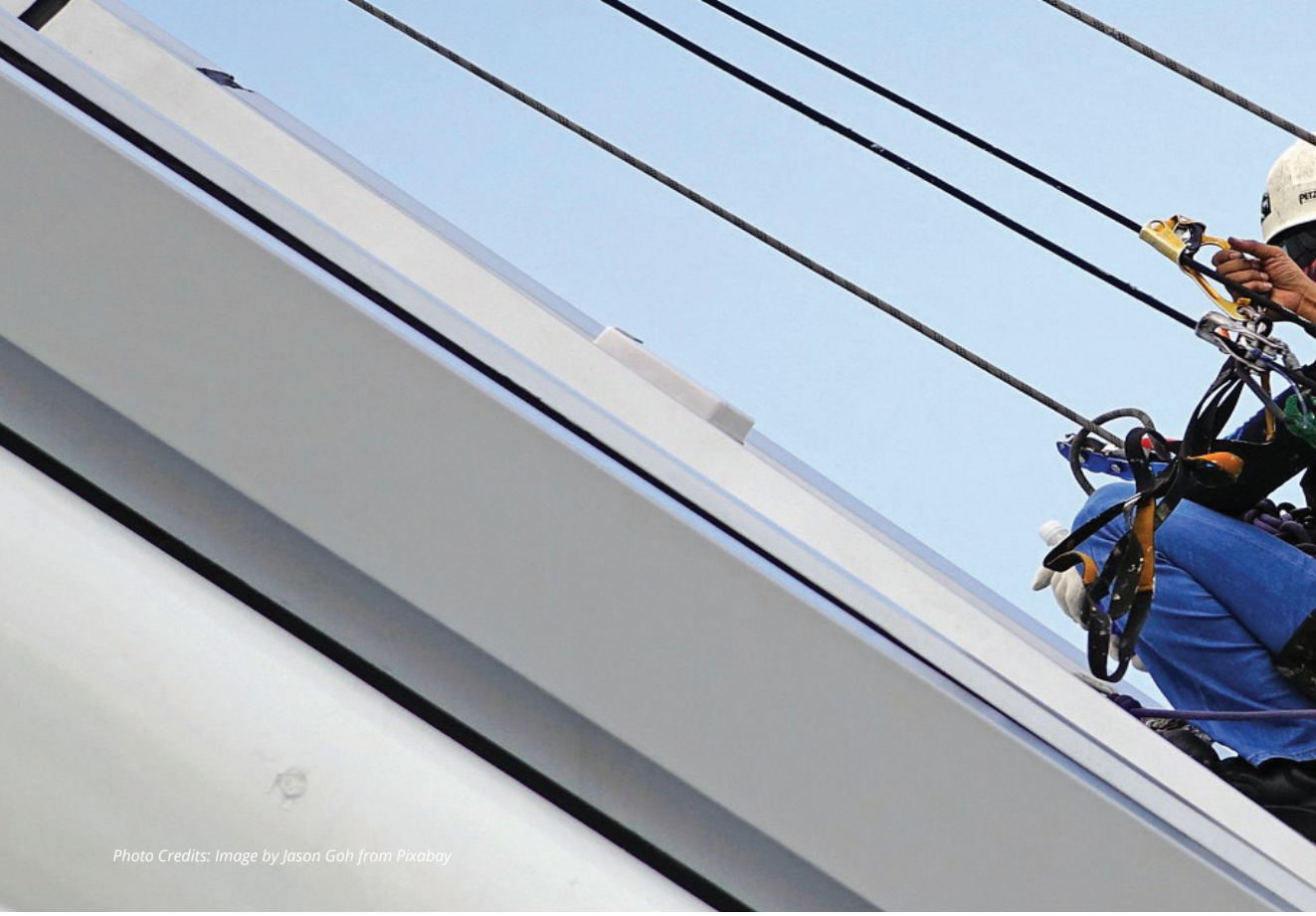


Photo Credits: Image by Jason Goh from Pixabay

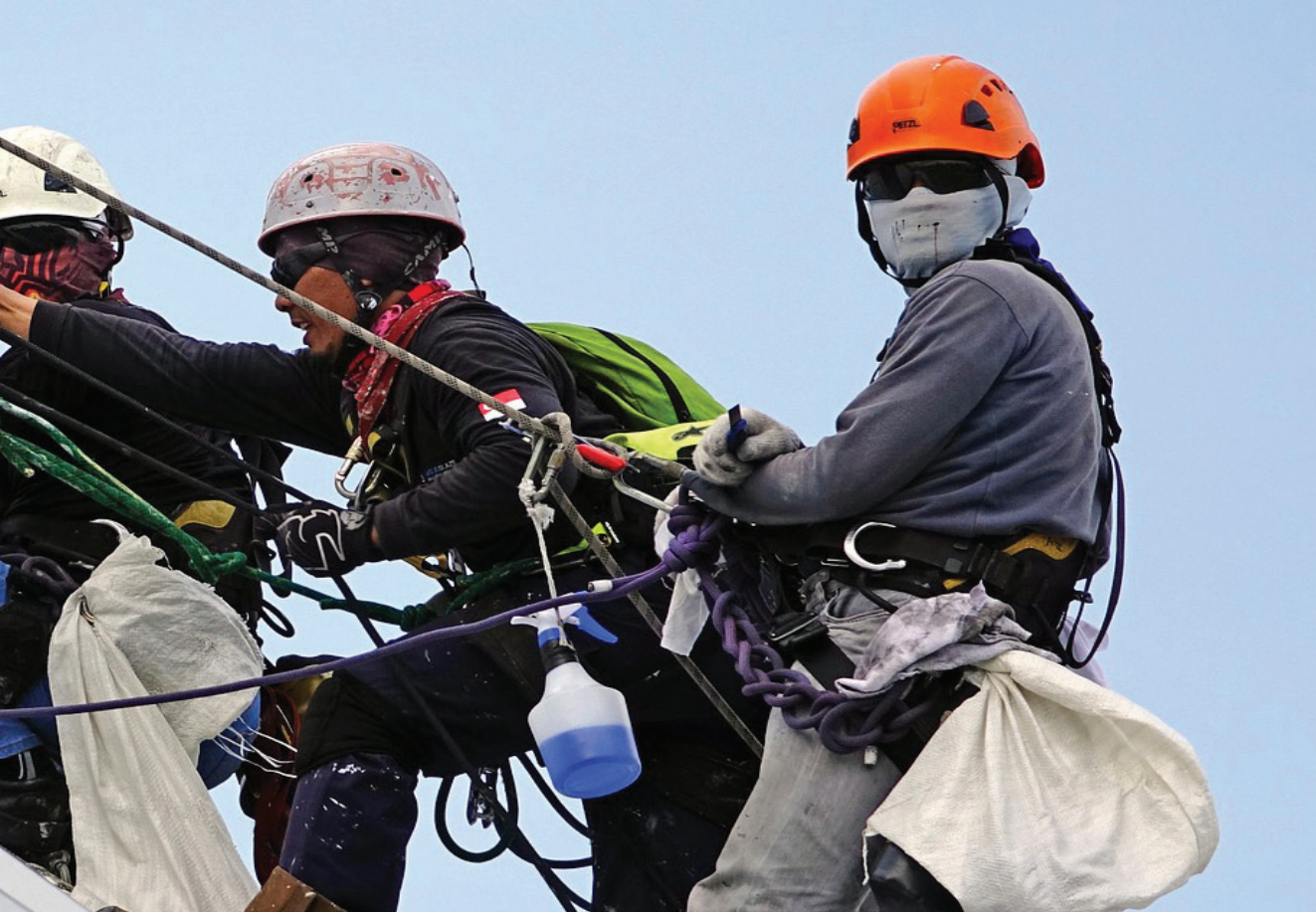
Reading time: 11 minutes

Cambodia v. Hackers: Balancing Security and Liberty in Cybercrime Law

Somaly Nguon[1] and Dr. Sopheak Srun[2]

1 Somaly Nguon is a Researcher in the field of Laws and Technologies. She is a researcher at Tallinn Law School, Tallinn University of Technology (TTU), Estonia and Research Fellow at Center for the Study of Humanitarian Law, Royal University of Law and Economics (RULE), Cambodia. She is a Co-founder and Legal Consultant at Lawtitude Tech OÜ in Tallinn, Estonia. Somaly holds Master in Law and Technology from Tallinn University of Technology in Estonia and Master in International Human Rights from Pañ̃ñāsāstra University of Cambodia (PUC). She is a lecturer in ICT Law and Cybersecurity course. She conducts extensive legal research and publications in the area of Cybersecurity law and e-Governance. Somaly also represented Cambodia and Tallinn Law School in the framework of Export Academy at Estonian House of Commerce.

