

Freedom of Expression and Opinion in the People's Republic of China and the Internet

Per Sevastik^{*}

1 Introduction	254
2 Human Rights in China	255
3 Freedom of Expression	258
4 Freedom of Expression and the Internet in China	259
5 Self-regulation and State Secrets	260
6 Means of Censoring the Web	263
7 The Golden Shield Project	267
8 Circumventing Censorship – Virtual Private Networks (VPNs) and The Onion Router (TOR)	269
9 Conclusion	270

* LLM University of Stockholm, LLM Harvard Law School '90, Ph.D. University of Uppsala 2002, has been appointed Guest Professor at Peking University Law School teaching Human Rights in 2006-2007, 2009-2012 and is currently working with human rights and rule of law related issues at the Swedish International Development Cooperation Agency (SIDA).

1 Introduction

The authoritarian government in the People's Republic of China (PRC) has controlled social media since the Tiananmen Square Massacre in 1989, and today the Chinese government has a firm grip over the Internet through sophisticated filtering systems and "fire walls". The echo of the Arab Spring did thus not effectively reach Beijing; neither does the discussion reach Beijing whether communications surveillance should be regarded as a highly intrusive act that potentially interferes with the rights to freedom of expression and privacy and that threatens the foundation of a democratic society. Any such discussion in China today is dismissed as groundless and any critique against China is reversed, with the comment that any state should look at "their own situation first" before they criticize the affairs of other countries.¹

The purpose with this article is not to comparatively assess conditions between countries in the area of communication surveillance or freedom of expression and opinion, which is a timely topic. Neither is it to assess countries' attempts to stop whistle blowers that are said to hurt their own countries' "national interests". Nor is it about assessing the US National Security Agencies (NSA), or the British intelligence agency's Government Communications Headquarters (GCHQ) net espionage. It is more about assessing the situation in the PRC that lacks the foundation of a democratic society and where any discussion on the Internet that threatens the power of the government is censored. However, even though the Chinese government has had a firm grip on, and controlled social media, the view of the Web in general is that it is more difficult for the Communist Party of China (CPC) to contain demonstrations as activists can turn to the country's Twitter-like micro blogs to spread information faster than it in reality can be blocked. China has one of the most dynamic Web user communities in the world, which also makes the country the fastest growing Internet community in the world, and possibly also the most difficult one to control. There is an estimated 618 million people active on social media in China today and the country's top ten sites actually have 3.2 billion individual accounts. The volume of social sharing went up by 60 per cent in 2012 alone.²

This article looks into the human rights situation in China in general, before going into the interrelated issue of freedom of expression and the Internet in China. What means are taken to control the Internet and what explanation does the CPC use to explain to the public why information is quelled? These are some of the issues addressed in this article.

1 "www.nytimes.com/2013/06/26/world/asia/china-united-states-snowden.html?_r=0".

2 "www.techinasia.com/2013-china-top-10-social-sites-infographic/".

2 Human Rights in China

The current 1982 Constitution of China has been amended four times, in 1988, 1993, 1999 and 2004. The term “human rights” was first introduced into the Constitution through the 2004 constitutional revision, where it is made clear that the “[s]tate respects and safeguards human rights”.³ The term was hardly ever used before the constitutional revision in 2004 and was ironically only officially used after the June 4 Tiananmen Square Massacre in 1989.⁴ However, after the State Council issued its first white paper, *Human Rights in China*, in 1991, the term is being used more often by government officials and by the Chinese media.⁵ It should be kept in mind that during the Chinese Cultural Revolution (1966–1976) the Ministry of Justice was dismantled and reestablished first in 1978, which is also when legal education was resumed in the country. Today China has some 630 law schools with varied quality and resources. Public international law is part of these schools’ curriculum today and in approximately 60 schools human rights education is conducted.⁶ However, it is necessary to underline that in the case of human rights education there is still a preference to focus more on economic, social and cultural rights and also a trend to downplay the universality of human rights.⁷

China’s real engagement with the United Nations (UN) began in 1971 when UN membership was transferred from the Taiwan based “Republic of China” to the People’s Republic in Beijing.⁸ While the development of human rights in China is a rather recent phenomenon, there has without a doubt been a swift development within the area of human rights, regardless of the fact that considerable work remains to be done in order for China to touch base with international acknowledged human rights standards. China has ratified over 20 human rights instruments,⁹ participated in the drafting of new instruments,

