Open Development Cambodia Organization

CYBERSECURITY IN CAMBODIA: CURRENT DEVELOPMENTS AND CHALLENGES AHEAD

March 2023

ABSTRACT

Cambodia's digitalisation process started two decades ago and has rapidly transformed its social, political, and economic spheres with a several new opportunities to develop the country. However, the popularity of the internet, digital tools, and digital media has also brough new challenges, namely security issues in the digital sphere. To address the problems that have emerged in the digital era, the Royal Government of Cambodia has put in place new legal measures to address cybercrime and make the digital space safer. Nonetheless, there is still room for improvement. This article examines the key laws and legal measures adopted by the Cambodia government to assess the progress that has been made in the country on cybersecurity. While substantial progress has been made in the last decade, this article suggests that there is still room for improvement. The government of Cambodia should work closely with a range of civil society stakeholders to make the drafting of cybersecurity laws a co-creation process that considers the views and needs of as many agents as possible. Only then, cybersecurity laws will be sustainable.

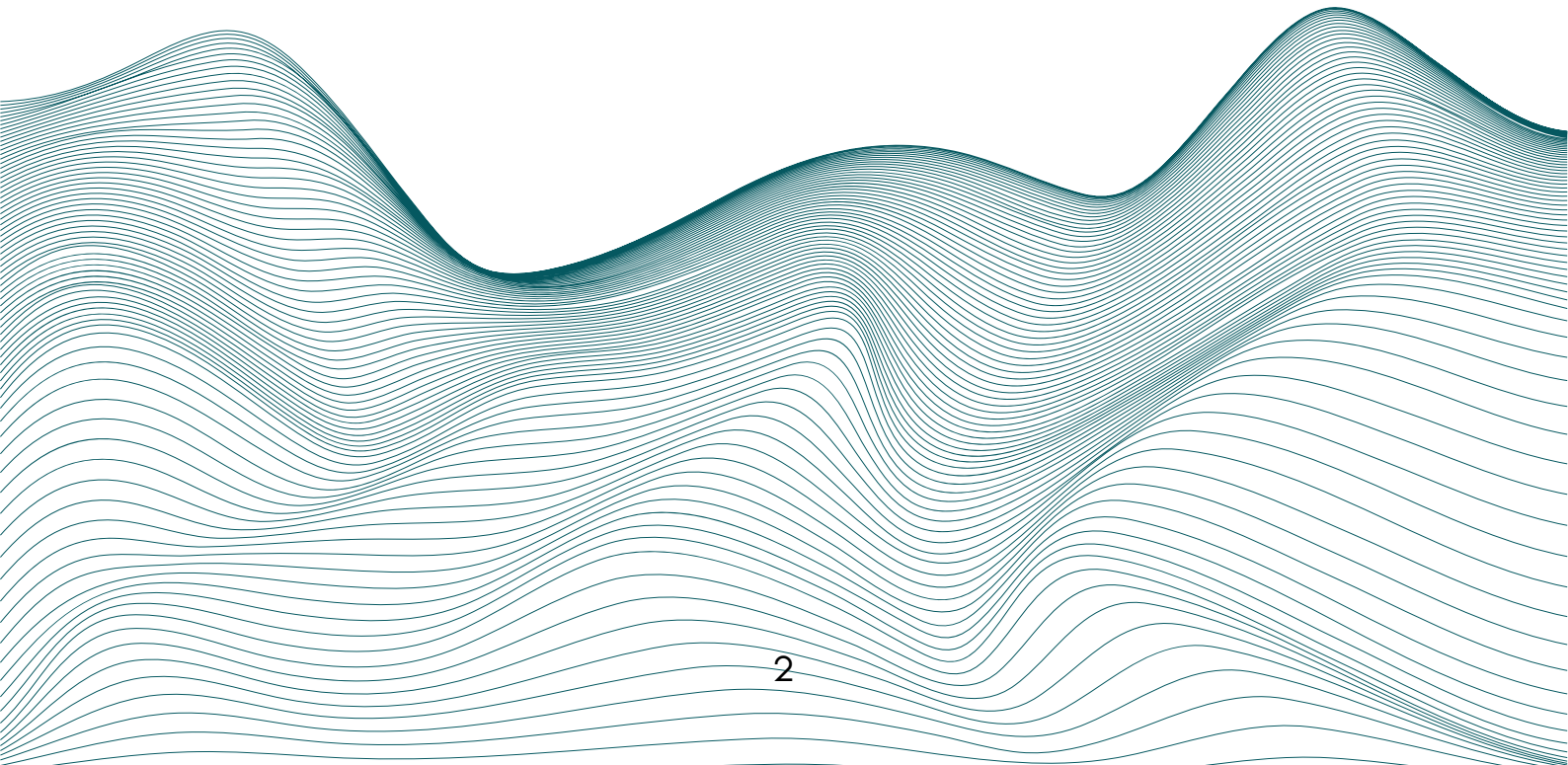

TABLE OF CONTENTS

1. CONTEXT

Cambodia is no exception to the global trend of digitalisation, making the internet a core element of its social, economic, and political systems. The country has witnessed how the internet and smartphones became extremely in the country since the late 2000s and, especially, since the early 2010s. The rapid development of the digital sphere has come with a range of positive outcomes like people's permanent access to a variety of news sources from domestic and international outlets. In this context, challenges like cybercrime arose. This is a two-fold problem. On the one hand, cybercrime is a challenge since it refers to a set of actions that take place in the digital sphere, which are, in nature, illegal. On the other hand, the legal system was not ready to cope with the rapid development of the digital sphere, comprising a new range of digital tools and media. As a response, the Cambodian government has created - or drafted, in some cases - new legislation to address the new digital challenges of the internet era, thus contributing to the development of the cybersphere with laws to address cybercrime. This article examines such progress with an overview of five legal previsions and also points out that, even if significant progress has been achieve to address cybercrime, new digital laws must be more specific considering the needs of a range of agents and must be drafted and development considering the views of all relevant stakeholders to increase its sustainability.

1.1. Cambodia's digitalisation

Cambodia has recently undergone a rapid digital transformation. One of the key factors driving the digitalisation of Cambodia is the increased access to the internet. According to a Kemp (2023), internet penetration in Cambodia stood at 67.5 % (11.37 million) users in early 2023. Between 2022 and 2023, internet users in the country increased by 6.7% or 714,000. Also in early 2023, Cambodia had a total of 22.16 million active cellular mobile connections. This is equivalent to 131.5% of the total population in the country.

More specifically, the popularisation of social networking sites (SNS) increased rapidly. As of January 2023, Cambodia had 10.95 million social media users, or 65.0% of the total population. Facebook emerged and consolidated as the most popular social media platform in the country. According to Meta,

Facebook had 10.45 million users in the country in early 2023. Regardless of its dominance in the landscape of social media platforms in the country, data also shows that Facebook's potential ad reach in Cambodia decreased by almost 10% between 2022 and 2023. Facebook's decline in number of users is partially explained by the emergence of other SNS and the new functions they offer. In early 2023, Instagram had 1.75 million users in Cambodia, and, like Facebook, its reach decreased by 14.6% or 300,000 users between 2022 and 2023. TikTok had just over 7 million users aged eighteen or above in early 2023.