2 Dr. Sopheak Srun is a Researcher in the field of Economics and International Trade. For more than seven years, he has been involved in working and managing many projects for both national and international NGOs, public and private sectors, and for foreign embassy. He is familiar with project design and project cycle management as well as in feasibility study and marketing research and evaluation. He holds a PhD degree in Economics from the University of Toulon and a Master degree of Business and Economic from the University of Lumière Lyon 2, both are in France. He is a lecturer in Project Management at the Royal University of Law and Economics (RULE) and lecturer in Business Strategic, Marketing research, and Statistics at French Cooperation Programs at RULE.



Abstract

Cybercrime is a well-known, yet poorly understood issue in Cambodia, and the country's existing legal framework is vague and unclear compared to international standards. Government websites have been subject to cyberattacks since 2002. Targets have included those of the Ministry of Foreign Affairs, the National Election Committee, the National Police, the military and the Supreme Court; thousands of official documents were leaked online by the hacktivist collective "Anonymous". There are also reports of malicious local hackers, but most go unnoticed and unpunished. As a developing country, Cambodia lacks good technology practices and legislation because of poverty, poor infrastructure, weak institutions, low literacy and low ICT awareness. This paper outlines the cybersecurity threats it faces and analyzes existing legal measures such as the Criminal Code and the new draft Cybercrime Law, also looking at how these laws could be interpreted too broadly and thereby potentially restrict fundamental rights. Cybersecurity practices in China, Japan and Singapore are briefly explored, followed by recommendations on making cybersecurity law in Cambodia more robust, specific and proportionate, in line with international treaties like the Council of Europe's Convention on Cybercrime.

Cambodia Under Attack

In 2012, the Cambodian government announced that it was in the process of drafting a Cybercrime Law which sparked fears that it could extend traditional media restraint to the online world.[3] After the announcement, a hacker group called NullCrew launched a campaign named "Operation The Pirate Bay (OpTPB)" to attack Cambodian websites to protest against 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 forces. As result, the operation leaked highly confidential information and posted a number of passwords for other hacktivist groups to use. Another hacktivist collective, Anonymous, caused over 5,000 documents to be stolen and leaked from Cambodia's Ministry of Foreign Affairs.[4] Following the above incidents, the Cambodian government announced a new law requiring surveillance cameras in internet cafes and telephone centers, and to retain footage for at least three months.[5]

Article 28 of the draft law regulates user content and websites. People who "establish contents deemed to hinder the sovereignty and integrity of the country or government agencies and ministries, incite or instigate, generate insecurity and political [incohesion], and damage the moral and cultural values, etc. are punishable from one to three years imprisonment and fine from five hundred U.S. dollars to one thousand and five hundred U.S. dollars ($500-1500)".[6] Before Cambodia's 2018 general election, a Chinese hacking group called TEMP.Periscope had shown extensive interest in the country's politics, causing active compromises of multiple Cambodian entities related to the Country's electoral system such as Cambodia's National Election Committee, foreign affairs, interior and ministry of finance and senate. FireEye said it had been tracking the group's activities since 2013 and believed that hackers were acting on behalf of the Chinese government in order to provide the Chinese government with widespread visibility into Cambodian elections and government operations. However, China denied supporting hacking attacks and said that they would not allow any individual to use any resources to commit cyber attacks.[7] ICT development in Cambodia is still at a sensitive stage compared to other countries in the region, and thus the country may be less prepared than others in terms of cybersecurity. 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 a Cybercrime Unit in the National Police department in charge of telecommunication crime. However, the country scores poorly in various categories of cybersecurity according to the Cyber-wellness profile published by the International

3 Freedom on the Net: Cambodia, (Washington, D.C., Freedom House, 2013), 8-9. Available at: https://freedomhouse.org/sites/default/files/resources/FOTN%202013_Cambodia.pdf

4 Security: How can we enhance cybersecurity in ASEAN?, (YMAC, 2016), 2. Available at: http://www.sp.edu.sg/ymac/documents/securitycybersecurity.pdf

5 Mong Palatino, Cambodia: Mandatory internet Surveillance Cameras, (Amsterdam, Global Voice, 2012). Available at: https://globalvoices.org/2012/09/09/cambodia-mandatory-internet-surveillance-cameras/

6 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

7 John Reed, Chinese hackers target Cambodia opposition ahead of election, (UK, Financial Times, July 11, 2018). Available at: https://www.ft.com/content/4d4482e6-84a0-11e8-96dd-fa565ec55929

Telecommunication Union (ITU) in 2014.[8] Cyber-wellness in Cambodia has been discussed in a small circle among scholars because it seems to be a new topic in the country.

This research looks at Cambodia's efforts in combating cybercrime, specifically trying to answer two questions: What are the main components of Cambodia's cybersecurity policy and how was it developed? Does the draft law on cybercrime address cybersecurity issues in Cambodia, and is it balanced and in line with international cybersecurity standards? This research also aims to propose international good practices and concrete steps that the government of Cambodia may consider implementing.

Understanding Cybersecurity

Cybersecurity and Law

The term "cybersecurity" was first used by computer scientists in the early 1990s in the context of networked computers. The term gained more widespread use, beyond a mere technical conception, when threats started to arise in the digital cyberspace.[9] Cybersecurity has been defined by the 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"*[10] 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".*[11] New technologies give rise to new trends in cyberspace crime. Their economic loss is estimated to exceed that of global drug trafficking. Some now consider global cybercrime the biggest underworld industry causing US$1 trillion loss worldwide annually.[12]

In light of these developments, the gap between law and technology has widened. Traditional legal systems have failed to keep pace with new technology and ICTs that have made the impossible possible.[13] The evolution of computers and information systems has given rise to new controversies regarding the boundaries and obligations, intellectual property rights, privacy rights, diplomatic relations and military affairs, critical infrastructure and, finally, public welfare. Cybercrime is one of the most serious threats to economic and national security around the world. The volume of data breaches, mostly caused by hacking and malware, is at the highest level ever. Highly confidential information is stolen and leaked causing significant legal and ethical concerns.[14] Cybercrime can be defined as *"any illegal behavior directed by means of electronic*

8 Global Cybersecurity Index & Cyberwellness Profiles, (Geneva, ITU 2015), 117-118. Available at: http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf

9 Lene Hansen, Helen Nissenbaum, Digital Disaster: Cyber Security, and the Copenhagen School, (Oxford, International Study Quarterly, 53, 2009), 1155. Doi:10.1111/j.1468-2478.2009.00572.x

10 Overview of Cybersecurity, Recommendation ITU-T X. 1205, (Geneva, ITU, 2008), 2. Available at: https://www.itu.int/rec/T-REC-X.1205-200804-I

11 Report on best practice for a national approach to cybersecurity: A management framework for organizing national cybersecurity efforts, (Geneva, ITU-D secretariat draft, 2008), 5. Available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf

12 Edita Gruodyte, Mindaugas Bilus, Investigating Cybercrimes: Theoretical and Practical Issues, Kerikmäe, T. (Ed.), Regulating eTechnologies in the European Union, (Switzerland, Springer, 2014), 218.

