CCHR Briefing Note – February 2014

Cyber Laws: Tools for Protecting or Restricting Freedom of Expression?

Executive summary

This Briefing Note focuses on the drafting of the Kingdom of Cambodia's ("Cambodia") first ever Cyber Crimes Law (the "Law"), initially announced in May 2012. This Briefing Note summarizes the current internet landscape in Cambodia, the worldwide increase in cyber-crimes, and the ways in which cyberspace can be legislated, and offers concrete recommendations to the Royal Government of Cambodia (the "RGC") on the draft Law to ensure it complies with international human rights standards and guarantees the right to freedom of expression. According to Cambodian officials, the Law is being drafted in response to the mushrooming of modern technology and to put a halt to the spreading of "false information" online.[1] However, in response to concerns that this proposed Law would result in internet censorship, the spokesman for the Council of Ministers, Phay Siphan, assured skeptics that the sole purpose of the Law would be to protect internet users in Cambodia from hacking and the destruction of online data.[2] He also mentioned that the RGC would be following European Union ("EU") guidelines when drafting the Law.[3] The Law is expected to be passed in the first half of 2014, although requests from civil society to review the draft have thus far been denied.

The first section of this Briefing Note describes the current status of internet freedom in Cambodia. The second section introduces the risks linked with legislating cyberspace, exposing the threat it can pause to human rights. The third section provides an overview of the international standards and EU regulations that the RGC must comply with when drafting the Law and gives the example of domestic legislation in Germany. Finally, the Briefing Note concludes with recommendations to the RGC regarding the content of the draft Law, including:

- Publically and widely publishing the draft of the Law to allow for genuine consultation with sufficient time for analysis and comments on the draft by relevant stakeholders such as civil society organizations;
- Ensuring that sufficient time is taken to draft the Law, including providing ample time for lawmakers, civil society organizations ("CSOs") and technical experts to read drafts and provide feedback, as well as a period to address and incorporate this feedback;
- Establishing an open forum or national congress in order to let CSOs, human rights activists, bloggers, individuals who work with new media, Internet Service Providers ("ISPs") and programmers discuss their needs and raise their concerns with the RGC, and using their input to inform the contents of the Law;

[1] CCHR, 'Cambodian Government is drafting first ever cyber law' (Alert) (24 May, 2012) http://bit.ly/1m6ajuH.
[2] Joshua Wilwohl, 'Anonymous Hacks Government Websites' *The Cambodia Daily* (13 September 2013) http://bit.ly/19tm2Tz.
[3] Faine Greenwood, 'As the Internet Raises Civic Voices in Cambodia, a Struggle Brews Over Net Control' *Personal Democracy Media* (27 March 2013) http://bit.ly/1clYzyF.

- Clearly and explicitly stating the extent of restrictions made through the Law and by the RGC, including narrowly and unambiguously defining content that is going to be deemed 'illegal' so as to avoid the possibility of abusive interpretation; and
- Establishing an independent working group made up of (*inter alia*) technical experts, members of CSOs and academics to properly investigate and analyze website content prior to prosecution or blocking requests and before it is forwarded to the judiciary.

This Briefing Note is written by the Cambodian Center for Human Rights ("CCHR"), a non-aligned, independent, non-governmental organization ("NGO"), that works to promote and protect democracy and respect for human rights – primarily civil and political rights – throughout Cambodia.

Introduction: the internet in Cambodia

While Cambodia has one of the lowest internet connectivity rates in Southeast Asia,[4] internet penetration is increasingly on the rise, especially in urban centers. This is partly due to the increase in the availability of smart phones: almost 100% of the population owns a mobile phone, with 40% owning a smart phone.[5] Social media networks, such as Facebook, are gaining popularity and are increasingly used to share information, such as breaking news, and to socialize.[6]

While traditional forms of media in Cambodia are heavily censored and biased in favor of the ruling Cambodian People's Party ("CPP"),[7] the internet, however, has thus far remained relatively free in comparison. Nevertheless, there have been several incidences whereby the RGC and its institutions have threatened online freedom, suggesting that the authorities are anxious to gain control over the medium. It is reported that the RGC routinely requests ISPs operating in Cambodia to block sites that host content critical of the RGC,[8] including such sites as Ki Media, Khmerization and Sacrava – all of which are well-known for propagating information critical of the authorities.[9] Many allege that access had been blocked on orders of the RGC. Moreover, in November 2012, the Ministry of Posts and Telecommunication issued a circular regulating access to internet cafes in order to prevent school children from accessing online games and pornography. Had it been implemented, it would have resulted in the closure of almost all such establishments in Phnom Penh.[10]

