HAUT-COMMISSARIAT AUX DROITS DE L'HOMME • OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS
PALAIS DES NATIONS • 1211 GENEVA 10, SWITZERLAND
www.ohchr.org • TEL: +41 22 917 9359 / +41 22 917 9407 • FAX: +41 22 917 9008 • E-MAIL: registry@ohchr.org

**Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression**

REFERENCE: OL
CHN 7/2015:

4 August 2015

Excellency,

I have the honour to address you in my capacity as Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression pursuant to Human Rights Council resolution 25/2.

In this connection, I would like to bring to the attention of your Excellency's Government information I have received **concerning the draft Cybersecurity Law.**

First of all, I would like to refer to and commend your Excellency's Government's commitment, expressed during its second cycle of the Universal Periodic Review in October 2013, in which it accepted recommendations to remove a number of restrictions on the freedom of expression. In particular, the UPR included commitments to make further efforts towards safeguarding the freedom of expression of all citizens (recommendation 186.54); reform legislation and law enforcement in order to ensure freedom of opinion and expression, including on the internet (recommendation 186.155); undertake measures enabling unrestricted use of the Internet by all members of the society (recommendation 186.161); and carry out judicial and administrative reform with a view to ratifying the International Covenant on Civil and Political Rights (recommendations 186.3 – 186.10, 186.14) (A/HRC/25/5/Add.1).

With regards to the draft Cybersecurity legislation, I welcome the inclusion of specific mechanisms in the law to ensure security of network products and services, network operations and network data and information, as well as the establishment of a public complaint system. However, I am nonetheless concerned that the draft contains a number of provisions which appear to unduly limit the right to freedom of expression and opinion in China, in particular, access to the internet. These restrictions include curbing users' anonymity rights, granting authorities broad powers in response to a wide variety of alleged threats, rigorous governmental monitoring and oversight of private networks, and stipulating that data must be stored in China.

In a spirit of co-operation and dialogue, and in line with the mandate entrusted to me by the Human Rights Council to protect and promote the right to freedom of opinion and expression, **I would like to bring to the attention of your Excellency's Government the concerns outlined in the attached annex**.

As it is my responsibility under the mandate of the Human Rights Council and reinforced by the appropriate resolutions of the General Assembly, to seek to clarify all cases brought to my attention, I would welcome any additional information or clarifications from your Excellency's Government on measures taken to ensure the compliance of the draft Cybersecurity law with China's obligations under international human rights law, particularly with regard to the right to freedom of opinion and expression.

I would like to add that the comments contained in the attached Annex do not imply that I have no concerns regarding other aspects the legislation to which the comments are not addressed. The issues highlighted strongly implicate the concerns under my mandate. I would be pleased to discuss the draft legislation in more detail with your Excellency's Government at your convenience.

I would also like to inform your Excellency's Government that I intend to publicly express my views on the draft legislation shortly. The press release will indicate that I have been in contact with your Excellency's Government to clarify the issues in question.

I further take this opportunity to reiterate that the right to freedom of opinion and expression, including the right to freely express opinions and to access information, as well as through the media and the Internet, is of central importance in the effective functioning of a democracy.

Your Excellency's Government's response will be made available in a report to be presented to the Human Rights Council for its consideration.

While awaiting a reply, I urge all relevant authorities in China to take all necessary measures to ensure the full compliance of domestic legislation with international human rights norms and standards, in particular revoking the legislative provisions, regulations, administrative and other measures that impose undue restrictions to the legitimate exercise of the right to freedom of opinion and expression.

Please accept, Excellency, the assurances of my highest consideration.

David Kaye
Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

## Annex

People's Republic of China Cybersecurity Law (Draft)
Pending Before the 12th National People's Congress

Comments Provided by David Kaye, the United Nations Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression

According to information received by the Special Rapporteur,

On 24 June 2015, at its 15th meeting, the Standing Committee of the 12th National People's Congress (NPC) had its first reading of the draft "People's Republic of China Cybersecurity Law." The draft law, which the Special Rapporteur has read in translation, aims to "ensure network security, preserve cyberspace sovereignty, national security and societal public interest" in addition to "protecting the lawful rights and interests of citizens, legal persons and other organizations" (article 1). The Special Rapporteur understands that the NPC has opened a period of public comments until 5 August 2015. Accordingly, I wish to submit the following comments on the draft legislation and respectfully to share these concerns directly with the Government.