3 See Article 33 of the 1982 Constitution.

4 Jianfu Chen, *Chinese Law: Context and Transformation*, Leiden 2008, p. 130.

5 Since then updated versions of White Papers on Human Rights have been issued in 1995, 1997, 1999, 2001, 2004, 2005 and 2010. All White Papers are available from: “english.gov.cn/official/2005-08/17/content_24165.htm” last visited 28 December 2012. There are currently in total 85 White Papers and a span of titles, for example, *Diaoyu Dao, an Inherent Territory of China* (2012); *Common Prosperity and Development of All Ethnic Groups* (2009), and *Sixty Years Since Peaceful Liberation of Tibet* (2011).

6 R. Smith and G. Bai, *Creating a Culture of Human Rights Education in China*, “rwi.lu.se/wp-content/uploads/2012/04/Human-Rights-Education-in-China-Smith-and-Bai.pdf”.

7 C. Tomuschat, *Human Right Between Idealism and Realism*, second edition, OUP 2008, pp.78-79.

8 GA Res.2758 (XXVI), Resolution on the Restoration of the Lawful Rights of the People's Republic of China in the United Nations Adopted by the 1967th plenary session of General Assembly on 25 October 1971.

9 Among the Core UN Conventions this includes the ICESCR 1966, (ratified 27 June 2001); the ICERD (ratified 28 Jan. 1982); the CEDAW (ratified 3 Dec. 1981); the CAT (ratified on 3 Nov. 1982); the CRPWD (1 Aug. 1988) and the CRC (ratified 1 Apr. 1992) along with the OP-CRC-CS (ratified 3 Jan, 2003) and the OP-CRC-AC (ratified 20 Feb. 2008). In

engaged in multilateral, regional, and bilateral dialogues on human rights issues and hosted a number of important human rights meetings.¹⁰ China has also enabled visits from monitors such as the Special Rapporteur on Freedom of Religion and Belief,¹¹ the Working Group on Arbitrary Detention,¹² the Special Rapporteur on the Right to Education,¹³ and the Special Rapporteur on Torture.¹⁴ China adopted a Human rights Action Plan 2009–2010 and has recently adopted a second, new National Human Rights Action Plan (2012–2015), where it is made clear that: “China still confronts many challenges in its development of human rights cause and China still has a long way to go before it attains the lofty goal of full employment of human rights.”¹⁵ The first Action Plan expresses support for the universality of human rights, but the new one has taken steps backward. The new Action Plan makes clear that “China’s national conditions and new realities to advance the development of its human rights cause” have to be on a “practical basis”. The vague principle of practicality referred to in the new Action Plan weakens the principle of universality and gives the government the option to bypass obligations that appear to be not so practical for the government to implement. The new principle appears to be another reiteration of the government’s justification that China’s “national conditions” do not allow for participatory politics. The new Action Plan is also silent on the issue when China intends to ratify the International Covenant on Civil and Political Rights (ICCPR) and its two Optional Protocols. Lacking democracy and rule of law, ratification of the ICCPR in China would imply a profound change in its constitutional system and would also have a considerable impact on the legal and political system in the country. There is currently no provision dealing with the domestic application of human rights treaties in China today, and it is therefore unclear whether international human rights treaties can be applied in Chinese courts.¹⁶

addition it has signed but not yet ratified the ICCPR (signed in 5 Nov. 1998). China has not ratified the CPED and CRMW.

- 10 Information Office of the State Council, Progress in China’s Human Rights Cause in 2012, “news.xinhuanet.com/english/china/2013-05/14/c_132380706.htm”.
- 11 E/CN.4/1995/1991.
- 12 E/CN.4/2005/6/Add.4.
- 13 Report Submitted by the Special rapporteur, Katarina Tomasevski (E/CN.4/2004/45/Add.1).
- 14 Report of the Special Rapporteur on torture and other cruel, inhumane or degrading treatment or punishment, Manfred Nowak – *Mission to China* (E/CN.4/2006/6/Add.6).
- 15 *National Human Rights Action Plan (2012-2015)*, China Daily, June 12, 2012, this is the second Human Rights Action Plan in China, the first was only valid for a year 2009-2010.
- 16 R. Gong, *The Status in China of Human Rights Treaties*, The Bulletin of Kyoto Human Rights Research Institute, No. 13, March 2008, p. 33; Björn Ahl, *Statements of the Chinese Government before Human Rights Treaty Bodies: Doctrine and Practice of Treaty implementation*, Australian Journal of Asian Law, Vol. 12, No. 1. (2010), pp. 82-105.

