MPTC, Fact Sheet on Telecommunication Sectors, June 2016. Available at: http://www.mptc.gov.kh/site/detail/607
3. New Comprehensive Chinese Cybersecurity Law Approved, Squire Pattion Boggs, 2016. Available at: http://www.squirepattonboggs.com/~/media/files/insights/publications/2016/11/New-Comprehensive-Chinese-Cyber-Security-Law-Approved/Comprehensive-Chinese-Cybersecurity-Law-Alert.pdf
4. A Peek into Singapore's New Cybersecurity Act. Baker Mckenzie, 26.10.2016. Available at: http://www.bakermckenzie.com/en/insight/publications/2016/10/peek-into-the-new-cybersecurity-act/
5. MoH. Health Information System Strategy Plan 2008-2015, 2008. Available at: http://www.hiscambodia.org/public/fileupload/HISSP_ENG.pdf
6. WHO. eHealth: The health data ecosystem and big data. Available at: http://www.who.int/ehealth/en/
7. WHO. eHealth Country Context Indicators: Cambodia, 2016. Available at: http://www.who.int/goe/publications/atlas/2015/khm.pdf?ua=1
8. Tech advisor. 4 different types of hackers. 28.04.2016. Available at: http://www.techadvisory.org/2016/04/4-different-types-of-hackers/
9. Ou, P. Status of Cybercrime in Cambodia. Presentation at Octopus Cooperation against Cybercrime in Stasbourg, France,November 2016. Avaiable at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806bdc39
10. Tan, S. Security is everyone business: Don't become the healing. Presentation in Cambodia-Korea Information Session workshop, Phnom Penh, 23 June 2015.
11. CamCERT, Who we are? Available at: https://www.camcert.gov.kh/who-we-are/
12. CCHR, The criminalization of defamation of expression in Cambodia. CCHR Briefing note 2014. Available at: http://cchrcambodia.org/admin/media/analysis/analysis/english/2014_05_27_CCHR_Briefing_Note_Defamation_in_Cambodia_(ENG).pdf
13. CCHR, Case Study Series on Phel Phearun case, Factsheet 2013. Available at: http://cchrcambodia.org/index_old.php?url=media/media.php&p=factsheet_detail.php&fsid=54&id=5

14. CCIM, “Charges on Defamation Cases Against Facebook User Dropped”, 19 March 2013. Available at: http://www.ccimcambodia.org/what-we-do/internet-freedom/36-charges-on-defamation-case-against-facebook-user-dropped
15. Kothara, H. Presentation on Economic Aspect of Spectrum Management, November 2016. Available at: http://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2016/Nov-SM-Economics/Presentations/Day%202%20-%20Session%204%20(Cambodia).pdf
16. TRC, History of Telecommunication Regulator of Cambodia. Available at: https://www.trc.gov.kh/about-us/background/
17. TRC, Mobile Phone Subscription. Available at: https://www.trc.gov.kh/mobile-phone-subcribers/
18. Tan, S. Presentation on Cambodian Master Plan 2020 and Draft T-ICT Development Policy. Cambodian-Korean Information Security Workshop on 23 June 2015.
19. Mok, K. Presentation on e-Government Status in Cambodia. Available at: https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2015/August-eGov2015/Session-2/S2B_Khemera_Mok.pdf
20. Article 19, Cambodia: Secret Draft Cybercrime Law seeks to undermine free speech online, Article 19, Press release 09. 04. 2014. Available at: https://www.article19.org/resources.php/resource/37516/en/cambodia:-secret-draft-cybercrime-law-seeks-to-undermine-free-speech-online
21. Sokha, C. Presentation on ICT Development in Cambodia. CICC Forum, Tokyo, December 2015. Available at: http://www.cicc.or.jp/japanese/kouenkai/pdf_ppt/pastfile/h27/151013-2kh.pdf
22. CCHR, Cyber Laws: Tools for Protection or Restriction Freedom of Expression? CCHR Briefing note February 2014, p 2-3. Available at: https://www.ifex.org/cambodia/2014/03/03/cambodia_cyber_crimes_legislation_cchr.pdf
23. About Politikoffee. Available at: http://politikoffee.com/about-us/
24. Peter, Z. “Cambodia’s bloggerati fear new Internet law”, 04.05.2014. Available at: http://www.aljazeera.com/indepth/features/2014/05/cambodia-bloggerati-fear-new-internet-law-201454115127157534.html
25. CCC, Minute of Consultative Meeting on the draft of Cybercrime Law, 05 June 2014. Available at: https://www.ccc-cambodia.org/downloads/events-archive/2014/cybercrime-draftlaw/Cybercrime%20Law_Minute_Meeting.pdf