13 Roger Brownsword, Morag Goodwin, Law and the Technology of the Twenty-first Century, (Cambridge, Cambridge University Press, 2012), 8.

14 Sean Harrington, Professional Ethics in the Digital Forensics Expert: Ultimate Tag-Team or Disastrous Duo?, (U.S., William Mitchell L. Rev. 38 (1), 2011), 2. Available at: http://open.mitchellhamline.edu/wmlr/vol38/iss1/8

operations that target the security of computer systems and the data processed by them".[15] 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".*[16]

Cybersecurity Actors

There are multiple actors perceived to be threats in the cyberspace, each with different behaviors and motivations behind their attack. According to Alexander Klimburg, cybersecurity actors are divided into three major groups includes: State Actors, Organized Non-State Actors, and Non-Organized Non-State Actors.[17] Hacking without permission and authorization is considered illegal. But people usually have misconceptions about the term "hacker", who according to Gross, *"is anybody looking to manipulate technology to do something other than its original purpose".*[18] Given the number of high profile data theft, severe compromises and stolen passwords, it is easy to see how the public forms negative opinions and assumes that all hackers have malicious intent. Nevertheless, there are some people who appreciate hackers as highly skilled computer experts who manipulate systems and expose vulnerabilities and point out flaws before really malicious actors can exploit them. Hackers' actions inspire computer programmers to code their software more securely against vulnerabilities.[19] Hence, hackers are categorized into several types, too.

For example, a "Script Kiddie" is a less experienced intruder who uses relatively simple programs written by expert hackers, thus automating all the difficult steps for them. A Script Kiddie usually cannot cause much damage due to their beginner level skills.[20] A "Hacktivist" describes someone who uses computer skills to make political statements and actions. Social justice campaigners can deploy a range of hacktivist strategies to further their cause.[21] Famous examples of hacktivists working in groups include Anonymous, LulzSec or AntiSec. "Cybercriminals" use technology to facilitate a crime, primarily to gain money and personal benefit. Their targets could be anyone, from individuals to small businesses to large enterprises and banks. Cybercriminals attack by using social engineering tricks to manipulate users into providing sensitive information, steal their banking credentials, infect organizations, health care records or credit cards with ransom ware or another form or malware, and to exploit any weakness in the network.[22] "Insiders" are hackers who are typically an employee, a former employee or a contractor who tries to steal sensitive documents or disrupt the organization's operations. Edward Snowden is a prime example of an insider who hacked his own organiza-

15 Gruodyte, Investigating Cybercrimes, 218.

16 Ibid.

17 Klimburg, A., Healey, J. Strategic Goals & Stakeholders, Klimburg, A. (Ed.), National Cyber Security Framework Manual, (Tallinn, NATO CCDCOE, 2012), 68-70.

18 Doug Gross, Mafiaboy breaks silences, paints portrait of a hacker, (U.S., CNN, 2011). Available at: http://edition.cnn.com/2011/TECH/web/08/15/mafiaboy.hacker/index.html?iref=obnetwork

19 Lalisa Long, Profiling Hackers, (Australia, SANS Institute InfoSec Reading Room, 2012), 2-3. Available at: https://www.sans.org/reading-room/whitepapers/hackers/profiling-hackers-33864

20 William A. Arbaugh, et al., Window of vulnerability: a case study analysis, (U.S., 33 (12), 2000), 52. DOI: 10.1109/2.889093

21 Matthew Eagleton-Pierce, The internet and the Seattle WTO Protests, (UK, Peace Review, 13 (3), 2001), 334. DOI: 10.1080/13668800120079027

22 Chicone, R. A Layman's Guide to Cyber Threats, Threat Actors, Attacks, and Intelligence, (U.S.,Kaplan University, 2015), 2. Available at: http://alliance.kaplan.edu/uploadedFiles/_Global_Content/Generic/Promotional_contents/Laymans%20Guide%20to%20Cyber%20Threats%20Article.pdf

tion. Employees of an organization know exactly where precious information is stored.[23] Last but not least, "state sponsored" actors are known as advanced persistent threats[24] that consist of talented, well-equipped, well-organized and resourceful cyber attackers with advanced cyberattack tools, who work for a government in order to disrupt or compromise other governments, organizations or individuals in order to gain access to valuable data or intelligence, and can create incidents that have international significance.[25]

Categories of cybercrime

Many different types of cybercrimes are committed every day on the internet, such as financial crimes, unauthorized access, theft, viruses/worms, Distributed Denial of Service (DDoS) attacks, trojan horse attacks, web jacking, cyber terrorism, cyber pornography, online gambling, IP crimes, email spoofing, cyber defamation, cyber stalking, etc.

In Cambodia, internet cafés have been an easy place for viruses to spread due to their limited cyber security measures.[26] Other common issues reported in the country are web defacement, phishing, hacking, email hijacking, telecom fraud and fraudulent money transfer.[27] The most targeted sites by hackers are government websites such those of ministries, government agencies and other high-ranking government officials. They are usually subjected to SQL injection and DDoS attacks. The Cambodian government experienced attack from groups such as Black Hats Team from Iran, Anonymous, Young Geek, Brothers Team and NullCrew, as mentioned earlier. Very few official reports are made about cyberattacks that target private companies offering online services, such as banks and telecommunication operators. The private sector and ISPs usually have better equipment and technical experts to monitor the network traffic, filter spam and defend against certain malicious acts in the cyberspace. Nevertheless, most cybercrimes and -attacks have gone unnoticed and most victims of cyber incidents are reluctant to report them. The low amount of incident reports may be either due to the low impact of the incidents or due to the limited legal procedures and enforcement.[28]

Threat Responses

According to Soafer and Goodman, a significant weakness in the current system of combating computer misuse is the inconsistency between individual states of laws and effective investigation and prosecution measures.[29] The ITU Global Cybersecurity Agenda (GCA) calls for strategies to develop cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures, as well as to organize 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

23 Tan Teck Boon, We, Cittizens of Smart Signapore: Data Protection in Hyper-connected Age, (Singapore, RSIS Commentaries, No. 036, 2016) 1. Available at: http://hdl.handle.net/10220/40253

24 Chicone, R. A Layman's Guide to Cyber Threats.

25 Klimburg, Strategic Goals & Stakeholders 2012, 68-69.

26 Sopheak Cheang, Sinawong Sang, State of Cybersecurity and the Roadmap to Secure Cyber Community in Cambodia, (U.S., International conference on availability, reliability and security, IEEE, 2009), 652. doi: 10.1109/ARES.2009.144

27 Phannarith Ou, Status of Cybercrime in Cambodia. Presentation at Octopus Cooperation against Cybercrime in Strasbourg, France, November 2016. Avaiable at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806bdc39

28 Ibid.

29 Abraham David Sofaer, Seymour E. Goodman, The transnational dimension of cybercrime and terrorism, (California, Hoover Institution Press, 2001), 15-16.

the integrity of national critical information infrastructures, is central to achieving global cybersecurity.[30] Since cyber threats can originate anywhere around the globe, the challenges are inherently 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 cooperation.

However, it can take time to update national criminal law and facilitate the prosecution of new forms of online cybercrime. Indeed, some countries have not yet gone through this adjustment process.[31] Cambodia does not have any specific legislation dealing with cybercrimes yet, although the new Cybercrime Law is being drafted and the Criminal Code 2009 takes care of the cybercrime issues.