China has also for a number of years held regular dialogues on human rights related issues with nearly 20 countries. These dialogues have, however, weakened in character, changed name in some cases to “consultations” and the only ongoing human rights dialogue is the one that China holds with the United States (US)¹⁷ and the European Union (EU). The EU-China Human Rights Dialogue has, with short interruptions, taken place twice annually since 1997. However, the overall Chinese attitude during the dialogues has been to defend sovereignty and non-interference and to “fend off the assertive attempts of Northerners to use human rights to bring legalism and modernity to their societies”.¹⁸ A natural explanation for the lack of success in the dialogue is that there were no appropriate preconditions to have a fruitful EU dialogue from the outset with China since it was based “on the (false) premise that a negotiation and exchange between equal partners is taking place, while in reality part A aims at changing part B and part B knows it and does not accept it”.¹⁹

China has also had two rounds of Universal Periodic Review (UPR) at the UN Human Rights Council in Geneva (UNHRC) in 2009, and in 2013 China was criticized for not having complied with the 2009 recommendations made by the UNHRC.²⁰ Despite international criticism of China’s policies on freedom of expression, rule of law, suppression of ethnic minorities, and labor re-education camps²¹ and “black-jails”, China was elected unopposed to the UNHRC in November 2013. The UN General Assembly voted for China to join Cuba, Russia, and Saudi Arabia, among others, for a three-year term (2014–2016) on the 47 nation Council.²²

17 Press Conference Following U.S.-China Human Rights Dialogue, August 2, 2013, “www.state.gov/j/drl/rls/rm/2013/212667.htm”.

18 Global Times, 2013-9-17, “www.globaltimes.cn/content/812173.shtml”, see also Katrin Kinzelbach and Hatle Thelle, *Taking Human Rights to China: An Assessment of the EU’s Approach*, The China Quarterly, Vol. 2005, March 2011, pp. 60-79.

19 Id., pp. 60-79.

20 *Note on China’s Progress Since the 2009 Universal Periodic Review*, Submitted by Human Rights in China, November 2011 at “www.upr-info.org/followup/assessments/session17/china/China-HRIC.pdf”.

21 However, see China abolishes reeducation through labor. The bi-monthly session of the Standing Committee of the National People’s Congress (NPC) adopted a resolution to abolish legal documents on “laojiao” (reeducation through labor) posted on Saturday 28 December 2013, “news.xinhuanet.com/english/china/2013-12/28/c_133003042.htm”; While the government has provided no details about what it intends to do, it is not likely that the re-education archipelago — an estimated 350 labor camps with about 160,000 inmates — will be closed anytime soon, see “www.nytimes.com/2013/01/30/opinion/global/re-education-revisited.html?_r=0”.

22 “www.un.org/en/ga/68/meetings/elections/hrc.shtml”.

3 Freedom of Expression

Within a relatively short period of time, progress has been made at the international level in terms of securing respect for the right of freedom of expression. This has mainly been achieved through the establishment of the United Nations and the term “human rights” that was referred to in the UN Charter of 1945. The pathway of securing human rights has gone through a number of international and regional human rights instruments. The normative structure that safeguards these rights is found in the 1948 Universal Declaration of Human Rights (UDHR), the 1966 International Covenant on Civil and Political Rights, and a number of regional instruments.²³ Article 19 in the ICCPR provides that everyone shall have the right to freedom of expression, which includes “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”. The reference to “other media” implies that the drafters of the Covenant had in mind to include any other technological developments that could accommodate individuals to express their right to freedom of expression. So the normative structures provided today in the ICCPR are still applicable to new global communication technologies.²⁴

Freedom of information and expression is not an absolute right and can in some exceptional cases be legitimately restricted, but they have to be narrowly drawn and specific in order to prevent abuse. Any restrictions on freedom of expression and information, as set out in Article 19(3), must pass the following three-part test. It must be provided by law, which is clear and accessible to everyone. It must protect the rights or reputation of others, or protect national security or public order (*ordre public*), or of public health and morals. It must be proven as necessary and the least restrictive means required to achieve the purported aim.²⁵ Freedom of expression can only be restricted in the most serious cases of a direct political or military threat to the entire nation – and as a result, peaceful expression is always protected.²⁶ Even when the reason to restrict is legitimately invoked, restrictions must be proportional and necessary, and must be the least restrictive means to achieve that purpose.²⁷ In addition,

23 See among others: *The European Convention on Human Rights* (ECHR), article 11, *The American Convention on Human Rights*, article 13; and *The African Charter of Human and Peoples’ Rights*, art. 9 (Elaborated by a specific declaration agreed in 2002).