Furthermore, two incidents in 2013 of local authorities targeting social media posts in order to suppress freedom of expression online have increased fears that cyber censorship is forthcoming in Cambodia.[11] The first is the case of Phel Phearun, a teacher who was summoned and threatened with defamation charges because of his criticism of the police on his Facebook page in February

[4] International Telecommunication Union, 'Information Society Statistical Profiles: Asia and the Pacific' (2009), http://bit.ly/1eIdyGf. For more information, see CCHR, 'New Media and the Promotion of Human Rights in Cambodia' (Report) (July 2012).
[5] Sothearith Im, 'Social Media Changing Cambodia's Digital Landscape' *Voice of America* (25 December 2012) http://bit.ly/1gJ0Zvx.
[6] CCHR Focus Group Discussions, 8 February and 15 February 2014, Phnom Penh, Cambodia. Participants in the two FDGs (23 in total) included students of several Phnom Penh-based universities – the Royal University of Phnom Penh, the Royal University of Law and Economics and the University of Cambodia – as well as NGO representatives.
[7] See CCHR, 'Repression of Expression: The state of free speech in Cambodia' (Report) (September 2013) http://bit.ly/1e9EjkG.
[8] For more information, see Freedom House, 'Freedom on the Net 2013: Cambodia' http://bit.ly/1hVJ20u
[9] CCHR, 'Policy Brief: Freedom of Expression in the Kingdom' (December 2013) http://bit.ly/1fBjXBR.
[10] For details, see Kounila, Keo; 'Cambodia Bans Internet Cafes Near Schools' *Global Voices* (19 December 2012) http://bit.ly/1gI9FlX
[11] Opinions expressed by participants in CCHR Focus Group Discussions on 8 and 15 February 2014. Supra note 6.

2013.[12] The second is the case of Cheth Sovichea, who, in November 2013, was also arrested for a Facebook post critical of the police. He too was threatened with defamation charges.[13] Although both cases were dropped and both men released after they were made to apologize to the authorities, they suggested that the Cambodian authorities are becoming increasingly paying attention to online activity and are keen to gain tighter control over what is said on the internet. More recently, in early February 2014, TV presenter and salon owner Duong Zorida was convicted on charges of defamation – resulting in a fine of two million Riels and an order to pay seven million Riels in compensation to the plaintiffs – after another woman accused Zorida of publically complaining, on Facebook, that the plaintiff was luring Zorida's employees to come work at her shop.[14] This case highlights the Cambodian courts' willingness to consider – and criminalize – online content similarly to offline discourse.

Threats to internet security

The expansion of the internet and cyberspace over the last few years has seen this sphere become integral to society and has changed the way people live and communicate on a global scale. The internet now serves as a primary source of information, a means of conducting business and a way of communicating with others. However, with the expansion of cyberspace has come the escalation of cyber-crime. Although definitions of "cyber-crime" can differ based on the sources and the range of acts included within any one definition can vary, a broad definition can include anything from state-sponsored attacks to gain intelligence – a form of modern-day espionage – to hacking websites in acts of dissidence and political protest to copyright offenses to the online dissemination of child pornography to crimes such as identify and information theft, e-scams, raids of bank accounts and more.[15]

More than one million people worldwide are victims of cyber-crime every day,[16] at a cost to the global economy of around USD 300 billion a year.[17] A February 2013 report by the United Nations ("UN") Office on Drugs and Crime ("UNODC") notes that "*Upwards of 80 per cent of cybercrime acts are estimated to originate in some form of organized activity, with cybercrime black markets established on a cycle of malware creation, computer infection, botnet management, harvesting of personal and financial data, data sale, and 'cashing out' of financial information. Cybercrime perpetrators no longer require complex skills or techniques.*"[18]

The frequency of cyber-crime is also increasing exponentially; for instance, between April and December 2012, the types of malware threats detected on Google's Android Platform increased an astonishing amount from 11,000 to 350,000.[19] Most worrying are indications that cyber-crime impacts a greater proportion of the population than traditional, offline crime; the UNODC study

[12] CCHR, 'Case Study: Phel Phearun' (Factsheet) (March 2013) http://bit.ly/1amOOAq
[13] Lieng Sarith, 'Facebook user busted over posts' *The Phnom Penh Post* (20 November 2013) http://bit.ly/1mzeS6a.
[14] -- 'Actress Duong Zorida loses case at Court' *The Cambodia Herald* (8 February 2014) http://bit.ly/1hDFvot.
[15] See: 'What is Cybercrime' (*Norton by Symantec*) http://bit.ly/1jTCtJK; 'Definition of cyber crime' (*Financial Times Lexicon*) http://on.ft.com/1hDIehB; 'Cybercrime' (*Technopedia*) http://bit.ly/1mzjKZ7.
[16] EU, 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace' (February 2013) http://bit.ly/1hxNYJO.
[17] Paul Taylor, 'Cybercrime costs US $100bn a year, report says' *The Financial Times* (23 July 2013) http://on.ft.com/LazZv7
[18] UNODC, 'Comprehensive Study on Cybercrime' (Draft, February 2013) p. xvii, http://bit.ly/1mzlotM.
[19] Andrea Renda, 'Cybersecurity and Internet Governance' (Council on Foreign Relations, 3 May 2013) http://on.cfr.org/1m6aDJR.