How Cambodia Defines Cybercrime

There are different names for cybercrime law in different legal systems. For example, it is called "Computer Misuse Act"[32] in Singapore. China got its "Cybersecurity Law" after The Standing Committee of China's legislature passed it in November 2016.[33] As of mid-2019 more Cambodians gain access to the internet, and the current "Cybercrime Law" is still in the drafting process. However, computer related offences were introduced for the first time in the Cambodian Criminal Code 2009 in Articles 317-320 and 427-432. The Criminal Code uses very general terms such as "Offences in information technology sector". [34] There is no specific definition of cyber offense or the specific categories of cybercrime in this legislation, so the Criminal Code alone cannot secure the nation from cyber threats and impose appropriate punishment on cyber criminals. The challenge for Cambodia's legal system is to stop the potential abuse of new technologies and make necessary amendments to the national criminal law.

Interestingly, some legal systems do not criminalize accessing another computer itself, unless the perpetrator has harmful intentions to obtain, modify, and damage the accessed data.[35] Opponents to the criminalization of 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 the targeted computer systems. In order to keep pace with innovation, the Cambodian government is putting more effort into legislating this space more appropriately.

Legislating Cyberspace

This section analyzes the existing legal framework and mechanisms that address cybersecurity in Cambodia, in particular the Criminal Code 2009, the Press Law, the Telecommunications Law 2015 as well as the new draft Cybercrime law, looking at whether these laws sufficiently address cybersecurity issues or not.

30 Understanding Cybercrime: Phenomena, Challenges and Legal Response, (Geneva, ITU, 2012), 179. Available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

31 Ibid.

32 Tan Teck Boon, We, Cittizens of Smart Signapore: Data Protection in Hyper-connected Age, (Singapore, RSIS Commentaries, No. 036, 2016) 1. Available at: http://hdl.handle.net/10220/40253

33 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

34 Criminal Code of the Kingdom of Cambodia, No.NS/RKM/1109/09, September 30, 2009.

35 Understanding Cybercrime: Phenomena, Challenges and Legal Response, (Geneva, ITU, 2012), 179. Available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

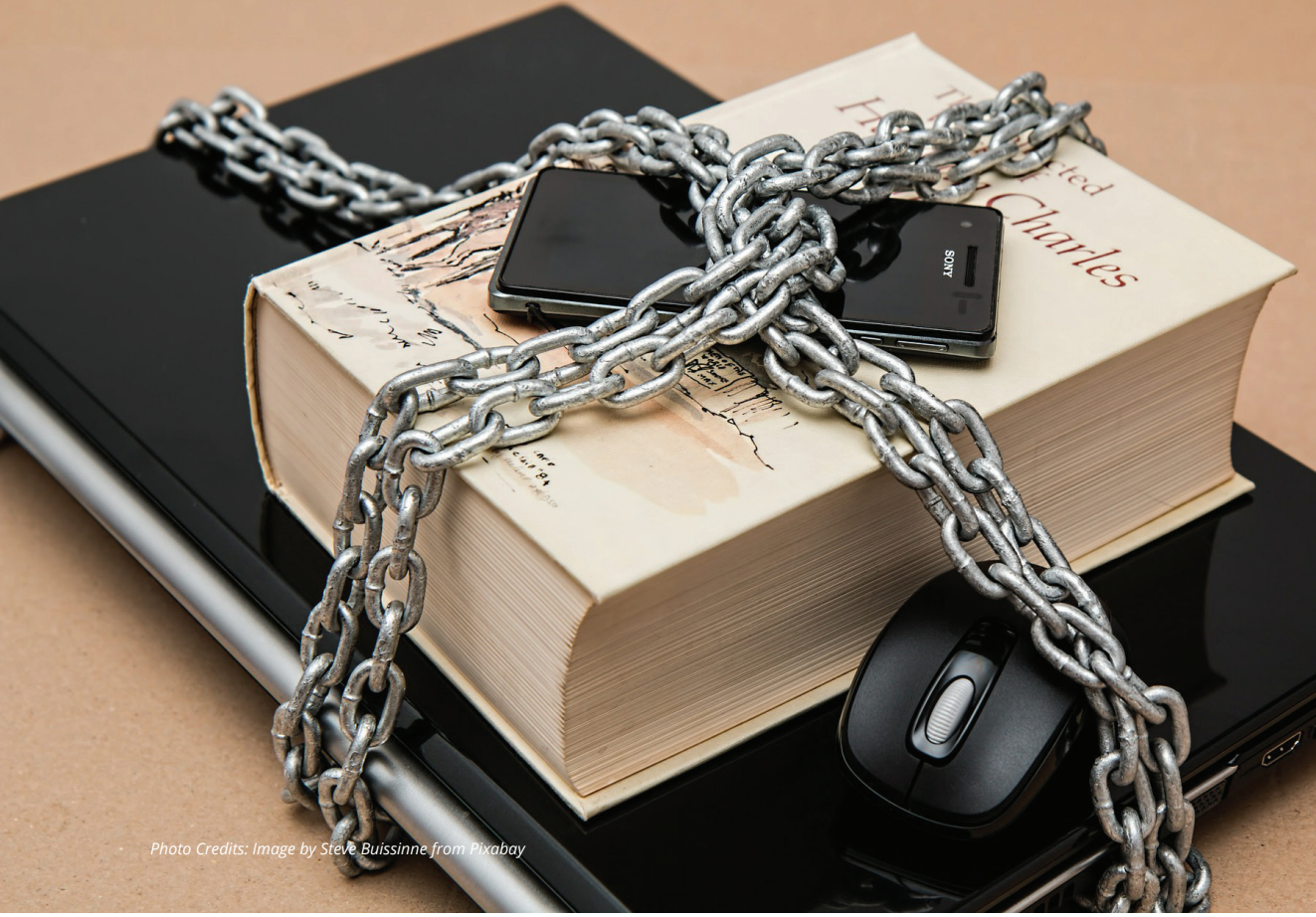


Photo Credits: Image by Steve Buissinne from Pixabay

Criminal Code of the Kingdom of Cambodia (2009)

The term "cybercrime" does not exist in any specific legislation in the Kingdom yet. While the controversial Cybercrime Law is still being drafted, the Cambodian Criminal Code 2009 has jurisdiction over the current cybercrime issues. Computer related offences were introduced for the time being in the Cambodian Criminal Code 2009 in Articles 317-320 and 427-432, the crimes being called *"Infringement on the secrecy of correspondence and telecommunication"* and *"Offences in the information technology sector". "Defamation and Insult"* is considered a type of cybercrime as well, if committed via computer networks.

Infringement on the secrecy of correspondence and telecommunication – the right to correspond is an international fundamental right part of private life recognized under international human rights law and 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 an interference and violation of the above rights.[36] According to the Cambodian Criminal Code, any act of opening, disappearing, delaying or diverting the correspondence addressed to a third party, in bad faith, is an infringement on correspondence.[37] In addition, fraudulently acquiring knowledge of the content of the correspondences addressed to a third party is categorized in the same way and is punishable by imprisonment of one to five years. Moreover, it can be fined between

36 Blanca Rodriguez Ruiz, Privacy in Telecommunications: A European and an American Approach, (Netherland, Kluwer Law International, 1997), 134-135.