Contextualising the development of the digital sphere is essential because it allows us to explain a range of impacts in the social, political, and economic spheres in the country. The surge of the internet and a range of SNS had a profound impact on Cambodia's society. Socially, the digital sphere allowed citizens not only to post about their daily lives, but also to gain access to a wide range of news outlets, both from Cambodia and overseas, and blogs by activists posting about several matters affecting their country and towns (Phong et al., 2016). The internet also revolutionised Cambodia's political scene with citizens becoming increasingly aware of the latest political developments, the role of opposition parties and overall, making the government more accountable by demanding better governance in terms of public services and being able to monitor progress (Vong and Hok, 2018). From a business perspective, the digital sphere opened the door to several opportunities for consolidated businesses and also entrepreneurs who adopted the internet as a vital mechanism to promote their business and reach out to potential new consumers of their products (ODCa, n.d).

Given the internets' capacity to shape the public and private spheres, the Royal Government of Cambodia (RGC) started implementing new policies to increase access to the internet and promote the development of the digital government and economic sector. The RGC has considered this digitalisation essential to the country since its inception. Elaborated by the Ministry of Telecommunications and Posts, the "Cambodia Digital Economy and Society Policy Framework 2021-2035 (MPTC, 2022)was formulated with three main pillars: digital citizens, digital government and digital business, among which building digital government must begin first to promote the adoption and use digital technology, and digital transformation in the economy and society as a

whole". Establishing a digital strategy has allowed the country to improve on many fronts with the help of digital tools and media, including improved education, increased economic growth, and enhanced communication. This growth has been facilitated by government policies that aim to improve internet infrastructure and reduce the cost of data plans (Property Report, 2021). The government has also launched initiatives to provide digital skills training to students and entrepreneurs, further driving the adoption of digital technology in the country (CADT, 2022).

The digitalisation of Cambodia has had a positive impact on the country's education system (UNESCO, 2020). Many schools and universities have adopted online learning platforms, allowing students to access educational resources from anywhere with an internet connection. This has been particularly important during the COVID-19 pandemic, which has forced many students to learn from home. Digitalisation has also opened up new opportunities for distance learning, enabling students in remote areas to access quality education. In addition to improving education, the digitalisation of Cambodia has also boosted economic growth. The development of the digital economy has created new job opportunities and enabled small businesses to reach new customers through e-commerce platforms. The government has launched several initiatives to support the growth of the digital economy, including the establishment of a start-up accelerator and the creation of tax incentives for tech companies.

Overall, the internet has become an indispensable tool for the Cambodian society, contributing to the development of the country on many fronts. Nonetheless, it must be noted that the development of the digital sphere has also supposed several challenges. Issues concerning cybersecurity is one of the clearest examples, which is addressed in the next section.