*(i) Lack of user anonymity*

Article 20 of the draft law provides that "network operators … shall require users to provide real identity information when signing agreements with users or confirming provisions of services. Where users do not provide real identify information, network operators must not provide them with relevant services."

A stringent real name registration requirement impedes online privacy, which is important as a gateway to freedom of opinion and expression. Articles 19 of both the Universal Declaration on Human Rights (UDHR), and the International Covenant on Civil and Political Rights (ICCPR) to which China is a signatory, provide for the right to hold opinions without interference and the right to freedom of expression, which entails the freedom to seek, receive and impart information and ideas of all kinds through any media and regardless of frontiers. Article 17 ICCPR also provides for the rights of individuals to be protected, inter alia, against arbitrary or unlawful interference with their privacy and correspondence and provides that "everyone has the right to the protection of the law against such interference or attacks."

Online anonymity can provide individuals with a limited private space to hold opinions, exercise freedom of expression and seek accountability or transparency from the State without arbitrary and unlawful interference. As it stands, the provisions in article 20 of the draft legislation may effectively force network operators to deny access to service to those users who refuse to provide their real names for legitimate reasons. Moreover, real name registration may also increase the risk of identity theft and leakage of personal data

as well as producing a "chilling effect" on those who may be reluctant to express their opinions online because of personal safety concerns.

I would like to take this opportunity to refer to your Excellency's Government to paragraph 9 of the 2015 report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression relating to the use of encryption and anonymity in digital communications, where I note that "anonymity may liberate a user to explore and impart ideas and opinions more than she would using her actual identity." As such, in paragraphs 59-60 of this report, I have recommended that "States should promote strong encryption and anonymity [and] national laws should recognize that individuals are free to protect the privacy of their digital communications by using encryption technology and tools that allow anonymity online." Furthermore, I have recommended that States should "refrain from making the identification of users a condition for access to digital communications and online services" (A/HRC/29/32).

*(ii) Data collected in China must be stored in mainland China*

Article 31 of the draft legislation provides that "critical information infrastructure operators shall store citizens' personal information, and other important data gathered and produced during operations, within the mainland territory of the People's Republic of China."

From this provision, is not clear exactly what data, for example, personal data or routine business data, in addition to how much data, is to be kept within China. Article 65(5) of the draft law defines "citizen's personal data" as including "all other kinds of data from which a citizen's identity may be determined, either by itself or combined with other data." An extensive collection of such may curb free expression, which is incompatible with the spirit of article 19 ICCPR. As I have noted in paragraph 55 of my report (A/HRC/29/32), "a State's ability to collect and retain personal records expands its capacity to conduct surveillance and increases the potential for theft and disclosure of individual information."

In addition, according to article 43 of the draft, the storage and transfer of Chinese citizens' personal information is subject to the evaluation and authorization of the relevant Government authorities, who are legally authorized to order technology companies to stop the transmission of illegal content or block their transmission from overseas. As such, foreign operators may be reluctant to operate in China under such restrictions, which in turn, may limit the expression of speech to domestic platforms.

*(iii) The government's broad discretion*

Although article 9 of the draft law "promotes widespread network access [and] raises the level of network services," it also specifies the "lawful and orderly dissemination of network information." A troubling aspect of this provision is that the language is so broad that it risks overreaching its application and thus licensing future abuse. The emphasis in article 9 to "observe public order and respect social morality", "not endanger network

security", nor use the network to "engage in activities harming national security", "disseminat[e] obscene … information," "slander or defame others" or "upset social order" is problematic as individuals cannot reasonably expect to know which conduct would violate this article. In fact, the wording of this article is such that almost any activity could potentially be construed as "harming national security". The Human Rights Committee has stated in its General Comment No. 34 that to be characterized as a 'law', a norm "must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly." A law must provide "sufficient guidance to those charged with their execution to enable them to ascertain what sorts of expression are properly restricted and what sorts are not."