37 Cambodia Criminal Code 2009, Art.317-320.

one hundred thousand and two million Riels. According Section 5 of this law, the act of listening or jamming a telephone conversation in bad faith shall be punishable in the same way.[38] There are additional penalties as well depending on the category and duration of the act, such confiscation of materials, prohibiting against pursuing a profession, posting and broadcasting the decision of the sentence.[39]

Offenses in the information technology sector – according to Article 427, the offenses refer to acts of *having access to automated data processing or maintaining access and when the act has resulted in either deletion or modification of the data contained in the system.*[40] Also the act of obstructing the operation of automated data processing systems, fraudulent introduction, deletion or modification of data, participation in a group, or agreement to prepare for the commission of offences are considered offenses in the information technology sector.[41] The phrase *"having access to automated data processing or maintaining access"* is being used in the current law without being specific as to whether it means *illegal* access, access to *unauthorized* data or *intentional* access to unauthorized data. The law also fails to specify the technical means and level of access and usage.

Defamation and insult – these are considered a type of cybercrimes as well if committed via computer network. Defamation is a concerning issue on the internet, 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"*.[42] 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".*[43] Defamation can be committed in the following ways: through speeches, announced in a public place or in a 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.[44] In February 2018, the National Assembly and Senate approved amendments to the Criminal Code, introducing a new *lèse-majesté* offense (Article 437) that makes it illegal to defame, insult or threaten the king. It carries a sentence of one to five years in jail, and a fine two to ten million riel (about USD$500 to USD$2,500). In May 2018, the Ministry of Information warned media outlets of the law, saying that distributing or reposting material that insult the king, in print, online or otherwise, constitutes a *lèse-majesté* offense.[45] Defamation and insult offenses under the Criminal Code are used together with the Press Law 1995. According to Article 306 and 308 of the Criminal Code, defamation and insults committed by means of media is subjected to the provision of the press law.[46] The Press Law also restricts journalists from publishing information that harms someone's honor and dignity and may be used to punish journalists who criticize public figures.[47] It also imposes

38 Ibid.

39 Ibid.

40 Ibid.

41 Ibid., Art. 428-432.

42 Sharon K. Black, Telecommunications Law in the internet Age, (San Francisco, Academic Press, 2002), 418.

43 Cambodia Criminal Code 2009, Art. 305.

44 Ibid.

45 Freedom on the Net 2018 – Cambodia, Freedom House, 2018. Available at: https://www.refworld.org/cgi-bin/texis/vtx/rwmain?page=printdoc&docid=5be16b22c

46 Cambodia Criminal Code 2009, Art. 306,308.

47 Yumiko Yasuda, Rules, Norms and NGO Advocacy Strategies: Hydropower development on the Mekong River, (New York,

restrictions on content which *"may affect the public order by inciting directly one or more persons to commit violence"*[48] or which *"may affect national security and political stability"*[49] or which affects *"the good custom of society".*[50]

Law on Telecommunications 2015

The Law on Telecommunications was promulgated in December 2015 as a legal instrument to supervise the telecom sector in Cambodia. The objectives of this law are to define the authority of the Ministry of Post and Telecommunication (MPTC), to establish and outline the duties of the Telecom Regulator Cambodia (TRC), to classify different types of authorization, certificate and licenses, and to set the supervision on the use of infrastructure and network, the fees, the fair competition and the protection of consumers.[51] A Report of the UN Special Rapporteur Rhona Smith on the situation of human rights in Cambodia submitted at the United Nations Human Rights Council highlighted concerns over the adoption of this law. She noted that "*the law requires telecommunications companies to turn over certain data to the government upon request"*[52]. She also highlighted that the degree of compliance with international human rights law lies in the interpretation and application of the law by law enforcement and judicial official.[53]

According to Article 6 the MPTC shall have the competence to control telecommunications and ICT service data, and all telecommunication operators shall provide their service user data to the MPTC.[54] A 2015 Regulation on Cell Phone Data threatens suspensions and fines for mobile operators who do not register the identities of consumers. The regulation obliges companies to supply police with identification details of SIM card holders on request. The TRC spokesman Im Vutha said that SIM card registration would enable the government to monitor telecom operators' databases.[55] Moreover, Article 97 allows secret surveillance of communications if conducted with the approval of the "legitimate authority".[56] Article 80 states that the *"establishment, installation and utilization of equipment in the telecommunications sector, if these acts lead to national insecurity, shall be punished by sentences from seven to fifteen years imprisonment."*[57] In addition to imprisonment, the offender shall be fined from 140 to 300 million Riels.[58] This could broadly mean that any communication conducted by any electronic means could be criminalized if it is deemed to create "national insecurity".

It should be noted that in May 2018 the Cambodian government also issued an interministerial "Prakas" (or proclamation) which ordered all ISPs to install the software necessary to monitor, filter, and block "illegal" content, including social media accounts. The Prakas ordered the MPTC to "block or close" websites and social media pages containing content deemed discriminatory or posing a threat to national security or unity.[59]

Routledge), 2015.

48 Law on the Press, Art 11.

49 Ibid., Art 12

50 Ibid., Art 14.

51 The Law on Telecommunications, No.NS/RKM/1215/017 dated 17 December 2015, Art 2.

52 Report of the Special Rapporteur on the situation of human rights in Cambodia, (United Nation, A/HRC/33/62), 10.

53 Ibid.

54 The Law on Telecommunications, Art. 6.

55 Freedom on the Net 2018 – Cambodia.

56 The Law on Telecommunications, Art. 97.

57 The Law on Telecommunications, Art. 80.

58 Ibid., Art 81.

59 Freedom on the Net 2018 – Cambodia

Cambodia vs Hackers

Cybercrime is a well-known, yet poorly understood issue in Cambodia, and the country's existing legal framework is vague and unclear compared to international standards.

Types of cyber criminals

Cyber Criminals

These guys break into systems purely with negative intentions.

- Stealing credit card information
- Altering public databases

Social Media Hacker

They focus on hacking social media accounts by using various techniques.

- Stealing social media accounts

Hacktivist

They are the protesters of the internet.

- Defacing websites
- Uploading promotional materials

Script Kiddie

They are the newbies.

- Running hacking softwares
- Running pre-written scripts

Crime & Attacks

Denial of e-services:
Infomation services are not available if needed.

Data integrity breach:
Data is modified in an unauthorised manner.

Data confidential breach:
Data is available for unauthorised entities.

DIGITAL INSIGHTS

KONRAD ADENAUER STIFTUNG

Why Cyber Security?

- Government efficiency
- Economic competitiveness
- E-way of life is susceptible to hackers
- Smart solution of information society
- Rapid digital innovations

Recommendations:

- Review existing laws to ensure that they do not overlap with each other and are applicable.
- The current draft law should adress cyber security properly.
- Determine the responsible authorities.
- Establish security measures for the nation more effectively.
- Actively involve in international and regional cyber engagement and cooperation.
- Provide cyber awareness programs to government officials, citizens, and schools.
- Cambodia should consider signing and ratifying the convention on cybercrime.

Content and Storyline: Somaly Nguon & Sopheak Srun
Infographic Designer: Singhtararith Chea
Editors: Robert Hör & Ann-Cathrin Klöckner

Article 66 provides for the general prohibition of any action in the communication sector that may *"affect public order and lead to national insecurity"*.[60] Because of the unclear wording, individuals may find it hard to understand when it may apply, or when the consequences of their actions may constitute as a violation to this law, and thus incur penalties.[61]

The law also provides specific powers for the destruction of evidence. Article 76 states that, *"in case the evidence of this offense is prohibited products or dangerous, telecommunication inspection officials have the right to request the prosecutor's ruling to destroy in line with applicable procedures"*.[62] It is unclear what the terms "applicable procedures" and "prohibited or dangerous products" mean. Destruction of evidence under this article could affect the right to fair trial for those charged under this law because if a defendant is deprived of material evidence, they are deprived of the fundamental right to a fair trial because they cannot present a complete defense.[63]

The New Draft Law on Cybercrime

Cybercrime can be categorized into three main categories: (1) Acts against confidentiality, integrity and availability of computer data or systems, which include illegal access to computer systems; illegal access, interception or acquisition of computer data; illegal interference with a computer system or computer data; production, distribution or possession of computer misuse tools; breach of privacy or data protection measures; (2) Computer related acts for personal or financial gain or harm, which are computer related fraud or forgery; computer related identity offences; computer related copyright or trademark offences; sending or controlling sending of spam; computer related acts causing personal harm; computer related solicitation or 'grooming' of children and; (3) Computer content related acts uch as computer related acts involving hate speech; computer related production, distribution or possession of child pornography; and computer related acts in support of terrorism offences.[64] This section will walk through the main components of the Cambodian draft law on Cybercrime and analyze its scope, structure, definitions and mechanisms to implement this law in the future. The main questions are: How does Cambodia define cybersecurity under this draft law? Is this law proportionate and address cybersecurity itself?