24 *Report on the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Frank La Rue, A/HRC/17/27, 16 May 2011, para. 21.

25 Art 19 3, ICCPR, *see also* Human Rights Committee, general comment No. 34 on article 19 of the International Covenant on Civil and Political Right, para. 20 ff.

26 U.N. Commission on Human Right, *Report of the Special Rapporteur on Promotion and Protection of the Right of Freedom of Opinion and Expression*, U.N. Doc. E./CN.4./1996/39(1996), principle 7, para. 48; *see also* “The Johannesburg Principles on national Security, Freedom of Expression and Access of Information”.

27 U.N. Commission on Human Right, *Report of the Special Rapporteur on Promotion and Protection of the Right of Freedom of Opinion and Expression*, U.N. Doc. E./CN.4./1996/39(1996), principle 7, para. 51.

any legislation restricting the right to freedom of expression must be applied by a body which is independent of any political, commercial or other unwarranted influences in a manner that is neither arbitrary nor discriminatory.²⁸

The way that any government deals with freedom of expression and access to information is seen as an “essential test right” reflecting that government’s true human rights and rule of law related intentions.²⁹

4 Freedom of Expression and the Internet in China

According to Article 35 of the 1982 Constitution of China, citizens of the People’s Republic of China enjoy freedom of speech. However, in reality government restrictions on journalists, bloggers and Internet users in the country undermine both the Constitution and China’s international legal obligations. In 2013, sixty netizens were imprisoned in China on charges related to the content of their online expression.³⁰

The problem with the Internet in China lies in the restricted view the government has on human rights, particularly freedom of information and expression. The Information Office of the State Council, or China’s cabinet, published a White Paper on the Internet in China on 10 June 2010 where it reemphasizes that “Chinese citizens fully enjoy freedom of speech on the Internet” and that the “government is determined to unswervingly safeguard the freedom of speech on the Internet ... in accordance to the law”. The basic goal of China’s Internet administration is said to be to promote general and hassle-free Internet. At the same time the White Paper makes clear that “China advocates the rational use of technology to curb dissemination of illegal information online”. The White Paper makes it also clear that the “Internet sovereignty of China should be respected and protected and that Chinese and foreign citizens, legal persons and other organisations within Chinese territory have the right and freedom to use the Internet; at the same time, they must obey the laws and regulations of China and consciously protect Internet security”.³¹

The Chinese government presented its own internal narrative in a report titled “Concerning the Development and Management of Our Country’s Internet”, two months before the White Paper was released in the media on 29

28 Two sides of the same coin – the right to privacy and freedom of expression “www.privacyinternational.org/opinion-pieces/two-sides-of-the-same-coin-the-right-to-privacy-and-freedom-of-expression”, see also Art 17 (*Privacy*) ICCPR; M. Nowak U.N. Commentary on Civil and Political Rights CCPR Commentary, N.P. Engel Publishers 2005, p. 337 ff; UNHRC Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue A/HRC/23/40, 17 April 2013, p 8-9.

29 U.N. Commission on Human Rights, *Report of the Special Rapporteur on Promotion and Protection of the Right to Freedom of Opinion and Expression*, E/CN.4/1995/32, para. 14.

30 Reporters without borders, “Enemies of the Internet”, March 2013 Report, available from “surveillance.rsf.org/en/wp-content/uploads/sites/2/2013/03/enemies-of-the-internet_2013.pdf”.

31 “english.gov.cn/official/2005-08/17/content_24165.htm#2012, released in June 2010”.