found that "*victimization rates for online credit card fraud, identity theft, responding to a phishing attempt, and experiencing unauthorized access to an email account, vary between 1 and 17 per cent of the online population for 21 countries across the world, compared with typical burglary, robbery and car theft rates of under 5 per cent for these same countries."*[20] Concerns about the increase in cyber-crimes are being reflected in Cambodia: participants in two Focus Group Discussions organized by CCHR in Phnom Penh in February 2014 expressed concerns over the spread of false information over the internet, in particular on social networks such as Facebook, hacking of e-mail and social network accounts, and theft of information over the internet.[21]

With such high expansion rates of threats, there is a need for a level of protection for internet users so that they can feel safe in the cyber sphere. The borderless nature of the internet, which connects people and businesses regardless of geographical limitations, makes it difficult to pin criminal activity down to one legal jurisdiction. This system of communication has enabled the easy conduct of transactions and interactions across the world, but has brought into question the jurisdiction of and responsibility for cyber security and cyber criminals. Many nations seek to afford a certain level of protection to their citizens accessing the cyberspace, for example by ensuring safe passage of personal data and protecting young children from indecent images. Cyber-crimes often replicate crimes that are traditionally committed offline, such as identity theft and fraud, and in most jurisdictions existing legislation covering these crimes can be applied online. However, the perpetuation of some crimes is considerably easier under the guise of internet anonymity.[22] There is a danger of cyber threats to not just individuals, but to businesses and governments as well.

Thus far, cyber-crime in Cambodia has most noticeably manifested in the form of Anonymous Cambodia, a branch of the worldwide hacking group Anonymous that aims to unveil governments' secrets. In July 2013, ahead of the elections, they claimed to have hacked into the Cambodian National Election Committee's ("NEC") database in protest against perceived attempts to register ineligible voters to vote in the National Assembly Elections.[23] In September 2013, Anonymous Cambodia also hacked into the websites of the Press and Quick Reaction Unit of the Council of Ministers, the Council of Legal and Judicial Reform and CPP-aligned TV station TVK.[24] In addition to Anonymous Cambodia, apolitical attacks on websites such as those of Legend Cinemas, Sabay News, Lao Airlines and Sorya Transport have also taken place, allegedly to "*draw attention to faulty security protocols*."[25] Finally, there are also growing concerns that as online credit card transactions and other forms of e-banking – thus far limited – increase in frequency in Cambodia, cyber-crime will increase correspondingly,[26] especially given Cambodia's weak internet infrastructure.[27]

Legislating cyberspace

[20] UNODC, 'Comprehensive Study on Cybercrime' (Draft, February 2013), p. xviii.
[21] CCHR Focus Group Discussions, 8 February and 15 February 2014, Phnom Penh, Cambodia. Supra note 6.
[22] Richard Wortley and Stephen Smallbone, 'Child Pornography on the Internet', Community Oriented Policing Services, US Department of Justice (May 2006), p.9, http://1.usa.gov/1iS1XHi.
[23] Bennett Murray, ''We are legion': Anonymous hackers target the Kingdom' *The Phnom Penh Post* (19 July 2013), http://bit.ly/1andLik
[24] Joshua Wilwohl, 'Anonymous Hacks Government Websites' *The Cambodia Daily* (13 September 2013) http://bit.ly/1ca77d3.
[25] Bennett Murray, ''We are legion': Anonymous hackers target the Kingdom' *The Phnom Penh Post* (19 July 2013).
[26] CCHR Focus Group Discussions, 8 February and 15 February 2014, Phnom Penh, Cambodia.
[27] Mak Lawrence Li, 'Web hacks a risk for banks' *The Phnom Penh Post* (7 June 2013) http://bit.ly/1jWiqh0.