Purpose, Objective and Scope

According to the Council of Ministers spokesman Ek Tha, the draft of the Cybercrime Law is designed to *"prevent any ill-willed people or bad-mood people from spreading false information and groundless information"*.[65] Article 1 of the draft law states that, *"This law has a purpose to determine education, prevention measures and combat all kind of offenses commit with computer systems"*.[66] Moreover, this law has the objective to *"ensure the implementation of law, anti-cybercrime and combating all kinds of offenses commit with computer systems"* and to

60 The Law on Telecommunications, Art. 66.

61 Licadho Cambodia's Law on Telecommunications 2016, 2.

62 The Law on Telecommunications, Art. 76.

63 Sarah M. Bernstein, Police Failure to preserve Evidence and Erosion of the Due Process Right to a Fair Trial, (U.S., Journal of Criminal Law & Criminology, 80 (4), 1990), 1274. Available at: http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=6649&context=jclc

64 Appazov, Legal Aspects of Cybersecurity, 23-24.

65 Kevin Ponniah, "Cyber bill raises concerns", (The Phnom Penh Post 09.04.2014). Available at: http://www.phnompenhpost.com/national/cyber-bill-raises-concerns

66 Cybercrime Law, Draft V.1, Art.1.

"ensure safety and prevent all [illegitimate] interest in using and developing technology".[67]

Structure

The Draft Cybercrime Law is divided into six main chapters. Chapter 1 is the general provision that covers the purpose, objective, scope, terms and definition of this law. Chapter 2 covers the establishment of a National Anti-Cybercrime Committee (NACC), its composition, duties, officials, budget and other details. Chapter 3 provides the procedures of dealing with cybercrime offences including investigation powers. Chapter 4 covers specific types of offences such as illegal access, data espionage, illegal interception, and data interference. Chapter 5 covers the topics of mutual legal assistance, international cooperation and extradition. Chapter 6 is the final provision.

It should be noted that the NACC will be chaired by the prime minister, with the deputy prime minister also acting as deputy chairman, and include five secretaries of state from the Ministry of Interior, the Ministry of Foreign Affairs, the Ministry of Information, the Ministry of Post and Telecommunications and the Ministry of Justice. There will be one general commissioner from the National Police who will be included as member. Other members are representatives from Anti-terrorism, Council of Justice, Ecosoc, Chamber of Commerce and NiDA.[68] The NACC will have the duty to create strategies, action plans and related programs in securing the cyber and information grid. It will advise and recommend courses of action to the General Secretariat of the National Anti-Cybercrime Committee, supervise workflows and implementations of the General Secretariat. Moreover, it will also issue findings and appropriate recommendations for ministries and departments to ensure the security of the cyber and information grid of the government, provides cyber and information grid security reports of the nation to the government and perform other duties directed by the government.[69]

Offenses

Compared to the Cambodian Criminal Code 2009, new and more specific cyber offences are introduced in the draft law on Cybercrime such as *illegal access, data espionage, illegal interception, unauthorized data transfer, and system interference.*[70] The unauthorized access to a computer system, interception

made by technical means, alteration, deletion or deterioration of computer data shall carry sentences of six months to fifteen years imprisonment and fines between one million and twenty four million Riels.[71]

Article 23 of the draft law introduces the offence of "illegal interception" of computer data. Interestingly, it resembles Article 3 of the Convention on Cybercrime, the international treaty adopted by the Council of Europe. However, unlike the European version, the Cambodian draft law fails to provide discretion of the criminalization based on *"dishonest intent"* or *"in relation to a computer system that is connected to another computer system".*[72]

The same issues remain in other offences of

67 Ibid., Art. 2.

68 Ibid., Art.7

69 Ibid., Art.7.

70 Cybercrime Law, Draft V.1, Art 21-26.

71 Ibid.

72 Convention on Cybercrime, ETS 185, 23.11.2001, Art. 3.

the draft law. The offences are defined in very broad terms and fail to make reference to malicious or fraudulent intent, considering that honest mistakes over the internet are likely to be caught and penalized.[73] British charity 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*".[74] Cambodia's draft Cybercrime Law falls well below international standards on the rights for freedom of expression, information and privacy.[75]

Investigating Cybercrimes and Collecting Digital Evidence

Gathering evidence is one of the main challenges in fighting cybercrime.[76] Cybercrime is different from physical crime in terms of motives, intent and outcomes, but especially also in terms of evidence. As evidence arises out of an electronic discovery process, it is very important for the investigator to understand the capabilities of the cybercriminal suspects.[77] Digital evidence can be destroyed during the discovery process, as it is typically made of binary data inscribed on a mass storage device and can contain executable code objects, images or other encrypted electronic content. Therefore, only computer forensic experts should conduct such investigations.[78]

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".*[79] The law requires that service providers make user data available to the competent authorities under confidentiality conditions.[80] Prosecutors are given significant powers to order the preservation of computer data or traffic data under the draft law, which may cause concern if a prosecutor is subject to political influence or lacks the necessary independence to balance the different interests involved, especially the protection of the right to privacy.[81]

Therefore, it would be necessary to use the "Principle of Proportionality" and "Reasonable data management" during a cybercrime investigation, in order to guarantee that rights and safety are considered at equally.[82]

While it is extremely important for a cybercrime investigator to understand the purposes, personalities and behaviors of the cybercriminals, and to use different analytical techniques with different types of digital evidence for a more effective result,[83] policymakers and citizens should jointly discuss whether, in order to balance security and the right to privacy, 'identity' and 'behavior' should be regulated separately.[84] There could be real

73 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

74 Ibid.

75 Ibid.

76 Gruodyte, Investigating Cybercrimes, 241.

77 Okechukwu Wori, Computer crimes: Factors of Cybercriminal Activities, (Switzerland, Int'l J. IJACSIT ISSN 2320-0235, Cloud Publications, 3 (1), 2014), 53-54.

78 Ibid

79 Cybercrime Law, Draft V.1, Art. 17.

80 Ibid.

81 Article 19, Cambodia: Secret Draft Cybercrime Law.

82 Agnes Kasper, Eneli Laurits, Challenges in Collecting Digital Evidence: A Legal Perspective, Kerikmäe, T. Rull, A. (Eds.), The Future of Law and eTechnologies, (Switzerland, Springer, 2016), 201.

83 Debra Littlejohn Shinder, Michael Cross, Scense of the Cybercrime, (United State, Elsevier, 2008), 118.

84 Chris C. Demchak, Kurt D. Frenstermacher, Balancing Security and Privacy in the 21st Century, (Switzerland,

additional dangers to citizens if extensive information on both 'identity' and 'behavior' is collected, as this data could be also exposed to malicious actors. Thus it would seem better for data collection efforts to focus on 'behavior' only.[85]

Cybersecurity Laws in China, Japan and Singapore

Governance, economy and society are important factors to consider when legislating cyberspace.