April.³² The report described the official government vision for the “scientific, healthy, and orderly development of the Internet” in China. The report was a comprehensive strategic plan that contained risks, campaign objectives, command structures and a legislative reform agenda for how to bring the Internet under control. The report also underlined the value of the Internet as an essential propaganda tool for directing a correct public opinion, “unifying thinking” and countering “the hegemony of Western media”. The report clarified that the problems with the Internet lied in its very openness and specified that “[a]s long as our Internet is open to the public, there will be channels and means for netizens to express all sorts of speech on the Internet”.³³ The text was posted in Chinese only on 4 May 2010 on the website of the National People’s Congress of the People’s Republic of China and shortly thereafter, on 5 May, a new revised version of the text was posted on the Chinese government’s official website where revealing sections of how the government aimed at controlling the Internet were deleted.³⁴ This example shows the Chinese government’s lack of transparency and the obvious intentions to not disclose to the Chinese people how they planned to control the Internet.³⁵ One may then ask how the Internet is controlled in China.

5 Self-regulation and State Secrets

The Whitepaper on the Internet from 2010 clearly indicates that the state proactively promotes self-regulation and public supervision.³⁶ It is through the national organization called the Internet Society of China (ISC) that a series of self-disciplinary regulations have been issued. One such self-regulatory

32 *How the Chinese Authorities View the Internet: Three Narratives*, “www.hrichina.org/en/content/3240”.

33 “www.hrichina.org/en/content/3241”.

34 *Id.*, “www.hrichina.org/en/content/3241”.

35 The deleted sections found in “www.hrichina.org/en/content/3240”, include:

- description of domestic propaganda and ideological work to guide public opinion online and unify public thinking and expansion of China’s cultural soft power abroad via news and commercial channels and websites in foreign languages;
- elaboration of the guiding principles for developing and managing the Internet: Deng Xiaoping theory, the “Three Represents,” and “blaz[ing] a new trail of Internet development and management with Chinese characteristics”;
- description of the preliminary Internet information security protection system and the policy of “active defense and comprehensive prevention”;
- description of the need to construct a legal system for the Internet; and
- description of the overall allocation of responsibility and management structure that integrates regulation, supervision, industry self-regulation, and technological safeguards, and calls for a cross-department mechanism for preventing infiltration and handling harmful information from overseas.

36 *White Papers: The Internet in China* (2010), section IV Basic Principles and Practices of Internet Administration.

instrument is the “Public Pledge of Self-regulation and Professional Ethics for the China Internet Industry” which is an agreement between the Chinese Internet industry regulator and companies that operate sites in China. Once signed, web companies pledge to identify and prevent the transmission of information that Chinese authorities deem to be illegal. The White Paper enumerates a number of incidents including subverting state power, undermining national unity, infringing upon national honor and interests, inciting ethnic hatred and secession, advocating heresy, pornography, violence, terror and other information that infringes upon the legitimate rights and interests of others. According to these regulations, service providers shall use technical measures to prevent the transmission of all types of illegal information. In order to strengthen public supervision of Internet information, the PRC has established the Chinese Internet Illegal Information Reporting Centre (CIIRC) and a number of other public reporting and reception organizations exist to control the flow of information since 2004.³⁷

State control of information has been a characteristic of the PRC regulation since the founding of the People’s Republic of China in 1949. Maintaining political control is the key from which the PRC legal framework originates and in 1951 the Provisional Regulation on Protecting State Secrets was promulgated.³⁸ The Regulation stipulates that Party members as well as non-Party members have the responsibility to safeguard state secrets.³⁹ The state secrets legal framework of the PRC consists today of the 1988 Law on the Protection of State Secrets of the People’s Republic of China (State Secret Law)⁴⁰ and the Measures for Implementing the Law on Guarding State Secrets (Implementation Measures Law).⁴¹ The State Secret Law explains the meaning, scope and classification of states secrets as well as the security system and its procedures. The law is comprehensive and includes all state organs, armed forces, political parties, organisations, enterprises, institutions, and citizens which have an obligation to protect states secrets. The Implementation Measures Law expands the scope of the state secret system by providing for a retroactive classification based upon specified “consequences” and pre-emptive classification which is based upon, if disclosed, on the determination of potential harm. The state secret legal framework also includes the State

37 Id.

38 Administrative Council, 87th Administrative Affairs Meeting, Central People’s Government, Provisional Regulation on Protecting State Secrets. Signed and enacted by Zhou Enlai in June 1951.