26. CHRAC, Compilation of the reports submitted by CSOs to UNHRC during 18th session of UPR of the Kingdom of Cambodia, July 2013, p 20. Available at: http://sithi.org/upr/docs/Compilation_of_Reports_CHRAC.pdf
27. CCIM, Report on Challenges for Independent Media Development in Cambodia, March 2013, p 3. Available at: http://www.ccimcambodia.org/report/CCIM_report_indepedent_media_promotion.pdf
28. About ASEAN. Available at: http://asean.org/asean/about-asean/history/
29. CoE, Chart of signatory and ratification of Treaty 185, The Convention on Cybercrime. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures
30. Kirsch, G. Controlling the Media in Japan. Available at: http://nottspolitics.org/2016/07/11/controlling-the-media-in-japan/

Annex I. Draft law on Cybercrime Law of Cambodia

Draft V.1 Unofficial Translation to English

Draft by Cybercrime Law Formulation Working Group of Council of Ministers

Chapter 1 – General Provision

Article 1: Purpose

This law has a purpose to determine education, prevention measures and combat all kinds of offense commit by computer system.

Article 2: Objective

This law has objectives:

Ensure the implementation of law, anti-cybercrime and combating all kinds of offense commit by computer system

Ensure safety and prevent all legitimate interest in using and developing technology

Article 3: Scope

This law is applicable to all offenses in this law in the following situation:

- Offense committed inside Kingdom of Cambodia or
- Offense committed inside or outside Kingdom of Cambodia and effect to legal and natural person or interest of Kingdom of Cambodia.

Article 4: Terms and Definition

The technical terms in this law are as follow:

1. *"computer system*" means any device or assembly of interconnected devices or that are in an operational relation, out of which one or more provide the automatic data processing by means of a computer program.
2. *"automatic data processing"* is the process by means of which the data in a computer system are processed by means of a computer program.
3. "Computer Program" means a sum of instructions expressed in letters, or codes, or illustrations, or in any other possible forms, once incorporated in a computer, which has its aim to accomplish a task or particular result by means of a computer or through an electronic procedure capable of information processing.
4. "computer data" are any representations of facts, information or concepts in a form that can be processed by a computer system. This category includes any computer program that can cause a computer system to perform a function.
5. "Content" refers to electronic form including text, images, graphics, animation, symbols, voices, and video.
6. Service providers refer to:
    1. any natural or legal person offering the users the possibility to communicate by means of a

computer system;

2. any other natural or legal person processing or storing computer data for the persons mentioned in paragraph 1 and for the users of the services offered by these;

7. "traffic data" are any computer data related to a communication by means of a computer system and generated by this, which represent a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, volume and duration, as well as the type of service used for communication.
8. "security measures" refers to the use of certain procedures, devices or specialised computer programs by means of which the access to a computer system is restricted or forbidden for certain categories of users;
9. "competent authority" refers to the Secretariat of National Committee on Anti-Cybercrime or any competent authority in other countries.
10. "Website" refers to place on the Internet, which you can find any information.
11. A person acts without right in the following situations:

    a) is not authorised, in terms of the law or a contract;

    b) exceeds the limits of the authorisation;

    c) has no permission from the competent natural or legal person to give it, according to the law, to use, administer or control a computer system or to carry out scientific research in a computer system.

Chapter 2 – National Anti-Cybercrime Committee (NACC)

Article 5: Establishment of National Anti-Cybercrime Committee (NACC)

The National Anti-Cybercrime Committee is established and the abbreviation is NACC.