Similarly, under article 50 of the draft law, authorities have broad powers to "take temporary measures regarding network communications in certain regions, such as restricting it", in the interests of "protect[ing] national security and social public order" or in relation to other "major security interests."

Any restrictions on expression, including restrictions that strongly implicate expression, must be consistent with article 19(3) ICCPR, i.e. be provided by law, serve a legitimate government interest, and be necessary in a democratic society. Allowing authorities to have broad discretion to shut down internet communication in response to threats is incompatible with article 19(3) ICCPR. As I have noted in paragraph 32 of my report (A/HRC/29/32), any proposals to impose restrictions on encryption or anonymity "should be subject to public comment and only be adopted, if at all, according to regular legislative process. Strong procedural and judicial safeguards should also be applied to guarantee the due process rights of any individual whose use of encryption or anonymity is subject to restriction. In particular, a court, tribunal or other independent adjudicatory body must supervise the application of the restriction."

The importance of internet communications as a means to express and share information and opinions, or seek emergency assistance, particularly during times of crises, cannot be undermined. Furthermore, linking the issue of access to internet communications and, by extension, the right to freedom of opinion and expression to the issue of national security in this legislation not only gives the Government wide-ranging powers to maintain social order when deemed necessary, but also effectively codifies these restrictions. This is inconsistent with international legal principles and poses a significant potential threat to freedom of opinion and expression.

In paragraph 60 of the report analyzing the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression (A/HRC/23/40), the previous Special Rapporteur noted that "the use of an amorphous concept of national security to justify invasive limitations on the enjoyment of human rights is of serious concern." He stated that "the concept is broadly defined and is thus vulnerable to manipulation by the State as a means of justifying actions that target vulnerable groups such as human rights defenders, journalists or activists. It also acts to warrant often unnecessary secrecy around investigations or law enforcement activities, undermining the principles of transparency and accountability."

In paragraph 60 of my 2015 report (A/HRC/29/32), I have recommended that "States should avoid all measures that weaken the security that individuals may enjoy online, such as backdoors, weak encryption standards and key escrows. Court-ordered decryption, subject to domestic and international law, may only be permissible when it results from transparent and publicly accessible laws applied solely on a targeted, case-by-case basis to individuals (i.e., not to a mass of people) and subject to judicial warrant and the protection of due process rights of individuals."

*(iv) Intensive government inspections, monitoring and oversight*

Article 40 of the draft legislation obliges internet service providers to actively monitor and report on user activity and delete forbidden content in order to prevent this information from spreading. Article 25 refers to "measures for establishing security safeguards for, inter alia, "critical information structures", military and government affairs networks, and other entities such as radio and television broadcasters. These provisions may prove especially problematic for journalists. If authorities are directly or indirectly monitoring their communications, sources may not wish to provide information regarding potential human rights violations for fear of personal risk. As I have noted in paragraph 12 of my report (A/HRC/29/32), "journalists, researchers, lawyers and civil society rely on encryption and anonymity to shield themselves (and their sources, clients and partners) from surveillance and harassment."

Article 28 of the draft law further specifies that network providers are required to "perform security background checks" on personnel, "periodically conduct network education" and "formulate emergency response plans for network security incidents" among other obligations, and fines are imposed if operators do not perform these duties. Although the above-mentioned duties are not clearly defined, failure to comply with them under article 51 of the draft legislation may incur fines of up to RMB 1,000,000 for large-scale network operators and RMB 100,000 for their management personnel who are held to be directly responsible for this non-compliance.

Similarly, in accordance with article 59 of the draft law, failure to report network security risks and/or refusal or obstruction of government supervision or inspection could result in a fine of up to RMB 500,000 for network operators and up to RMB 100,000 for personnel who are found to be directly liable. These references to penalties are incompatible with article 19 ICCPR and could create a deterrent effect which may be used against the media and restrict its freedom of expression on particularly sensitive subjects. In addition, fines imposed on smaller companies could be detrimental and lead to their closure. Additionally, these penalties do not meet the proportionality requirement of article 19(3) ICCPR, as they are not proportionate to the activities they are designed to sanction.