39 For a thorough presentation, see *Human Rights in China, State Secrets: China’s Legal Labyrinth* (New York: Human Rights in China, 2007), “www.hrichina.org/public/contents/41421”.

40 Id.

41 *Measures for Implementing the Law on the Protection of State Secrets of the People’s Republic of China*, issued by the National Administration for the Protection of State Secrets, promulgated and effective on May 25, 1990.

Security Law of the PRC,⁴² Criminal Law of the PRC,⁴³ and Criminal Procedure's Law of the PRC.⁴⁴ These laws are complemented with a number of other laws and regulations that are not actually part of the state secrets legal framework, but make reference to provisions not to divulge state secrets. These references are for example found in the work of lawyers,⁴⁵ in the work of accountants,⁴⁶ and in the use of the telecommunication network.⁴⁷ The Implementation Measures Law puts primary responsibility to ICT companies operating within the country to comply with measures to protect state secrets. "State secrets" are defined as "matters that are related to state security and national interests"⁴⁸ and there are six types of state secrets enumerated in the State Secret Law: major policy issues on state affairs, building of national defense and activities of national forces, diplomatic activities related to foreign countries, as well as commitments to foreign countries, national economic and social development, science and technology, activities for safeguarding state security and investigation of criminal offences. There is also a seventh widely defined "catch-all" provision for all other matters that are classified as state secrets by the National Administration for the Protection of State Secrets of the Republic of China (NAPSS).⁴⁹ Secrets can be classified into one of three categories, "top secret", defined as "vital state secrets whose disclosure would cause extremely serious harm to state security and national interests"; "highly secret", defined as "important state secrets whose disclosure would cause serious harm to state security and national interests"; and "secret", defined as "ordinary state secrets whose disclosure would cause harm to state security and national interest".

The overall aim of using "state secrets" as a legitimate ground of restricting information creates a problem of over-classification, subjectivity and

42 *State Security Law of the People's Republic of China*, issued by the Standing Committee of the National People's Congress, promulgated and effective February 22, 1993. Official English translation available at: "www.npc.gov.cn/englishnpc/Law/2007-12/12/content_1383844.htm".

43 *Criminal Law of the People's Republic of China*, issued by the National People's Congress, promulgated July 1, 1979, amended 1997, 1999, 2001, 2002, 2005, 2006, 2009, 2011, *See* Section II, page 120, for relevant provisions.

44 *Criminal Procedure Law of the People's Republic of China*, issued by the National People's Congress, promulgated July 7, 1979, effective January 1, 1980; amended March 17, 1996, effective January 1, 1997; revised March 14, 2012, effective January 1, 2013, "www.gov.cn/flfg/2012-03/17/content_2094354.htm". Official English translation of the 1996 CPL available at: "www.npc.gov.cn/englishnpc/Law/2007-12/13/content_1384067.htm".

45 *Law on the People's Republic of China on Lawyers*, issued by the Standing Committee of the National People's Congress in 1966, amended in 2001, Art. 45.

46 *Accounting Law of the People's Republic of China*, issued by the Standing Committee of the National People's Congress in 1985, amended in 1993 and 1999, Arts. 34 and 47.

47 *Regulation on Telecommunications of the People's Republic of China*, issued by the State Council in 2000, Art. 57.

48 State Secret Law, Art. 2.

49 State Secret Law, Art. 8.

arbitrariness.⁵⁰ It is still difficult to ensure compliance with the law because what constitutes a violation of the law remains unclear.

The ambiguity of the State Secret Law is of concern given the criminal implications of state secrets violations under China's Criminal Law and Security Law. Article 111 of the Criminal Law⁵¹ provides for penalties ranging from public surveillance and deprivation of political rights to life imprisonment, depending on the severity of the act, for "[w]hoever steals, spies into, buys, or unlawfully supplies state secrets or intelligence for an organ, organization or individual" outside the territory of China. For an especially severe act that endangers national security, the Article states that individuals may receive the death penalty. Article 282 provides for up to three years imprisonment for whoever "unlawfully holds documents, material, or other objects classified as 'strictly confidential' or 'confidential' state secrets and refuses to explain their sources and purposes." The Security Law addresses similar violations in the state security context.