Article 6: Composition of NACC

The NACC shall composed of the following:

1. Prime Minister		Chairman
2. Deputy Prime Minister, Minister in Charge of Council of Ministers		Deputy Chairman
3. Secretary of State	Ministry of Interior	Member
4. Secretary of State	Ministry of Foreign Affair	Member
5. Secretary of State	Ministry of Information	Member
6. Secretary of State	Ministry of Posts and Tel	Member
7. Secretary of State	Ministry of Justice	Member
8. General Commissioner	National Police	Member
9. Representative	Anti-Terrorism	Member
10. Representative	Council of Jurist	Member
11. Representative	Ecosocc	Member
12. Representative	Chamber of Commerce	Member

13. Secretary General	NiDA	Member
14. Secretary General	NACC	permanent Member

The actual person of NACC will be determined in separate Royal Decree.

Article 7: Duties of NACC

The National Anti-Cybercrime Committee has the following duties:

- Devises strategies, action-plans, and related programs in securing cyber and information grid for the Royal Government of Cambodia.
- Advises and recommend course of actions to the General Secretariat of the National Anti-Cybercrime Committee
- Supervises work-flows and course of action-plans implementations of the General Secretariat of the National Anti-Cybercrime Committee
- Issues findings and appropriate recommendations for ministries and departments to ensure the security of cyber and information grid of the Royal Government of Cambodia.
- Provides cyber and information grid security report for the nation to the Royal Government bi-semester and annually.
- Performs duties directed by the Royal Government of Cambodia.

Article 8: General Secretariat of NACC

NACC has one General Secretariat as an operation unit. General Secretariat of NACC is lead by one Secretary General and a number of Deputy Secretary General as assistance.

Secretary General and Deputy Secretary General are appointed by Royal Decree.

The organization and function of the General Secretariat is defined by Sub Decree.

Article 9: Duties of The Secretary General of NACC

The General Secretariat of the NACC has the following duties:

- Enforces laws, orders, and laws related to cyber-crime.
- Investigates, supervises, and researches including develops measures relating to cyber-criminal activities.
- Leads, manages, prevents, interrupts, and counter strikes against any cyber- criminal activities directed toward the Kingdom of Cambodia.
- Develops regulations, standardization, and strategic plans related to cyber-
- Supervises, evaluates, and certifies security qualities meeting standards for computers systems, network architecture, computer programs, and information technology (cyber) services.
- Enforces, publicizes, educates, and elevates the nation's knowledge in information technology.
- Work in cooperation with ministries, organizations of the Royal Government of Cambodia, national organizations, regional organizations, and international communities in order to investigate, supervise, research, manage, prevent, interrupt, and counter strike against cyber-criminal activities.

- Appoints, replaces, and manages, or requests for appointment and replaces government's employees under the direction of the General Secretariat of NACC.
- Supervises and develops the NACC's yearly budget for submission.
- Writing all official reports of all related for the NACC and the Royal Government of Cambodia.
- Performs duties directed by the NACC and the Royal Government of Cambodia.

Article 10: Officials of the General Secretariat of NACC

The officials of the Secretariat General of NACC include the persons appointed or transferred or assigned to work for the Unit and the contractual officials. These officials have to follow the provisions of the law and legal norms in force.

The Secretary General of the NACC can recruit local or international experts, specialists or researchers, on the voluntary or contractual basis, to provide technical expertise on anti-cybercrime.

Article 11: Branches of General Secretariat of NACC

The Secretariat General of NACC may have its offices in the Capital and all provinces of the Kingdom of Cambodia to serve as its branches. The Offices for General Secretariat of NACC perform their work under the leadership of Secretary General of General Secretariat of NACC. The Office for General Secretariat of NACC is led by one chief and a number of deputy chief as his assistants.

Article 12: Budget and Resources for NACC

The NACC has a separate budget package for its operation and the package is within the budget package of the Office of the Council of Ministers.

The NACC receives needed resources from the Royal Government and has the right to receive donations or assistance from national and international organizations.

Chapter 3: Procedure Provision Article

13 - Procedure for Cybercrime Offence

Procedure for Cybercrime offenses, which is stated in this law, shall be implemented as stated in the penal code procedure if there is no separate procedure in this law.