As a consequence of the rapidly expanding threat to cyberspace many nations have sought to consolidate legislation into comprehensive and coherent laws on cyber security. As the UNDOC study notes,

> "*At the national level, […] cybercrime laws most often concern criminalization, indicating a predominant focus on establishing specialized offences for core cybercrime acts. Countries increasingly recognize, however, the need for legislation in other areas. Compared to existing laws, new or planned cybercrime laws more frequently address investigative measures, jurisdiction, electronic evidence and international cooperation. Globally, less than half of responding countries perceive their criminal and procedural law frameworks to be sufficient, although this masks large regional differences. While more than two-thirds of countries in Europe report sufficient legislation, the picture is reversed in Africa, the Americas, Asia and Oceania, where more than two-thirds of countries view laws as only partly sufficient, or not sufficient at all."*[28]

However, the undeniable danger with cyber laws or policies is that they can infringe on rights such as freedom of expression and access to information online.

Case Study 1: Thailand

Thailand's 2007 Computer Crime Act ("CCA") focuses on lèse majesté,[29] security and politics. It criminalizes anything that could be deemed as critical of the Thai Royal Family, and can be used as a means to silence any political opposition,[30] severely infringing on rights to privacy, rights to access information and the right to freedom of expression. From April to December 2010, the Thai government declared a state of emergency and enabled a mechanism to block any website considered to be publishing politically sensitive or controversial material without the requirement of a court order. In July 2011 a new democratically elected opposition took office and proved to be just as committed to internet censorship and curbing online activities with lèse majesté content.[31] By May of 2012 some websites were made accessible once again, but many more websites were added to the list.[32] In 2012, nearly 21,000 URLs were blocked by 161 court orders, the majority of which were due to lèse majesté content.[33]

Moreover, Articles 14 and 15 of the CCA allow for the prosecution of content providers and intermediaries accused of posting or allowing the dissemination of content considered to be harmful to national security or public order,[34] meaning that someone hosting an online forum can be held liable for a post made by one of the forum's users even if the host is unaware of what was posted. The 2008 Internal Security Act ("ISA") has also had a negative impact on freedom of expression in Thailand. The Ministry of Information and Communication Technology ("MICT") opened a hotline for the reporting of offensive websites and, along with the Ministry of Justice, introduced a "cyber

[28] UNODC, 'Comprehensive Study of Cybercrime' (Draft, February 2013) p. xviii.
[29] This means the crime of insulting of a monarch or another sovereign power - similar to treason.
[30] Pavin Chachavalpongpun, 'Thailand's Lèse-majesté laws: a potent weapon' (26 December 2011) http://bit.ly/1aEiaxN
[31] Ibid.
[32] Ibid.
[33] Freedom House, 'Freedom on the Net 2013: Thailand' (2013) http://bit.ly/1fpqMpi.
[34] Pavin Chachavalpongpun, 'Thailand's Lèse-majesté laws: a potent weapon' (26 December 2011).

scout" scheme to train students as web monitors.[35] This, paired with an online monitoring group called the "Social Sanctions," [36] has resulted in "cyber witch-hunting."[37]

In March 2010, Chiranuch Premchaiporn, the editor of the *Prachatai* news website, was arrested and charged under Article 15 of the CCA and under the Thai Penal Code for content posted by *Prachatai* readers related to the 2006 military coup and the role of the Royal Family. In May 2012, she was convicted and sentenced to one year in prison and fined 30,000 bahts ($920). In November 2013, the Court of Appeal upheld her conviction. Premchaiporn is currently appealing her case to the Supreme Court, on the grounds that she should be held criminally responsible for comments posted by others.

Nevertheless, the need to provide protection for internet users and to combat crimes such as child pornography or fraud does not necessarily contradict online freedom. As Ms. Neelie Kroes, Vice-President of the European Commission explains:

> "*Too often, freedom and security are caricatured as incompatible alternatives. As though measures to ensure one can only be at the expense of the other. In fact the opposite is true. Because there is no freedom without security; these concepts are interdependent and complementary. I may have the legal right to walk down a particular road at night: but am I truly free to do so, if it is not safe? Likewise, people aren't really going to use the internet freely, unless they know they are in control of their privacy – that their personal data will be handled transparently and fairly. That interdependence is why liberty and security are mentioned in the very same Article, the very same sentence, of the European Convention on Human Rights."*[38]

Internet freedom under international law

Both the EU and UN human rights bodies have weighed in heavily on the question of internet freedom, acknowledging a need to restrict certain online content, such as child pornography, while calling for caution and respect of human rights such as freedom of expression and access to information. Internet rights have been affirmed under both Articles 19 of the Universal Declaration of Human Rights ("UDHR")[39] and the International Covenant on Civil and Political Rights ("ICCPR").[40] Article 19 of the ICCPR, which was ratified by Cambodia in 1992 and is a part of Cambodia's national legislation,[41] requires the protection and promotion of the rights to hold opinions, to freedom of expression and to access information. It acknowledges that the right to freedom of expression is not absolute, but can be restricted under exceptional circumstances for *"the respect of the rights and reputations of others"* and for *"the protection of national security (order public), or of public health*