6 Means of Censoring the Web

The 2010 White Paper on the Internet in China indicates that the "basic goals of China's Internet administration are to promote general and hassle-free Internet". In reality, however, Internet administration is anything else than "hassle-free", but everyday netizens are not necessarily aware of the existence of a meticulously controlled apparatus architected by the CPC. Only if you are trying to access sensitive information such as Falun Gong, "human rights in Tibet", Dalai lama, "Taiwanese independence", freedom of speech, attempts to disparage the Chinese government, and a great number of other sensitive keywords and webpages – will you be aware of censorship.⁵² An attempt to retrieve any information on the "Tiananmen Square massacre" on Google.com or Google.cn will for instance only provide information about architecture and tourist information that may be needed about the Square. Some of the blocked sites include Wikipedia, YouTube, Hotmail, Facebook and Twitter. The White Paper indicates that the Chinese government wants to curb the harmful effects of illegal information on state security, public interest and children.

The Internet was introduced in China in 1994 as an inevitable tool to develop the "socialist market economy", and has since then been a supporting tool to develop the country's economy. At the same time the Internet has become a common platform and an instrument to enhance communication and

50 See supra note 39, *State Secrets: China's Legal Labyrinth* (New York: Human Rights in China, 2007), "www.hrichina.org/public/contents/41421, p. 10".

51 *Criminal Law of the People's Republic of China*, Adopted at the Second Session of the Fifth National People's Congress on July 1, 1979; revised at the Fifth Session of the Eighth National People's Congress on March 14, 1997 and promulgated by Order No.83 of the President of the People's Republic of China on March 14, 1997

52 "China Takes Aim at Western Ideas" New York Times, Aug., 19. 2013, "www.nytimes.com/2013/08/20/world/asia/chinas-new-leadership-takes-hard-line-in-secret-memo.html?_r=0&pagewanted=print".

for sharing information. Throughout this development the CPC has strived to protect its values and political ideas from becoming Westernized and from feared and destructive forces from within China. The overarching aim of the CPC is to build a socialist market economy with Chinese characteristics.

There are more than 60 laws and regulations that have been made by the Chinese government that have been implemented by provincial branches of state-owned Internet Service Providers (ISPs), companies and organizations. Basically access to the Internet in China is provided by a number of licensed providers which are controlled by the Ministry of Public Security.

Some of the key regulations forming the backbone of censorship in China today are discussed here. One of the first key regulations is the Temporary Regulation for the Management of Computer Information Network International Connection which was passed by the 42nd Standing Convention of the State Council on 23 January 1996 and updated again on 20 May 1997.⁵³ Section 3 explicitly states that “[t]he organization of the Ministry of Public Security is responsible for the security, protection and management of computer information networks and the Internet in the PRC. The Ministry is responsible for the day-to-day law enforcement operations in the PRC”. The regulation also states that “no units or individuals are allowed to establish direct international connection by themselves”. Only government-approved ISPs may offer private Internet service to citizens. The regulation provides that no “individual may use the Internet to harm national security, disclose state secrets, harm the interests of the State, of society or of a group, the legal rights of citizens, or to take part in criminal activities” or “inciting to overthrow the government or the socialist system”. The regulation requires that ISPs be licensed and that Internet information has to go through currently four approved providers: ChinaNet, GBNet, CERNET or CSTNET.⁵⁴

The Ordinance for Security Protection of Computer Information Systems is another important regulation, issued on 18 February 1994. While the first regulation was established to set out specific guidelines for Internet use, this regulation is more concerned with the enforcement of these Internet regulations and gives the responsibility for the Internet to the Ministry of Public Security.⁵⁵ The Ordinance allows for the investigation and prosecution of regulation violations. Article 4 of the Ordinance focuses on safeguarding “national affairs, economic construction, national defense, construction, and advanced science and technology” within the computer information systems.

A third regulation is the Computer Information Network and Internet Security, Protection, and Management Regulation (State Council Order 292), approved by the State Council on 11 December 1997. This regulation is the

53 G. Taubman, *A not-so world wide web: the Internet, China, and the challenges to non-democratic rule*, *Political Communication* (1998), Vol. 15, 255-272.

54 Jack Linchuan Qiu, *Virtual Censorship in China: Keeping the Gate Between The Cyberspaces* in *International Journal of Commercial Law and Policy*, Issue 4, Winter 1999/2000, pp. 1-25. Retrieved at, "citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.106.532&rep=rep1&type=pdf".