Article 14 - Officials competent to investigate Cybercrime offence

Secretary General, Deputy Secretary General and officials of National Anti- Cybercrime Committee who gain an advantage as judicial police official are empowered to investigate cybercrime offenses that are stipulated in this law and those in the panel code.

Other persons or units that are aware of cybercrime offenses are stipulated in this law and cybercrime offenses stated in the panel code share make complaints to the National Anti-Cybercrime Committee.

Article 15 – Appointment of National Anti-Cybercrime Committee officials as judicial police

Secretary General and Deputy Secretary General of National Anti-Cybercrime Committee are legally entitled to a status as judicial police officials in order to perform their duties.

Officials of National Anti-Cybercrime Committee may be entitled to status as judicial police officials in accordance with the provisions in the penal procedure code.

The Secretary General of National Anti-Cybercrime Committee takes charge of preparing list of officials of National Anti-Cybercrime Committee who are entitled to status as judicial police officials through Prakas of the Minister of Justice.

Article 16 – Investigation Power of NACC

Officials of National Anti-Cybercrime Committee who are appointed as judicial police take charge of investigating cybercrime offences. If during the course of a cybercrime offence, investigation different offenses are found whose facts are related to the offence being investigated by National Anti-Cybercrime Committee, officials of National Anti-Cybercrime Committee shall make complaint to competence authority.

Secretariat of National Anti-Cybercrime Committee can not investigate other offences except ones unless with the court order.

The court can order National Anti-Cybercrime Committee to undertake forensic inquiries in order to facilitate the work of the court.

In the framework of these investigations and contradictory to article 85 (power of judicial police officials in flagrant offence investigation), article 91 (searching), article 94 (subpoena in the case of flagrant offence investigation) and the article 114 (subpoena for preliminary investigation) of the code of criminal procedure, the Secretary General of National Anti-Cybercrime Committee or officially assigned representative has the duty to lead, coordinate and control the mission of those officials instead of the role of prosecutor to the point of arresting a suspect.

After the arrest, prosecutor exercises his power as stated in the code of criminal procedure.

At the end of each investigation, the National Anti-Cybercrime Committee shall submit all facts to the prosecutor for further action in conformity with the provisions of the code of criminal procedures. **Article 17: Preservation of Computer Data and Traffic Data**

1. In urgent and dully justified cases, if there are data or substantiated indications regarding the preparation of or the performance of a criminal offence by means of computer systems, for the purpose of gathering evidence or identifying the doers, the expeditious preservation of the computer data or the data referring to data traffic, subject to the danger of destruction or alteration, can be ordered.
2. During the criminal investigation, the preservation is ordered by the prosecutor through a motivated ordinance, at the request of the criminal investigation body or ex- officio, and during the trial, by the court order.
3. The measure referred to at paragraph (1) is ordered over a period not longer than 90 days and can be exceeded, only once, by a period not longer than 30 days.
4. The prosecutor's ordinance or the court order is sent, immediately, to any service provider or any other person possessing the data referred to at paragraph (1), the respective person being obliged to expeditiously preserve them under confidentiality conditions.
5. In case the data referring to the traffic data is under the possession of several service providers, the

service provider referred to at paragraph (4) has the obligation to immediately make available for the criminal investigation body or the court the information necessary to identify the other service providers in order to know all the elements in the communication chain used.

6. Until the end of the criminal investigation, the prosecutor is obliged to advise, in writing, the persons that are under criminal investigation and the data of whom were preserved.

Article 18: Copying Data

1. Within the term provided for at art. 17 paragraph (3), the prosecutor, on the basis of the motivated authorisation of the prosecutor specially assigned by the general prosecutor of the office related to the Court of Appeal or, as appropriate, by the general prosecutor of the office related to the Supreme Court, or the court orders on the seizing of the objects containing computer data, traffic data or data regarding the users, from the person or service provider possessing them, in view of making copies that can serve as evidence.
2. If the objects containing computer data referring to the data for the legal bodies in order to make copies, the prosecutor mentioned in paragraph (1) or court orders the forced seizure. During the trial, the forced seizure order is communicated to the prosecutor, who takes measures to fulfil it, through the criminal investigation body.
3. The copies mentioned in paragraph (1) are achieved by the technical means and the proper procedures to provide the integrity of the information contained by them.