1.2. Cybersecurity: a key challenge in the digital age

Cybersecurity is a growing concern worldwide, and Cambodia is no exception. As the country becomes more digitalised, the risk of cyber-attacks increases, and protecting sensitive information from unauthorised access is crucial. Cybersecurity is a significant challenge for Cambodia, and there are several reasons why this is the case.

One of the main challenges of cybersecurity in Cambodia is the lack of awareness among the general population (Corrado and Sakal, 2021). Many people in Cambodia have limited knowledge about the risks of using the internet and are not familiar with best practices for online safety. This lack of awareness makes them more vulnerable to cyber threats such as phishing attacks, malware, and social engineering.

Another challenge is the lack of technical expertise in cybersecurity (Flynn, 2019). There is a shortage of skilled cybersecurity professionals in Cambodia, which makes it difficult for organizations to implement robust security measures. This shortage of cybersecurity experts is compounded by the lack of investment in training and education in the field.

In addition – and regardless of the efforts made by the RGC – the Cambodian legal framework for cybersecurity is still in its early stages of development. There is a lack of comprehensive legislation regulating cybersecurity and data protection. As a result, there is no clear legal framework to deal with cybercrime, and there are no standard procedures for reporting cyber incidents. Moreover, the lack of effective regulation and enforcement of cybersecurity creates a challenging environment for businesses operating in Cambodia. The absence of regulatory requirements and standards means that businesses are left to develop their cybersecurity policies and practices, which can result in a lack of consistency and effectiveness.

Cambodia's political situation is another factor that complicates the country's cybersecurity environment. Cambodia has faced accusations of using cyber espionage to monitor opposition figures, journalists, and civil society groups. This creates a challenging environment for businesses and individuals to operate in, and it reinforces the need for robust cybersecurity measures.

Therefore, cybersecurity is a significant challenge for Cambodia, and there is a need for greater awareness, investment in education and training, and regulatory frameworks to improve cybersecurity practices. With the right policies and practices, Cambodia can mitigate the risks of cyber threats and protect its citizens and businesses from the negative consequences of cybercrime. Below, the key reasons why cybersecurity laws are needed are streamlined.

1.3. The urgency for more cybersecurity laws

Cybersecurity has become an essential element in the legal frameworks of countries worldwide since government institutions and systems hold a vast amount of sensitive information, and any breach of this information can have serious consequences affecting the economy or national security of countries. Therefore, government institutions have a responsibility to protect the personal information of citizens, safeguard national security secrets, and ensure the smooth functioning of government operations.

Cybersecurity is essential to protect national security (Tunggal, 2023). Government institutions and systems hold a wealth of information related to national security, including military secrets, classified documents, and intelligence data. A cyber-attack on government systems could compromise this sensitive information, putting national security at risk. Additionally, cybersecurity has become necessary to ensure government operations. Cyber-attacks on government systems can cause disruptions to government operations, such as the inability to process payments or provide essential services. Ensuring the smooth functioning of government operations is essential to maintaining the stability of the country.

As mentioned earlier, the development of the digital sphere and internet infrastructure has resulted in a range of positive developments and also many challenges, like threats against public institutions that can potentially affect lager segments of the population or society. In such a context, government institutions have a responsibility to address cyber threats that could impact the wider society. This includes developing policies and strategies to prevent cyber-attacks, identifying potential threats, and responding quickly to any cyber incidents. Fraud is another more specific examples. Cybersecurity is essential for preventing fraud, particularly in government financial systems. Hackers may try to gain access to government financial systems to steal money or manipulate financial data, and effective cybersecurity measures are necessary to prevent such attacks.

Last but not least, cybersecurity is needed to maintain public trust, an essential element widely studies by political scientists (Levi and Stoker, 2020). When people share their personal information with government institutions, they

expect that their data will be kept secure. Any breach of this trust could damage public confidence in government institutions and undermine the legitimacy of government activities.

As the examples above show, cybersecurity is crucial for government institutions and systems to protect sensitive information, maintain public trust, ensure government operations, prevent fraud, and address cyber threats. Developing of a strong cybersecurity strategy is nowadays more necessary than ever before given the accelerated digitalisation and the increasingly sophistication of cyberthreats (ASEAN, 2022), which have become cross-boundary problems requiring regional cooperation. To confront these threats and promote cooperation among Southeast Asian nations, ASEAN developed the ASEAN Cybersecurity Cooperation Strategy 2021-2015 (ibid). Its five pillars aim at (1) advancing cyber readiness cooperation, (2) strengthening regional cyber policy coordination, (3) enhancing trust in cyberspace, (4) [creating] regional capacity building, and (5) [promoting] international cooperation. Therefore, Cambodia's efforts to strengthen its cybersecurity is not only necessary to improve safety in the Cambodian digital sphere. It is also a positive contribution to the collective efforts made by ASEAN to address global cybersecurity issues.

By investing in effective cybersecurity measures, government institutions can help to mitigate the risks of cyber-attacks and ensure the stability and security of the country. The rest of this document evaluates Cambodia's cybersecurity developments to show that although Cambodia has made significant progress in the development of cybersecurity laws, legal provisions need to be further developed with the inputs from various civil society agents so the new laws are rights-friendly, inclusive and, overall, contribute more to the country's sustainable development.