[35] Freedom House, 'Freedom on the Net 2012: Thailand' http://bit.ly/1iS3MUH.
[36] Sawatree Suksri et al, 'Situational Report on Control and Censorship of Online Media, Through the Use of Laws and the Imposition of Thai State Policies' (December 2010) p.14 http://bit.ly/1drzeVA.
[37] OpenNet Initiative country profile: 'Thailand' (7 August 2012) http://bit.ly/1ma8aOt.
[38] Neelie Kroes, 'The European public on the Net', Digital Agenda Internet Freedom Republica conference (Berlin, 4 May 2012) http://bit.ly/1b1EYUy.
[39] UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III).
[40] UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966.
[41] Constitutional Council of the Kingdom of Cambodia, Decision No. 092/003/2007 (10 July 2007).

or morals."[42] However, all limitations on the right must be prescribed by law and must not jeopardize the essence of the right itself.[43]

Although the internet was not in existence when the ICCPR was drafted and adopted and thus does not feature specifically in the text, paragraph 2 of Article 19 of the ICCPR specifically states that the right *"shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or* ***through any other media of his choice****"* (emphasis added). It is therefore held by human rights bodies that the right to freedom of expression readily applies online.

In an August 2011 report to the UN Human Rights Council on the "Promotion and protection of the right to freedom of opinion and expression,"[44] Frank La Rue, the Special Rapporteur on the Right to Freedom of Expression (the "Special Rapporteur"), noted that although the internet provides potential for misuse and illegal activities, ultimately it is a positive new development that gives people access to information and a means of communication like never before. In July 2012, the UN Human Rights Council adopted a resolution affirming the application of rights online, especially freedom of expression,[45] reasserting that Articles 19 of both the UDHR and the ICCPR apply both online and offline and that attempts by governments to illegitimately censor internet content or block websites are not compatible with the ICCPR.[46]

Internet regulation in the European Union

Due to the transnational nature of much of these crimes, many States – including those of the EU – have sought to cooperate in combating cyber-based offenses. As asserted by the spokesman for the Cambodian Council of Ministers, Phay Siphan, the planned Cyber Crimes Law is to be in line with the relevant EU guidelines.[47] A number of different instruments, declarations and conventions regulate internet within the EU.

The European Convention on Human Rights

Article 10 of the European Convention on Human Rights ("ECHR") protects the right to freedom of expression and association. Similar to Article 19 of the ICCPR, Article 10 of the ECHR acknowledges that freedom of expression is not an absolute right and is therefore subject to restrictions in exceptional circumstances that are lawful in a democratic society.[48] Article 8 of the ECHR states that surveillance, monitoring and seizures of information should only be carried out in accordance with the law and when necessary to protect "national security, public safety or the economic well-being

[42] UN General Assembly, International Covenant on Civil and Political Rights.
[43] UN Commission on Human Rights, The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, 28 September 1984, E/CN.4/1985/4.
[44] Frank La Rue, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report (10 August 2011) (A/66/290) http://bit.ly/1d2PaiZ
[45] UN Human Rights Council, 'The Promotion, Protection and Enjoyment of Human Rights on the Internet', A/HRC/20/L.13.
[46] Ibid, paragraph 15.
[47] Faine Greenwood, 'As the Internet Raises Civic Voices in Cambodia, a Struggle Brews Over Net Control' (*Personal Democracy Media*, 27 March 2013) http://bit.ly/1clYzyF
[48] According to Article 10(2) of the ECHR, the restrictions must be necessary in a democratic society in "*the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary*."

of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

The Budapest Convention

The Council of Europe Convention on Cybercrime, CETS no.185 (the "Budapest Convention"), which opened for signature in 2001, came about, as the Preamble states, because of the States' belief in "*the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation*" and because of they were "*Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks."*[49] The Budapest Convention focuses primarily on copyright infringements, computer-related fraud, child pornography and violations of network security, dividing requirements for signatories into two main Chapters: "Measures to be taken at the national level" (Chapter II) and "International co-operation" (Chapter III). The Budapest Convention also includes a safeguard in the form of Article 15, requiring States to ensure "*the adequate protections of human rights and liberties*," including those that come under the ECHR, the ICCPR and other human rights instruments.[50]

The Declaration by the Committee of Ministers on Internet governance and principles

The Committee of Ministers at the Council of Europe, in September 2011, in their recommendation to member states on "the protection and promotion of the universality, integrity and openness of the internet," recommended that the "*right to freedom of expression applies to both online and offline activities, regardless of frontiers*" and that the internet "*provides essential tools for participation and deliberation in political and other activities of public interest."* [51] In addition, the Council of Europe's Declaration of the Committee of Ministers on Internet Governance Principles, also adopted in September 2011, aims to consolidate efforts internationally to regulate the internet, making it safe for users while upholding the principle of maximum human rights with minimum restrictions:[52]