Article 19: Searching and Seizing Computer Data

1. Whenever for the purpose of discovering or gathering evidence it is necessary to investigate a computer system or a computer data storage medium, the prosecutor or court can order a search.
2. If the criminal investigation body or the court considers that seizing the objects that contain the data referred to at paragraph (1) would severely affect the activities performed by the persons possessing these objects, it can order performing copies that would serve as evidence and that are achieved according to art. 18, paragraph (3).
3. When, on the occasion of investigating a computer system or a computer data storage medium it is found out that the computer data searched for are included on another computer system or another computer data storage medium and are accessible from the initial system or medium, it can be ordered immediately to authorize performing the search in order to investigate all the computer systems or computer data storage medium searched for.

Article 20: Condition and Safeguard

1. The access to a computer system, as well as the interception or recording communication carried out by mean of computer system are performed when useful to fine the truth an the fact or identification

of the doers cannot be achieved on the basis of other evidence.

2. The measures referred to at paragraph (1) are performed by motivated authorisation of the prosecutor specially assigned by the general prosecutor related to the Court of Appeal or, as appropriate, of the general prosecutor of the office related to the Supreme Court, and for the corruption offences, of the general prosecutor of the National Anti-Corruption Office, by the criminal investigation bodies with the help of specialised persons, who are obliged to keep the confidentiality of the operation performed.
3. The authorisation referred to at paragraph (2) is given for 30 days at the most, with the extension possibility under the same conditions, for duly justified reasons, each extension not exceeding 30 days. The maximum duration of these measures is 4 months.
4. Until the end of the criminal investigation, the prosecutor is obliged to inform, in writing, the persons against whom the measures referred to in paragraph (1) are taken.
5. The procedures of the Criminal procedure Code regarding the audio or video recordings are applied accordingly.

Chapter 4: Offences

Article 21: Illegal Access

1. The access without right to a computer system is an offence shall be sentenced from 06 months to 03 years and fined from one million Riel (1,000,000) to six million Riel (6,000,000).
2. It is an offence where the act provided in paragraph (1) is committed with the intent of obtaining computer data, shall be sentenced from 06 months to 05 years and fined from one million Riel (1,000,000) to ten million Riel (10,000,000).
3. It is an offence where the act provided in paragraphs 1-2 is committed by infringing the security measures, shall be sentenced from 03 years to 12 years and fined from six million Riel (6,000,000) to twenty four million Riel (24,000,000).

Article 22: Data Espionage

1. Any person who obtains without authorization, for himself or for another, data which are not meant for him and which are specially protected against unauthorized access, shall be sentenced from 01 years to 03 years and fined from two million Riel (2,000,000) to six million Riel (6,000,000).
2. Data within the meaning of subsection 1 are only such as are stored or transmitted electronically or magnetically or in any form not directly visible.

Article 23: Illegal Interception

The interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data, shall be sentenced from 02 years to 07 years and fined from four million Riel (4,000,000) to fourteen million Riel (14,000,000).

Article 24: Data Interference

The alteration, deletion or deterioration of computer data or restriction to such data without right is an offence, shall be sentenced from 02 years to 07 years and fined from four million Riel (4,000,000) to fourteen million Riel (14,000,000).

Article 25: Unauthorized Data Transfer

The unauthorized data transfer from a computer system or by means of a computer data storage medium is an offence shall be sentenced from 03 years to 12 years and fined from six million Riel to twenty four million Riel (24,000,000).

Article 26: System Interference

The act of causing serious hindering, without right, of the functioning of a computer system, by inputting, transmitting, altering, deleting or deteriorating computer data or by restricting the access to such data, shall be sentenced from 03 years to 15 years and fined from six million Riel to thirty million Riel.

Article 27: Child Pornography

1. Any person when committed intentionally and without right, the following conduct:
    a) producing child pornography for the purpose of its distribution through a computer system;
    b) offering or making available child pornography through a computer system;
    c) distributing or transmitting child pornography through a computer system;
    d) procuring child pornography through a computer system for oneself or for another person;
    e) possessing child pornography in a computer system or on a computer-data storage medium.