2. CYBERSECURITY LEGISLATION

Compared to other types of laws, cybercrime needs further legal development. Nonetheless, it is not inexistent in the domestic legal framework (Corrado and Sakal, 2021). Computer-related offences were already contemplated in the Criminal Code (2009) in Articles 317-20 and 427-432. However, these provisions are rather vague and, given the rapid development of the digital space in the country, have fallen behind.

Accordingly, Cambodia has enacted several laws and regulations related to cybersecurity in the last decade to protect its citizens, businesses, and critical infrastructure from cyber threats. Overall, they represent a meaningful progress towards the creation and consolidation the regulatory framework of the digital sphere in Cambodia. Despite of the progress that had been made with the creation of new legal provisions, this section also shows that the legal provisions created to address the challenges of the digital sphere need to be further developed so they become more inclusive while considering the views and needs of all relevant civil society stakeholders. Below, five cybercrime laws are examined: Law on the Management of the Nation's Telecommunications Sector; Law on Cybercrime; Sub-decree on the Establishment of the National Authority for Combating Cybercrime; Prakas on Cybersecurity Management; and the Sub-decree on the Establishment of the National Cybersecurity Committee. These five laws are examined by looking at the advancements that these have supposed. Then, their associated challenges are presented. Together, this allows to analyse what the provisions regarding cybercrime have in common and flag how they can be strengthened in section 3.

2.1. The Law on the Management of the Nation's Telecommunications Sector

The Law on the Management of the Nation's Telecommunications Sector (WTO, n.d) was passed in 2015. The law governs the management and regulation of the country's telecommunications sector, including issues related to cybersecurity. This law presents several key provisions, like the establishment of the Telecommunications Regulator of Cambodia (TRC) as the regulatory body responsible for overseeing the telecommunications sector in Cambodia. It also regulates licensing requirements. The law sets out the licensing requirements for telecommunications service providers in Cambodia, including the need to

obtain a license from the TRC before providing telecommunications services. The spectrum management is also affected by the Law on the Management of the Nation's Telecommunications Sector. The law regulates the allocation and management of radio frequencies and other forms of spectrum used for telecommunications services. This law also concerns the universal service obligation. It establishes a universal service obligation for telecommunications service providers, requiring them to provide affordable and accessible telecommunications services to all citizens of Cambodia, regardless of their location or economic status. Last but not least, it also addresses matters of cybersecurity itself with provisions related to cybersecurity, requiring telecommunications service providers to implement appropriate security measures to protect their networks and systems from cyber threats. Overall, the Law on the Management of the Nation's Telecommunications Sector aims to promote the development of a competitive and innovative telecommunications sector in Cambodia, while ensuring that the sector operates in a fair, transparent, and secure manner.

While the Law on the Management of the Nation's Telecommunications Sector in Cambodia has been praised for its efforts to promote the development of a competitive and innovative telecommunications sector, there have been some criticisms of the law. Critics (HRW, 2021) have argued that the law is not sufficiently clear or specific in its provisions, particularly when it comes to issues related to cybersecurity. This lack of clarity could potentially lead to inconsistencies in the implementation and enforcement of the law (Seng, 2022). Another concern associated with this law is limited competition. Some observers have raised concerns that the law does not do enough to promote competition in the telecommunications sector. There are concerns that the licensing requirements and other regulations could make it difficult for new players to enter the market. Similarly, limited consumer protection has also raised concerns since the law does not do enough to protect the rights and interests of consumers. For example, some critics argue that the law does not adequately address issues such as quality of service, pricing, and accessibility. Finally, lack of enforcement is another key point to look at. Critics have also noted that the law may not be effectively enforced, particularly in rural and remote areas of the country where access to telecommunications services is limited.

Overall, while the Law on the Management of the Nation's Telecommunications Sector represents an important step forward in the development of Cambodia's telecommunications sector, there are concerns that the law may need to be revised and improved to address these and other criticisms.

2.2. The Law on Cybercrime

The Law on Cybercrime (ODCb, n.d) in Cambodia was drafted in 2018 to address the growing threat of cybercrime in the country. The law criminalises a range of cyber activities and provides a legal framework for investigating and prosecuting cybercrime cases. This law is important because it conceptualises key concepts. Cybercrime is defined as any criminal offense committed using information and communication technology (ICT) systems, including hacking, phishing, identity theft, and distribution of malware. Accordingly, it also establishes its related penalties. The law imposes penalties for cybercrime offenses, ranging from fines to imprisonment. For example, the maximum penalty for unauthorised access to a computer system is three years in prison and a fine of up to 10 million riel (US$2,500) (Narin, 2022).

If the law is enacted, Cambodian courts can exercise extraterritorial jurisdiction over cybercrime offenses committed outside of Cambodia if the offense has an impact on Cambodia or involves a Cambodian national (Kelliher, 2023). If necessary, the law provides for the investigation and prosecution of cybercrime offenses by the police and the courts. It also establishes procedures for the collection and admissibility of electronic evidence in cybercrime cases. The law includes provisions to protect the rights of victims and witnesses of cybercrime, including the right to privacy, confidentiality, and protection from retaliation.