Council of Europe, Declaration by the Committee of Ministers on Internet governance principles[53]

1. Human rights, democracy and the rule of law

Internet governance arrangements must ensure the protection of all fundamental rights and freedoms and affirm their universality, indivisibility, interdependence and interrelation in accordance with international human rights law. They must also ensure full respect for democracy and the rule of law and should promote sustainable development. […]

2. Multi-stakeholder governance

[49] Council of Europe Convention on Cybercrime, CETS no.185, Budapest 23.11.2001, http://bit.ly/1k1pMN2
[50] Article 15 (1) Council of Europe Convention on Cybercrime, CETS no.185, Budapest 23.11.2001.
[51] Recommendation CM/Rec(2011)8 of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet (Adopted by the Committee of Ministers on 21 September 2011 at the 1121st meeting of the Ministers' Deputies) http://bit.ly/1fmshe1.
[52] Council of Europe, Declaration by the Committee of Ministers on Internet governance principles (Adopted by the Committee of Ministers on 21 September 2011 at the 1121st meeting of the Ministers' Deputies) http://bit.ly/1js9VHG.
[53] Ibid.

The development and implementation of Internet governance arrangements should ensure, in an open, transparent and accountable manner, the full participation of governments, the private sector, civil society, the technical community and users, taking into account their specific roles and responsibilities. The development of international Internet-related public policies and Internet governance arrangements should enable full and equal participation of all stakeholders from all countries.

3. Responsibilities of states

States have rights and responsibilities with regard to international Internet-related public policy issues. In the exercise of their sovereignty rights, states should, subject to international law, refrain from any action that would directly or indirectly harm persons or entities outside of their territorial jurisdiction. Furthermore, any national decision or action amounting to a restriction of fundamental rights should comply with international obligations and in particular be based on law, be necessary in a democratic society and fully respect the principles of proportionality and the right of independent appeal, surrounded by appropriate legal and due process safeguards.

4. Empowerment of Internet users

Users should be fully empowered to exercise their fundamental rights and freedoms, make informed decisions and participate in Internet governance arrangements, in particular in governance mechanisms and in the development of Internet-related public policy, in full confidence and freedom.

5. Universality of the Internet

Internet-related policies should recognise the global nature of the Internet and the objective of universal access. They should not adversely affect the unimpeded flow of transboundary Internet traffic.

6. Integrity of the Internet

The security, stability, robustness and resilience of the Internet as well as its ability to evolve should be the key objectives of Internet governance. […] it is necessary to promote national and international multi-stakeholder co-operation.

7. Decentralised management

The decentralised nature of the responsibility for the day-to-day management of the Internet should be preserved. The bodies responsible for the technical and management aspects of the Internet, as well as the private sector should retain their leading role in technical and operational matters while ensuring transparency and being accountable to the global community for those actions which have an impact on public policy.

8. Architectural principles

The open standards and the interoperability of the Internet as well as its end-to-end nature should be preserved. […]

9. Open network

Users should have the greatest possible access to Internet-based content, applications and services of their choice, whether or not they are offered free of charge, using suitable devices of their choice. […]

10. Cultural and linguistic diversity
Preserving cultural and linguistic diversity and fostering the development of local content, regardless of language or script, should be key objectives of Internet-related policy and international co-operation, as well as in the development of new technologies.

The Cyber Security Strategy
Building on this convention and declarations, in February 2013, the EU issued a Cyber Security Strategy, setting out priorities for EU cyberspace policy and for effective cyber regulation.[54] Key priorities include improving access to information in cyberspace, preventing cyber threats, encouraging international cooperation in order to address issues related to the internet and to cyberspace and expanding access to the internet. Through this strategy, the EU affirmed the importance of fundamental rights to the development of cyber security by stating: "*cyber security can only be sound and effective if it is based on fundamental rights and freedoms*."[55] Through this Strategy, the EU will "*engage with international partners and organisations, the private sector and civil society to support global capacity-building in third countries […] These actions will focus on enhancing criminal justice capabilities in training prosecutors and judges, and introducing the Budapest Convention […] principles in recipient countries' legal framework, building law enforcement capacity to advance cybercrime investigations and assisting countries to address cyber incidents."*[56]

In comparison to the EU, the Association of Southeast Asian Nations ("ASEAN"), of which Cambodia is a member, has yet to provide any real leadership in terms of cyber legislation. ASEAN has acknowledged that cyber-crimes are an area to address through "*capacity building, information sharing and intelligence exchange"* between member states,[57] indicating willingness for interstate cooperation. Moreover, in October 2011, ASEAN members declared cyber-crime to be one of the eight priority areas for preventing and combatting transnational crime;[58] however, little has been done so far towards developing related conventions or strategies which would provide concrete solutions for these issues.