In 2013 a United Nations Working Group of Government Experts concluded that the UN Charter and international law are fully applicable to the state behavior in cyberspace, which has also been adopted by NATO countries.[86] However, China does not fully agree that international law should have jurisdiction on the national cyberspace. China holds the view that each state should have the right to set its own rules. With a strong belief in "cyber sovereignty", China, together with Russia and some other Asian countries, introduced its alternative position through the Shanghai Cooperation Organization (SCO) in the UN General Assembly.[87] China has been actively participating in high level dialogues and has signed several agreements for the purpose of protecting and improving cybersecurity. Yet, several of its national policies give extensive jurisdiction to the Chinese government to control cyberspace in areas of society and economy as well. The new Chinese Cybersecurity Law continues to enforce self-censorship on content and control over personal and business data. Therefore, the principle of international law that covers cyberspace and fundamental human rights is not being fulfilled in China.

In Japan, although freedom of expression, access to information and the right to privacy are arguably still practiced in a limited way, the country is a good role model in the fight against cybersecurity issues, notably in terms of public-private partnerships and effective international cooperation.

Japan launched its new Cybersecurity Strategy Plan in September 2015. It highlights the role of industry and civil society in maintaining Japan's cybersecurity and the centrality of two-way information sharing. The Cybersecurity Strategic Headquarters functions as the command and control body to promote the plan, and the National Information Security Center (NISC) takes the lead in promoting cybersecurity policies set forth in this strategy.

Interestingly, the NISC is allowed to monitor government-affiliated agencies for the first time.[88] The Japanese government adopted the Cybersecurity Basic Act in November 2014 and amended it in April 2016 in response to the Japan Pension Service hack to give the NICS new powers to monitor and audit the security of entities created by direct government approval or laws.[89]

Japan is also a member of the Global Forum on Cyber Expertise and has been a member of two UNGGEs. The country is actively involved

Intelligence and Security Informatics (ISI), 2004), 327.

85 Ibid, 328.

86 Mikk Raud, China and Cyber: Attitudes, Strategies, Organization, (Tallinn, CCD COE Publications, 2016), 7. Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016.pdf

87 Ibid.

88 The Government of Japan, Cybersecurity Strategy, (Japan, NISC, 2015), 52. Available at: https://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf

89 Cyber Maturity in the Asia-Pacific Region, 43.

in high level international political dialogues and has a strong Asia-Pacific engagement program, working closely with ASEAN countries. JPCERT/CC, Japan's national Computer Emergency Response Team Coordination Center (CERT/CC), was established in 1996 in order to work with government agencies, critical infrastructure operators, security vendors and civil society. It actively promotes collaboration and monitoring across the Asia-Pacific and enhances the sharing of threat information. It is also undertakes extensive capacity building across and outside the Asia-Pacific, and works with global partners on a Cyber Green Initiative, an effort to improve the general internet ecosystem health.[90]

Singapore's government created a new Cybersecurity Strategy Plan 2018 with the aim to establish a resilient cyber environment based on a strong infrastructure, a safer cyberspace and a vibrant ecosystem with international partnerships.[91] Moreover, the Communication and Information Minister has promised to spend up to 10% of Singapore's IT budget on boosting cybersecurity.[92] In addition to this, an existing Computer Misuse and Cybersecurity Act was amended in April 2017, setting new standards for incident reporting, audits and risk assessment, such as dealing with personal information obtained via cybercrimes (e.g. hacked credit card details).[93] Singapore also engages in a strong international program to establish itself as one of the region's leading central government cybersecurity bodies. It has signed several MoUs with other ministries inside and outside the region. Singapore is active in forums such as the East Asia Summit, ASEAN cybercrime meetings and the ASEAN Regional Forum. The SingCERT, like the one in Japan, was established in 1997 and works to detect, resolve and prevent security-related incidents on the internet affecting Singaporean companies and users. SingCERT signed an MoU with India's CERT-In to enable information sharing and incident response collaboration.[94]

Conclusion and Recommendations

Classifying different aspects of cybersecurity into manageable categories facilitates the development of national and international law governing the rights and duties of individuals and nations with respect to each category of activity. Cyberattacks can be categorized into three general categories: cybercrime, cyberterrorism and cyberwarfare. Cyberespionage is another separate concern connected to either state intelligence or hacktivism. This separation helps to address the shortcomings of present national and international legal frameworks in a more effective manner.[95]

Cyberattacks largely defy the simple categorization of activity defined by existing laws, making it difficult for countries to apply the traditional definitions of crime, terrorism, warfare or espionage as understood under existing law. Traditional classifications break due to the aforementioned asymmetric na-

90 Ibid.

91 Cyber Security Agency of Singapore, Singapore's Cybersecurity Strategy, (Tallinn, CCDCOE, 2016). Available at: https://ccdcoe.org/sites/default/files/documents/SingaporeCybersecurityStrategy.pdf

92 Global Cybersecurity Index & Cyberwellness Profiles 2015, 70.

93 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

94 Cyber Maturity in the Asia-Pacific Region, 70.

95 Artur Appazov, Legal Aspects of Cybersecurity, (Denmark, University of Copenhagen, 2014), 14-15. Available at: http://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf

ture of network communication.

The legal and legislative analyses of cybersecurity issues must distinguish not only between different cyber-threat actors such as nations-states, terrorist, criminals, and malicious hackers, but also between the different targets of cyberthreats. Such targets include critical infrastructure, which could lead to loss of life or significant damage to the economy, and intellectual property, which could affect a country's long-term competitiveness.[96]

Cambodia has made steady developments in the area of cyber policy and security. In order to strengthen the area of national telecommunication legislation, its 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 bilateral engagement with Japan, South Korea and the United States. The engagement is focused on technical capacity building, and legislative and policy development assistance.[97]

However, the existing legislation of Cambodia does not address cybersecurity well enough. Current criminal law provides a broad perspective of crime related to telecommunications without clear definitions of the types of crime. The offence of infringement on the secrecy of the correspondence and telecommunication, and offences in information technology sector are being used to address cybercrime in Cambodia during the absence of a specific Law on Cybercrime. Other legislations such as the Press Law and Ministry Prakas do not describe cybercrime appropriately. There are a number of good recommendations proposed by stakeholders and international partners that should be taken into consideration in order to improve cyber wellness in Cambodia.

The current draft law on Cybercrime needs to address cybersecurity issues based on specific classifications and characteristics of crime. The terms and definitions used in the draft law should be clear and accurate in order to prevent broad and vague interpretations or confusion among authorities, judicial bodies, law practitioners and stakeholders implementing the law. The law should at least reach the minimum international cybersecurity standard norms and practices.

For instance, the collection of digital evidence during the investigation should be handled by professional data forensics because digital data is fragile and can break easily. Moreover applying the principle of proportionality and reasonable data management during cybercrime investigation is necessary to avoid data and privacy violations.

Special training and capacity building conducted by experts is very important for effective cybercrime investigation, especially for law enforcement officials and others who work in government institutions.

Cambodia doesn't need to establish an NACC, unless it is to become an independent body overseeing cybersecurity practices in terms of technical and general implementation.

The Cambodian government should also promote open discussion between government, public, private, civil societies and international partners when adopting any national legisla-

96 Ibid.

97 Ibid., 28.

tions and policies, especially on ICTs and cybersecurity matters, because it involves multiple different aspects that are linked with long term development and competitiveness at local and international level.