Shall be sentenced from 01 year to 03 years and fined from two million Riel (2,000,000) to ten million Riel (10,000,000).

2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:
    a) a minor engaged in sexually explicit conduct;
    b) a person appearing to be a minor engaged in sexually explicit conduct;
    c) realistic images representing a minor engaged in sexually explicit conduct.

Article 28: Contents and Websites

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

1. Establishing contents that deemed to hinder the sovereignty and integrity of the Kingdom of Cambodia is a punishable offense of incarceration from one to three years and fined of 2,000,000.00 Riels (Two Million Riels) and up to 6,000,000.00 Riels (Six Million Riels).
2. Publications that deemed to incite or instigate the general population that could cause one or many to generate anarchism is punishable of incarceration from one to three years and fined of 2,000,000.00 Riels (Two Million Riels) and up to 6,000,000.00 Riels (Six Million Riels).
3. Publications or continuation of publication that deemed to generate insecurity, instability, and political cohesiveness is a punishable office of incarceration from one to three years and fined of 2,000,000.00 Riels (Two Million Riels) and up to 6,000,000.00 Riels (Six Million Riels).

4. Publications or continuation of publication that deemed to be non-factual which slanders or undermined the integrity of any governmental agencies, ministries, not limited to departments, federal or local levels, is a punishable offense of incarceration from one to three years and fined of 2,000,000.00 Riels (Two Million Riels) and up to 6,000,000.00 Riels (Six Million Riels).
5. Publications that deemed damaging to the moral and cultural values of the society as stated herein:
    a) Information that incites or instigates prejudice on race or clans, color, gender, language, religion, beliefs or political views, origin of race or nationality, and not limited to levels or class in society.
    b) Writings or pixilation that deemed to display inappropriate activities of persons, copulations between humans or animals, or devalue the moral of family values and pixilation that deemed to display domestic violence
    c) Manipulation, defamation, and slanders
    d) Drawings, pictorials, or pixilation that deemed to slander or defame human beings or commoners of the state performing activities unbecoming, with animals of any species is punishable of incarceration from one to three years and fined 2,000,000.00 Riels (Two Million Riels) and up to 6,000,000.00 Riels (Six Million Riels).

Publicizing with the intent to threatened and commit a crime not limited to one form of felonies or other felonies with the intent to interrupt a person or persons well- beings is punishable of incarceration from one to three years and fined 2,000,000.00 Riels (Two Million Riels) and up to 6,000,000.00 Riels (Six Million Riels). In the case of with the intent to threaten shall be treated as such law that is currently being enforced.

Article 29: Intellectual Property Right and Related Rights

Offences related to Intellectual Property Right and Related Rights need to implement it base on the existing Copyright and Related Right Law of Kingdom of Cambodia.

Article 30: Computer Related Fraud

The causing of a loss of property to another person by inputting, altering or deleting of computer data, by restricting the access to such data or by any interference with the functioning of a computer system with the intent of procuring an economic benefit for oneself or for another shall be sentenced from 03 years to 12 years and fined from six million Riel (6,000,000) to twenty four million Riel (24,000,000).

Article 31: Computer Related Forgery

The input, alteration or deletion, without right, of computer data or the restriction, without right, of the access to such data, resulting in inauthentic data, with the intent to be used for legal purposes, is a criminal offence and shall be punished with imprisonment from 2 to 7 years.

Article 32: Misuse of Device

1. Any person when committed intentionally and without right:

a. the production, sale, procurement for use, import, distribution or otherwise making available of:

i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 21 through 32;

ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 21 through 32; and

b. the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 21 through 32. A Party may require by law that a number of such items be possessed before criminal liability attaches.

Shall be sentenced from 1 year to 6 years and fined from two million Riel (2,000,000) to twelve million Riel (12,000,000).

2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 21 through 32 of this Convention, such as for the authorised testing or protection of a computer system.