Domestic regulation of cyberspace
The Special Rapporteur emphasizes in his 2011 report certain elements that should be sought in domestic cyberspace legislation, in order to protect freedom of expression. Firstly, he notes that an independent court or body, free of political influence, must govern any legislation blocking or filtering content.[59] He also notes that intermediaries (e.g. webmasters and administrators) should

[54] EU, 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace' (February 2013) http://bit.ly/1hxNYJO.
[55] Ibid.
[56] 'EU Cyber Security Strategy – open, safe and secure' (*European Union External Action*) http://bit.ly/1ffqocZ.
[57] See: ASEAN, 'Co-Chairs Summary Report on the meeting of the ASEAN Regional Forum Inter-Sessional Support Group on Confidence Building Measures' (11-14 April 2004) http://bit.ly/1eCWtwR
[58] ASEAN Regional Forum, 'ASEAN Cooperation in Combatting Transnational Crime Moving Towards 2015 and Beyond' (Bali, Indonesia, 13 October 2011) http://bit.ly/1hWraTk
[59] Frank La Rue, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report (10 August 2011) (A/66/290), paragraph 38.

not be held responsible for content posted by third party users.[60] Finally, he emphasized the following four areas as "exceptional types of expression that States are required to prohibit under international law," both offline and in cyberspace:

1. Child pornography;
2. Direct and indirect incitement to genocide;
3. Advocacy of national, religious or racial hatred that constitutes incitement to discrimination, hostility or violence; and
4. Incitement to terrorism.[61]

The drafting of a cyber-crime law requires thorough investigations into cyber legislation around the world. After offering an overview of international and European regulations and standards that the RGC should follow when drafting the Law, the following case study is offered as a potential example of domestic legislation to Cambodia.

Case study 2: Germany

Germany is an EU State whose information regulation and freedom, both online and off, on the whole, manages to balance the need to combat cyber-crimes while respecting the right to freedom of expression and information. Germany scored 17 out of 100 points (with zero being the best score) and has a status of "Free" in Freedom House's 2013 Freedom on the Net and Press Freedom indexes.[62] Article 5 of the German Constitution (Basic Law) protects freedom of expression, opinion and the press, with the stipulation that the provisions of general laws, the protection of youth and the protection of one's personal honor can limit those freedoms. Article 10 protects the privacy of letters, post and telecommunications but may be restricted for the purpose of upholding democracy and national security. Article 18 stipulates that whoever abuses any of the following rights in order to attack the free democratic order forfeits those rights: freedom of opinion, freedom of the press, freedom of association, privacy of mail and telecommunications, property or right of asylum.

Unlike the severe censorship of traditional Cambodian media, there is no systematic censorship in the German press. Freedom House notes in its 2013 Freedom on the Net report that there were no publically known instances of censorship on websites by the State in 2012 or 2013.[63] The German Press Council has drawn up a "German Press Code" (*Pressekodex*) which sets out rules of conduct and publishing principles and seeks to strike a balance between public interest and the protection of personal rights.[64] The 2012 Act on Strengthening Press Freedom protects journalistic sources and sets high barriers for searching and seizing journalistic properties. Online journalists are subject to the same protections as offline journalists but a distinction is drawn between online journalists and bloggers by only issuing press cards to full-time journalists.

Online content does have some restrictions, however. The Interstate Treaty on the Protection of Minors in Broadcasting ("JMStV") bans content online that is also outlawed by the criminal code,

[60] Ibid, paragraph 39.
[61] Ibid, paragraph 81.
[62] Freedom House, 'Freedom of the Press: Germany' (2013) http://bit.ly/1d4N26L; Freedom House, 'Freedom on the Net: Germany' (2013) http://bit.ly/1hJ5vPc.
[63] Freedom House, 'Freedom on the Net: Germany' (2013).
[64] Pressekodex (12 December 1973) http://bit.ly/1k4cbYB.

restricting content glorifying violence and requiring age verification systems before adult-only content can be viewed.[65] Some online information is prohibited for the protection of children from extreme left-wing and right-wing groups; generally this is clearly defined in law and is legally unambiguous.[66] Access to other forms of online media is occasionally blocked, but not repeatedly, where the State can provide specific reasons, supported by legislation, as to why these websites have been blocked and where any affected persons can file a complaint.[67] Restrictions on dissemination of content follow Article 130 of the German Criminal Code, for example content in support of National Socialism and holocaust denial, which is an offense because expression of such opinion dishonors the Jewish dead. However, ISPs and intermediaries are protected from liability via Article 8 of the Telecommunication Media Law, which explicitly states that providers are not responsible for content posted by others unless content transmitted violates reasonable audit requirements or when the intermediaries collaborate with users in unlawful behavior.