In addition, the current legal framework concerning cybersecurity, such as the Criminal Code 2009, Press Law, Telecommunication Law 2015 and other relevant regulations, should be amended in terms of the provisions concerning the interpretation of crime itself and authority power, including those that provide unnecessary restriction and violations of fundamental rights. Cyber awareness programs should be implemented at all levels in order to help citizens become more aware of the potential risks and threats on the internet. The government should integrate such cyber awareness programs in school curricula because large numbers of young Cambodian are increasingly using the internet for various purposes without knowing about its dangers.

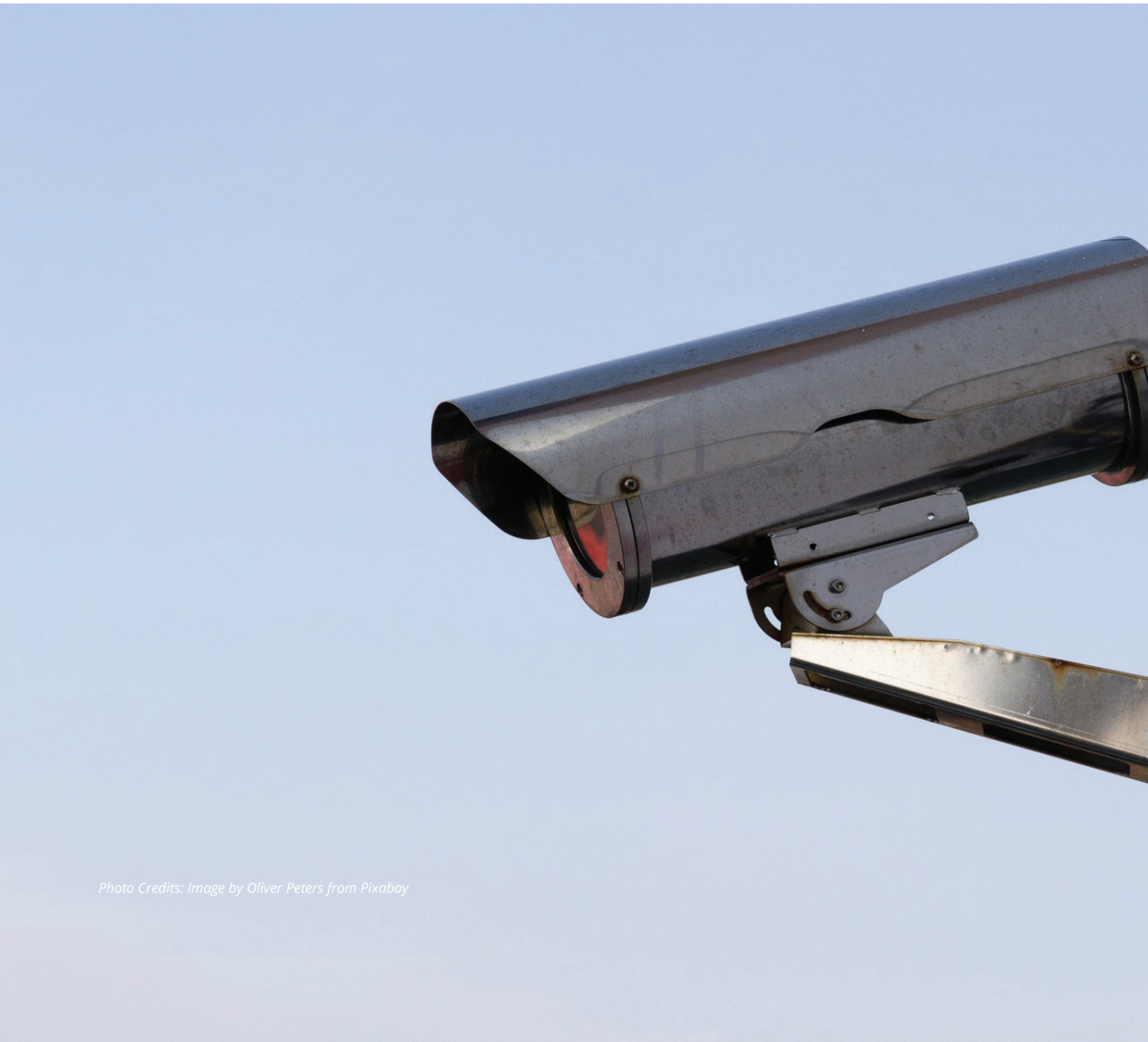
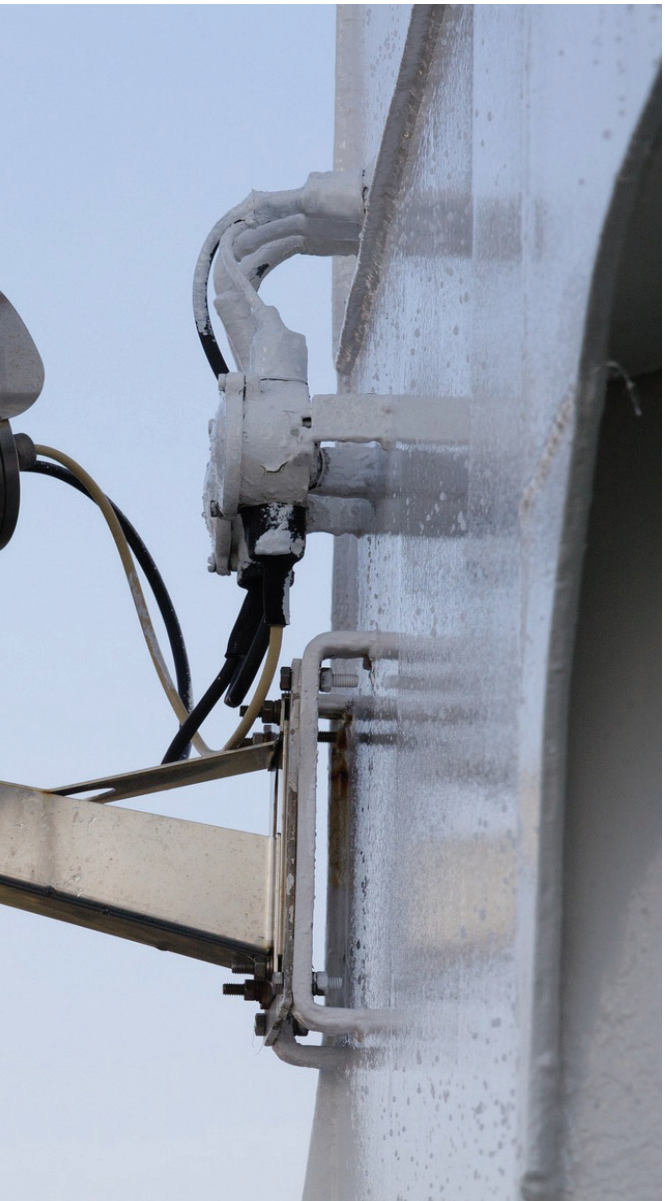


Photo Credits: Image by Oliver Peters from Pixabay

Last but not least, the government should increase its regional and international cooperation and partnerships in the field of cybersecurity. Cybercrime law will certainly play a major role in addressing cybersecurity in Cambodia, but it has to match international cybersecurity standards and comply with Cambodia's legal oblations at all levels.

One major positive step would be for Cambodia to consider signing and ratifying the Convention on Cybercrime, also known as the Budapest Convention, the first international treaty seeking to address internet and computer crime by harmonizing different national laws, improving investigation techniques, and increasing cooperation among nations.



Even though the Convention on Cybercrime was adopted by the Committee of Ministers of the Council of Europe in 2001, as of March 2019, 63 states have already ratified the convention, including the United States, Canada, Australia, Japan, Philippines and Sri Lanka.

An effective, robust and balanced cybercrime law is important for Cambodia's political, social and economic development, and therefore it will be in its best interests it to integrate best practices and effective measures from around the world.