While the Law on Cybercrime in Cambodia is an important step forward in addressing cybercrime in the country, there are some critiques of the law. The law has been criticised due to being too vague and overly broad, leaving room for interpretation and potential abuse. This could lead to the targeting of political dissidents, human rights activists, and other individuals who express dissenting opinions online. Lack of due process has also been flagged (Ibid.). Some observers have raised concerns that the law does not provide adequate due process protections for individuals accused of cybercrime offenses. For example, the law allows for pre-trial detention of up to six months, which some

argue is excessive. Its lack of clarity on electronic evidence is another issue showing that there is still room for improvement in Cambodia's cybersecurity legal framework. There are concerns that the law does not provide clear guidelines on the admissibility and reliability of electronic evidence in cybercrime cases. This could lead to inconsistencies in the application of the law and undermine the fairness of trials. Finally, its potential impact on freedom of expression should not be overlooked (IPI, 2020). There are concerns that the law could be used to stifle free speech and dissenting opinions, particularly given the broad definition of cybercrime offenses. Some critics argue that the law could be used to target journalists, human rights activists, and opposition figures who use online platforms to express their views.

The cases above show meaningful positive steps towards the regulation of the digital space. Nonetheless, there are concerns that the law may need to be revised and improved to address these and other criticisms that must not be overlooked. It is important to strike a balance between protecting citizens from cyber threats and safeguarding their fundamental rights and freedoms.

2.3. The Sub-decree on the Establishment of the National Authority for Combating Cybercrime

The Sub-decree (Article19, n.d) was issued in 2014 to strengthen the country's efforts to combat cybercrime. It outlines the functions and responsibilities of the National Authority for Combating Cybercrime (NACC) and provides a legal framework for its operations. Here are some of the key provisions of the sub-decree. The NACC as the national authority responsible for combating cybercrime in Cambodia. It also takes charge for developing policies, strategies, and plans for preventing and combating cybercrime, as well as coordinating and cooperating with other government agencies, civil society organizations, and international partners. The composition of the NACC includes representatives from various government agencies, including the Ministry of Interior, the Ministry of Post and Telecommunications, the Ministry of Justice, and the Ministry of Information.

The NACC has power conduct investigations, collect, and analyse cybercrime-related data, provide technical assistance and capacity building to other agencies and stakeholders, and promoting public awareness and education on

cybercrime issues. Additionally, the sub-decree provides for the allocation of funding and resources for the operation of the NACC, including the establishment of a Cybercrime Investigation Unit within the National Police.

Overall, the Sub-decree on the Establishment of the National Authority for Combating Cybercrime in Cambodia is meaningful since it contemplates the establishment of a dedicated national authority, provides a legal framework for its operations, and helps to ensure that cybercrime is taken seriously so that the government can create the tools and resources it needs to effectively address this growing threat. Still, the sub-decree has not been immune to criticism. Critics have raised concerns that the NACC is not transparent in its operations, decision-making processes, and activities. This could lead to questions about the legitimacy and accountability of the NACC and its activities. The Sub-decree has also been criticised due to its lack of independence from the government, which could limit its ability to effectively investigate and prosecute cases of cybercrime. This could also lead to questions about the impartiality and fairness of the NACC.

Other concerns touched upon its lack of clarity on jurisdiction since the sub-decree does not provide clear guidelines on the NACC's jurisdiction and scope of authority, which could lead to inconsistencies in the application of the law and undermine the fairness of trials. Like the Law on Cybercrime, the Sub-decree also has the potential to affect freedom of expression since it could be used to stifle free speech and dissenting opinions, particularly given the broad definition of cybercrime offenses. Some critics argue that the sub-decree could be used to target journalists, human rights activists, and opposition figures who use online platforms to express their views.

Therefore, the overall evaluation of the Sub-decree is in line with the two previous legal provisions. While it can be read as a positive development for the country, there is still room for improvement to strengthen it to address its criticisms. This way, its shortcomings will not outweigh its potential to make the digital sphere a safer place.

2.4. The Prakas on Cybersecurity Management

The Prakas on Cybersecurity Management was issued by the Ministry of Posts and Telecommunications in Cambodia in 2018. It is aimed at establishing guidelines and standards for cybersecurity management in the country and sets out several provisions relating to cybersecurity practices and procedures like the establishment of a cybersecurity management framework, which outlines the roles and responsibilities of various stakeholders, including government agencies, private sector entities, and individuals. The Prakas requires that organisations conduct regular cybersecurity risk assessments to identify potential threats and vulnerabilities, and to develop appropriate risk mitigation strategies. Additionally, it also requires that organisations develop and maintain an incident response plan to ensure that they are prepared to respond effectively to cybersecurity incidents. Organisations must also provide regular cybersecurity awareness and training programs to their employees, to raise awareness of potential threats and to ensure that employees are equipped with the necessary skills and knowledge to prevent and respond to cybersecurity incidents. Cybersecurity incidents to the relevant authorities must be reported - guidelines for reporting and information sharing in the event of a cybersecurity incident are provided.