Article 33: Attempt

Attempt to commit a misdemeanor as stated in Article 427 (Accessing or Maintaining Access to Automated Data Processing System), Article 428 (Act of Obstructing the Operations of Automated Data Processing System), Article 429 (Fraudulent Introduction, Deletion or Modification of Data), Article 430 (Participation in Group or a Agreement to prepare for the commission of Offences) of Criminal Code and Article 21 (Illegal Access), Article 22 (Data Espionage), Article 23 (Illegal Interception), Article 24 (Data Interference), Article 25 (Unauthorized Data Transfer), Article 26 (System Interference), Article 27 (Child Pornography), Article 28 (Contents and Websites), Article 29 (Intellectual Property Rights and Related Rights), Article 30 (Computer Related Fraud), Article 31 (Computer Related Forgery) and Article 32 (Misuse of Device) of this law shall face the same punishment as misdemeanor.

Article 34: Accessory Penalty applicable to certain Cybercrime Offences

For the felonies and the misdemeanors described in this present chapter, the following additional penalties may be pronounced:

1. the deprivation of civil rights;
2. the prohibition against pursuing a profession during which time the crime was committed in course of or during the occasion of pursuing of this profession;
3. the confiscation of any instruments, materials or any objects which have been used to commit the offense or were intended to commit the offense;
4. the seizure of the objects or funds with which the offense was funded and/or carried out ;
5. the confiscation of incomes or properties earned/generated by the offense;
6. the seizure of the utensils, materials and the furniture garnishing a premise in which the offense

was committed;

7. the confiscation of one or several vehicles belonging to the convicted person;
8. the posting of the decision of the sentence for 02 (two) months maximum;
9. the publication of the decision of the sentence in the newspapers;
10. Broadcasting of the decision of the sentence by all means of audio-visual communications for 08 (eight) days maximum.

Article 35: Accessory Penalty Applicable to Certain Legal Entities

The legal entity that commits offences as stated from article 21 to 32 in this law shall be subjected to fine of ..... to ..... and face accessory penalties as follows:

1. Dissolution
2. Placement under the court watch
3. Baring of operation of an activity or activities
4. Expulsion from public procurement
5. Prohibition on public saving appeal
6. Prohibition of the business establishment open to the public or used by the public
7. Confiscation of instrument, material or any objects which are used to commit offence or aimed to commit offence
8. Confiscation of objects or funds which are subject of committing offence
9. Confiscation of proceeds, materials and furniture in building where an offence is committed
10. Posting of conviction judgment
11. Publication of the conviction judgment on print media or the announcement on non-print media outlets

Chapter 5: Mutual Legal Assistance, International Cooperation and Extradition

Article 36: Extradition Provision

Provisions of Chapter 2, content 1, part/section 9 of Penal Procedure Code shall be applicable in terms of the extradition of the case related to cybercrime offenses.

Article 37: Mutual Legal Assistance

In the case of cyber-crime offences, the court authority of the Kingdom of Cambodia may delegate power to competent court authority of any foreign state and may also obtain power from the court authority of any foreign state, in order to:

1. Collect evidence, proof or answer, response through court means
2. Inform about documents of the court
3. Search, arrest, and confiscate
4. Examine objects and crime scene
5. Providing information and exhibit
6. Issue original process-verbal or its authentic copies and dossier, including bank statement,

accounting transactions, records of concerned institution, records of concerned company and trade records, as well as authentic and private documents;

7. Identify or provide expert witnesses and others, including detainees who agree to assist in the investigation or participate in the legal proceedings.
8. Identify or seek resources, property, equipment, and materials that derive from offence and offence means.
9. Place under temporary holding the products and properties obtained from corruption offences as well as equipment, materials being used or kept for committing offences.
10. Enforce the decision of confiscation, seizure or repatriation of products, properties, equipment, material derived from offence.
11. Order to confiscate all objects as stated above.
12. Inform about the criminal charge.
13. Interrogate the accused based on criminal procedure.
14. Find out and identify witnesses and suspects.

Article 38: Mutual Legal Assistance Procedure

Procedures for Implementing mutual legal assistance shall be in agreement with the principles stated in treaties or bilateral and multi-lateral agreement, and national law in force.

Chapter 6: Final Provision

Article 39: Abrogation

Any provisions that contradict with this law shall be abrogated.

Article 40: Law Implementation

This law shall go into effect 12 (twelve) months after the promulgation.