Nevertheless, there have been some concerns regarding Germany's cyberspace regulations. In 2007, a complaint was filed at the Constitutional Court of the Federal Republic of Germany by more than 30,000 Germans seeking a ruling on the constitutionality of legislation[68] mandating that internet providers document traffic for at least six months in the event that this could be used to combat terrorism. In March 2010, the legislation was ruled as unconstitutional for violating personal rights and the rights to communicate.[69] In 2011, the Federal government found itself in trouble again for breaching the privacy of its citizens. It established a cyber-defense center operating under the auspices of the Federal Office for Information Security, which frequently monitors online chat rooms and other public websites and has on occasions uploaded a "Trojan" onto a suspect's personal computer, a form of spyware which enables them to track all data entered onto that device.

Conclusion

The way the Law is drafted will have a broad impact on freedom of expression in Cambodia in the long-term. The RGC must ensure that the draft Law complies with both the RGC's obligations under international law and with EU standards regulations related to cyber-crimes, in order to ensure that freedom of expression, protected under the Constitution and the UDHR, the ICCPR, and other human rights instruments to which Cambodia is a signatory, is respected both offline and online.

Ensuring civil society participation

Internet legislation, regardless of the country-specific context, is complex and thus drafting any cyber law must be an inclusive and lengthy process. A multi-stakeholder model of internet governance needs to be preserved and enhanced so that it is truly representative of the public interest. As such, CCHR recommends that, before drafting the law, the RGC should:

- Publically and widely publish drafts of the Law to allow for genuine consultation with sufficient time for analysis and comments on the draft by relevant stakeholders, including CSOs;

[65] Ibid.
[66] Sawatree Suksri et al, 'Situational Report on Control and Censorship of Online Media, Through the Use of Laws and the Imposition of Thai State Policies' (December 2010) p.21.
[67] Ibid, p.22.
[68] Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (December 2007).
[69] Ibid, p.23.

- Ensure that sufficient time is taken to draft the law; sufficient time must be provided for lawmakers, CSOs and technical experts to read drafts and provide feedback, as well a period to address these concerns; and
- Establish an open forum or national congress for internet users in order to let CSOs, human rights activists, bloggers, individuals who work with new media, ISPs and programmers discuss their needs and raise their concerns with the RGC; their input should inform the contents of the new Law.

Protecting freedom of expression

There are many aspects of regulations that must be considered in order to ensure that the law is not excessive or unlawful in its restrictions, and provides for "the adequate protections of human rights and liberties." There is often a tension between the need to draft effective internet regulation and the danger of violating basic human rights in the process. As such, CCHR recommends that the RGC:

- Clearly and explicitly state the extent of restrictions made through the Law; content that is going to be deemed "illegal" in the draft Law must be narrowly and unambiguously drafted and define so as to avoid the possibility of abusive interpretation and any content restriction must be exceptional and absolutely necessary;
- Strictly limit content prohibitions to child pornography; to direct and indirect incitement to genocide; to advocacy of national, religious or racial hatred constituting incitement to discrimination, hostility or violence; and to incitement to terrorism;
- Establish an independent working group made up of (*inter alia*) technical experts, members of CSOs and academics to properly investigate and analyze website content prior to prosecution or blocking requests and before it is forwarded to the judiciary;
- Provide effective privacy and data protection, to be subjected to a rigorous set of criteria to prove that it meets international privacy standards; and
- Develop a thorough training mechanism for officials to interpret, apply and enforce the Law.

Fostering regional and international cooperation

As noted in the Budapest Convention, in recommendations and principles issued by the Council of Europe's Committee of Ministers and in the EU's Cyber Security Strategy, international co-operation is necessary in order to address the growth in cyber-crimes and, consequently, to ensure individual users' privacy and freedom on the internet. As such, CCHR recommends that the RGC:

- Ratify the Budapest Convention;
- Seek assistance from the EU and other partners to build law enforcement capacity and to reinforce co-operation mechanisms; and
- Promote international cooperation between ASEAN member states to implement and enforce multi-jurisdictional internet legislation which conforms to EU principles.

For more information, please contact CCHR Freedom of Expression Project Coordinator Sorn Ramana via telephone at +855 (0) 1765 5591 or e-mail at ramanasorn@cchrcambodia.org or CCHR Consultant Juliette Rousselot via telephone at +855 (0) 1535 0620 or e-mail at julietterousselot@cchcambodia.org.