By promoting a risk-based approach to cybersecurity management and requiring organisations to develop appropriate policies and procedures, the Prakas helps to ensure that organisations are better prepared to prevent and respond to cybersecurity incidents. However, the effectiveness of the Prakas will depend on its implementation and enforcement, as well as the level of awareness and understanding of cybersecurity issues among stakeholders in the country.

Still, the Prakas presents certain weaknesses. First, its scope is limited. The Prakas primarily focuses on cybersecurity management in the private sector, and does not provide comprehensive guidelines for government agencies or critical infrastructure operators. This could limit the effectiveness of the Prakas in addressing cybersecurity threats that may impact the country's national security. The Prakas has also been criticised because of its lack of enforcement mechanisms. The Prakas does not specify penalties or sanctions for non-compliance, which could limit its effectiveness in promoting cybersecurity best

practices and creating incentives for organizations to improve their cybersecurity posture. Another cause of concern is due to its ambiguity in some provisions. Some provisions in the Prakas are not clearly defined, such as the requirements for incident response plans or the criteria for risk assessments. This could lead to inconsistent interpretation and implementation of the Prakas across different organizations. Finally, public awareness of this legal mechanism is relatively low. There is a lack of public awareness and understanding of cybersecurity issues in Cambodia, which could limit the effectiveness of the Prakas in promoting cybersecurity best practices and creating a culture of cybersecurity awareness among stakeholders.

2.5. The Sub-decree on the Establishment of the National Authority for Combating Cybercrime

The Sub-decree on the Establishment of the National Cybersecurity Committee was issued by the Cambodian government in 2020. The Sub-decree is aimed at establishing a national cybersecurity strategy and framework (Pradeep, 2021), and creating a centralised body responsible for coordinating and overseeing cybersecurity efforts across different government agencies and private sector organisations. The National Cybersecurity Committee is composed of representatives from various government agencies and private sector organizations, including the Ministry of Posts and Telecommunications, the National Police, the Ministry of National Defence, and the Ministry of Interior. It establishes the National Cybersecurity Committee as the main body responsible for coordinating and overseeing cybersecurity efforts in Cambodia. The National Cybersecurity Committee is responsible for developing and implementing a national cybersecurity strategy and framework, as well as coordinating cybersecurity efforts across different government agencies and private sector organizations. The Sub-decree requires that the National Cybersecurity Committee provide regular reports on cybersecurity issues to the Prime Minister, and that government agencies and private sector organizations report any cybersecurity incidents to the National Cybersecurity Committee.

Furthermore, the RGC also created a cyber war team in 2014 to monitor online activity in digital platforms like websites, Facebook, Twitter, Google-plus, blogs, YouTube and other media outlets. The official narrative is that the

stance and prestige of the government needs to be protected (Blomberg, 2014).

Overall, the Sub-decree on the Establishment of the National Cybersecurity Committee represents an important step forward in establishing a centralized body responsible for coordinating and overseeing cybersecurity efforts in Cambodia. By creating a national cybersecurity strategy and framework, and promoting coordination and information sharing among different stakeholders, the Sub-decree helps to ensure that Cambodia is better prepared to prevent and respond to cybersecurity threats. However, the effectiveness of the Sub-decree will depend on its implementation and enforcement, as well as the level of commitment and collaboration among different stakeholders in the country.
The Sub-decree primarily focuses on government agencies, with limited involvement from private sector organizations. Given that the private sector is a key target for cyberattacks, it is important to ensure that private sector organizations are actively engaged in cybersecurity efforts. There is also a relative lack of detail on the national cybersecurity strategy. While the Sub-decree calls for the development of a national cybersecurity strategy, it does not provide details on the specific elements of the strategy. This could lead to inconsistencies in interpretation and implementation of the strategy across different stakeholders. The Sub-decree outlines the functions and composition of the National Cybersecurity Committee, but there may be ambiguity in the roles and responsibilities of individual members and participating organizations. Critiques have also focused on its limited enforcement mechanisms, since penalties or sanctions for non-compliance are not specified, which could limit its effectiveness in promoting cybersecurity best practices and creating incentives for organizations to improve their cybersecurity posture.

3. DISCUSSION: WHAT NEXT?

The two previous sections have shown how the popularisation of the internet have brought remarkable social, economic, and political developments in Cambodia. Given the significance of these changes in the digital sphere – a relatively new concept – new legal provisions became necessary to regulate the use of the internet. An assessment of the state of cybercrime laws devises two key outcomes. First, Cambodia has taken important steps to improve its cybersecurity landscape. This is the most remarkable and necessary development given the lack of legal regulations for the cyberspace and, crucially, given the increasing number of threats associate to the use of the internet that affect not only Cambodia, but the region as a whole. Although some of the legal provisions found in the Criminal Code address computer-related offenses, a legal reform was needed. The second outcome from the overview of some of the key legal developments that regulate cybercrime is that, although new laws have been created or are being drafted, they still present urgent challenges that need to be addressed. The rest of this section outlines some of them.

First, public awareness. One of the primary challenges is the lack of cybersecurity awareness (Corrado and Sakal, 2021) among the general public and private sector organisations. Many individuals and organizations in Cambodia are not aware of the risks of cyber threats and do not take necessary precautions to protect their digital assets. This can leave them vulnerable to cyberattacks, such as phishing scams or malware infections. In this sense, education and more specifically, digital literacy are key strategies to increase people's awareness of cybersecurity as a problem and make them aware of how to protect themselves against cyberattacks – or how to reduce the risk of being a victim.

Second, limited resources. Another challenge is the limited resources available for cybersecurity initiatives in Cambodia (ASEAN, 2022). This includes limited funding, as well as a shortage of trained cybersecurity professionals. Without proper funding and resources, it can be difficult for the government and private sector organizations to implement comprehensive cybersecurity measures and respond effectively to cyber incidents. Additionally, the fast-paced evolution of technology poses a challenge to cybersecurity in

Cambodia. As new technologies emerge, new vulnerabilities and threats arise, and it can be difficult for organizations to keep up with the latest cybersecurity best practices.

Third, limited international cooperation. Furthermore, the lack of international cooperation (JICA, 2022) and coordination can also pose challenges for cybersecurity in Cambodia. As cyber threats often cross borders, countries need to work together to share information and collaborate on cybersecurity initiatives. Additionally, joint efforts to develop and adhere to international framework like Council of Europe's Convention on Cybercrime (COE, n.d) is a key strategy all countries – not only Cambodia – can improve.

Fourth, domestic cooperation. Like the previous point, cooperation must again be highlighted but at a domestic level (ODC, 2021). International cooperation is important because it helps aligning the views of the international community on cybersecurity. Additionally, it adds a layer of accountability since signing international treaties creates a system of checks and balances that, in theory, should protect netizens. Nonetheless, domestic cooperation between key stakeholders is necessary for that to happen. Cooperation must happen between the government and key agents like civil society organisations (CSOs), activists, the media sector, academics, and any other political force or group that represents the interests of specific social cohorts. It is essential so the development of a legal framework concerning the digital sphere is made with the consensus of all actors, so each provision can be negotiated and agreed by all.

4. CONCLUSION

In the last decade, Cambodia has achieved significant progress in the development of cybersecurity laws to make the digital sphere a safer environment. The development of a legal framework in this field was – and still is necessary due to the rapid popularisation of digital tools and media in the country. While the internet has resulted in a range of opportunities, including the possibility to improve communication between people and other civil society actors or gain access to different and more varied sources of information, the rapid development of the digital sphere has also presented multiple challenges, such as addressing cybercrime or determining who and how should manage the activity taking place in the virtual space.

The examination of five key legal developments – the Law on the Management of the Nation's Telecommunications Sector; Law on Cybercrime; Sub-decree on the Establishment of the National Authority for Combating Cybercrime; Prakas on Cybersecurity Management; and the Sub-decree on the Establishment of the National Cybersecurity Committee – show two key traits of the current state of cybersecurity laws in Cambodia. First, and as previously mentioned, the Cambodian government has been able to identify a number of the ongoing challenges in the digital sphere and develop a plan to improve security in the digital sphere. Second, the completion of a legal framework addressing the ongoing challenges that have resulted from the popularisation of the internet is not likely to happen in the upcoming years. On the one hand, because the digital sphere is in constant evolution and with every new development in the technological sector, new challenges will appear. On the other hand, the completion of a robust cybersecurity needs a more direct implication from all relevant civil society stakeholders in Cambodia, including NGOs, activists, the media sector, academia, and the private sector. Making all these stakeholders active participants in the conversations with the government to shape the norms that regulate the digital sphere in the Cambodia is not only essential to make such regulations more inclusive, but also sustainable at a domestic level, and also regionally.

BIBLIOGRAPHY

Article19 (n.d.) Draft law on cybercrime english, Cybercrime Law. Article19. Available at: https://www.article19.org/wp-content/uploads/2018/02/Draft-Law-On-CyberCrime_Englishv1.pdf

ASEAN (2022) Asean Cybersecurity Cooperation Strategy, ASEAN cybersecurity cooperation strategy. ASEAN. Available at: https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

Blomberg, M. (2014) 'Cyber War Team' to monitor web, 'Cyber War Team' to Monitor Web. The Cambodia Daily. Available at: https://english.cambodiadaily.com/news/cyber-war-team-to-monitor-web-72677/

CADT (2022) Demand for and supply of digital skills in Cambodia, CADT. Available at: https://www.cadt.edu.kh/resources/digital-skills-assessment-event-2021/demand-for-and-supply-of-digital-skills-in-cambodia-2021/

COE (n.d.) Budapest Convention - Cybercrime. COE. Available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention?_82_struts_action=%2Flanguage%2Fview&_82_languageId=fr_FR

Corrado, R. and Sakal, M. (2021) Cybersecurity in Cambodia: Awareness as a first step, CD_Center. Available at: https://cd-center.org/wp-content/uploads/2021/08/P124_20210805_V3IS11_EN.pdf

Criminal Code (2009) Criminal Code. Kingdom of Cambodia. Available at: http://www.skpcambodia.com/PDF/storage/uploads/files/Criminal%20and%20Criminal%20Procedure%20Laws/criminal-code%20Eng.pdf (Accessed: March 18, 2023).

Flynn, G. (2019) Cambodia's cybersecurity challenges, CapitalCambodia. Available at: https://capitalcambodia.com/cambodias-cybersecurity-challenges/

HRW (2021) Cambodia: Scrap draft cybercrime law, Human Rights Watch. Available at: https://www.hrw.org/news/2020/11/13/cambodia-scrap-draft-cybercrime-law

IPI (2020) Cambodia cyber-crime law will stifle press freedom, International Press Institute. Available at: https://ipi.media/cambodia-cybercrime-law-will-stifle-press-freedom/

JICA (2022) Signing of Record of Discussions on Technical Cooperation Project with Cambodia: Project for Improvement of Cyber Resilience. JICA. Available at: https://www.jica.go.jp/english/news/press/2022/20221205_41.html

Kelliher, F. (2023) Leaked law proposal would give Cambodia expanded powers to censor critics, Rest of World. Available at: https://restofworld.org/2023/cybersecurity-law-draft-cambodia-elections/

Kemp, S. (2023) Digital 2023: Cambodia - DataReportal - Global Digital Insights, DataReportal. DataReportal - Global Digital Insights. Available at: https://datareportal.com/reports/digital-2023-cambodia

Levi, M. and Stoker, L. (2000) "Political Trust and trustworthiness," Annual Review of Political Science, 3(1), pp. 475-507. Available at: https://doi.org/10.1146/annurev.polisci.3.1.475.

MPTC (2022) Cambodia Digital Government policy 2022-2035, ក្រសួងប្រៃសណីយ៍ និងទូរគមនាគមន៍. Available at: https://mptc.gov.kh/en/documents/policies/28365/

Narin, S. (2020) Activists: Cambodia's draft Cybercrime Law Imperils Free Expression, privacy, VOA. Voice of America (VOA News). Available at: https://www.voanews.com/a/east-asia-pacific_activists-cambodias-draft-cybercrime-law-imperils-free-expression-privacy/6196959.html

ODCa (n.d.) OpenDevelopment, Open Development Cambodia (ODC). Available at: https://opendevelopmentcambodia.net/tag/digital-economy/

ODCb (n.d.) Open Development Cambodia, Open Development Cambodia (ODC). Available at: https://opendevelopmentcambodia.net/tag/draft-cybercrime-law/#!/story=post-127300

ODC (2021) Cambodia pledges cooperation in push for Inclusive Cyberspace. Open Development Cambodia. Available at: https://opendevelopmentcambodia.net/news/cambodia-pledges-cooperation-in-push-for-inclusive-cyberspace/#!/story=post-155739

Phong, K., Srou, L. and Solá, J. (2016) Mobile phones and internet use in Cambodia 2016 - The Asia Foundation, Asia Foundation. Asia Foundation. Available at: https://asiafoundation.org/wp-content/uploads/2016/12/Mobile-Phones-and-Internet-Use-in-Cambodia-2016.pdf?source=post_page----

Pradeep, A. (2022) Cambodia to strengthen personal data protection measures - Khmer Times, Khmer Times - Insight into Cambodia. Available at: https://www.khmertimeskh.com/501063124/cambodia-to-strengthen-personal-data-protection-measures/

Property Report (2021) Cambodia improves digital infrastructure with Digital roadmap 2021-2035, Asia Property Awards. Available at: https://www.asiapropertyawards.com/en/cambodia-improves-digital-infrastructure-with-digital-roadmap-2021-2035/

Seng, M. (2022) Fears Raised Over Cybercrime Draft Law, Fears raised over cybercrime draft law. Kiripost2. Available at: https://kiripost.com/stories/fears-raised-over-cybercrime-draft-law

Tunggal, T. (2023) Why is cybersecurity important?, RSS. Available at: https://www.upguard.com/blog/cybersecurity-important
UNESCO (2020) Cambodia: Digital Education is here to stay, IIEP. Available at: https://www.iiep.unesco.org/en/cambodia-digital-education-here-stay-13492

Vong, M. and Hok, K. (2018) “Facebooking,” South East Asia Research, 26(3), pp. 219–234. Available at: https://doi.org/10.1177/0967828x17754113.
WTO (2015) WTACCKHM5 leg 10 - World Trade Organization, WTO. Available at: https://www.wto.org/english/thewto_e/acc_e/khm_e/WTACCKHM5_LEG_10.pdf

contact@opendevcam.net
+855 23 902 196
Open Development Cambodia
Open Development Cambodia Organization
Open Development Cambodia Organization
Open Development Cambodia Organization
www.opendevelopmentcambodia.net
#23B, Street 606, Sangkat Boeng Kak Ti Pir, Khan Tuol Kouk, Phnom Penh, Cambodia