55 Bryce T. McIntyre, *China's Use of the Internet: A Revolution on Hold*, in *Telecommunications and Development in China* (Paul S. N. Lee ed. 1997)

first in the PRC to focus specifically on Internet censorship. Section 5 of the Management Regulation states the following: “No unit or individual may use the Internet to create, replicate, retrieve, or transmit the following kinds of information: Inciting to resist or breaking the Constitution or laws or the implementation of administrative regulations; Inciting to overthrow the government or the socialist system; Inciting division of the country, harming national unification; Inciting hatred or discrimination among nationalities or harming the unity of the nationalities; Making falsehoods or distorting the truth, spreading rumors, destroying the order of society; Promoting feudal superstitions, sexually suggestive material, gambling, violence, murder; Terrorism or inciting others to criminal activity; openly insulting other people or distorting the truth to slander people; Injuring the reputation of state organizations; Other activities against the Constitution, laws or administrative regulations”. The Management Regulation also sets out specific fines for infractions.

Two other key regulations, chiefly aimed at controlling and censoring news information, are the Measures on the Administration of Internet Information Services, promulgated by the State Council on 25 September 2000, and the Provisions on the Administration of Internet News and Information Services (Order of the SCIO and MII no. 37), jointly promulgated by the Information Office of the State Council and the Ministry of Information Industry on 25 September, 2005. The Measures on the Administration of Internet Information Services prevents Chinese ISPs from providing access to foreign media without government approval. Foreign news can only be provided by entities officially licensed by the State Council Information Office and from the State Council Information Agency. According to its provisions “content providers are responsible for ensuring the legality of any information disseminated through their services”.⁵⁶ The relevant department in charge has also promulgated a supporting regulation. On 29 December 2007, the Regulation on the Administration of Internet-Based-Audio-Visual Program Services was simultaneously published on the websites of the State Administration of Radio, Film, and Television (SARF) and at the website of the Ministry of Information Industry (MII). Article 7 requires operators of Internet-based audio-video program services to obtain a license for spreading audio-video programs over the Internet issued by radio, film and television authorities or are required to complete record-filing procedures as required by the regulations. The Article specifies that “no units or individuals” shall operate in Internet-based audio-video program services without obtaining the requested license. In December 2009 a large number of video-sharing websites were shut down because they were lacking a license.⁵⁷

The second regulation aimed at controlling and censoring news information is the Provisions on the Administration of Internet News and Information Services which established a news publication qualifications permission

56 Bei Feng, *Chinese Internet Censorship System*, Published on Human Rights in China, July 14, 2010, at “www.hrichina.org/en/content/3244”.

57 Id.

system. These Provisions refer to news and information related to reports and commentary on social and public affairs including politics, economics, military affairs, and diplomatic affairs, as well as reports and sudden occurrences in society.⁵⁸ The regulation divides the news websites into three categories which can operate legally. In the first category there are websites established by news entities (*e.g.* People's Daily Online operated by People's Daily, Xinhuanet operated by Xinhua News Agency, and Southern Online operated by the Southern Media Group). The second category contains news websites established by non-news-entities (*e.g.* Sina, Sohu, NetEase and Tencent). Finally there is a third category of news websites that only carry the contents of what has already been published by specific entities (*e.g.* Fangzhou Online operated by Southern Weekend).⁵⁹ Only the Information Office of the State Council has the authority to issue news publication qualification certificates.⁶⁰ The most noticeable difference between these categories of websites is that in the first category they can choose and edit news items themselves, while in the second category news websites can only reprint news that came from legitimate news sources. Websites that only carry the contents of what has already been published are strictly prohibited from reporting on news about current government affairs. Only eight websites out of a total of 430,000 in the Guangdong Province were able to obtain news qualification permits by the end of 2008.⁶¹

Regarding the Supervisory Management of the regulation, Section 4 clarifies that the Information Office of the State Council and the Information Office of the people's government of the provinces, autonomous regions, and municipalities directly under the central government shall supervise and inspect the Internet news and information services and they are expected to undertake on-site examination and produce law enforcement credentials. Not only fines can be imposed by the authorities in charge but if the circumstance is serious the respective authorities can terminate the Internet news and information services or order the entities engaging in Internet access services to stop their services.

On 28 December 2012 the Standing Committee of China's National People's Congress passed a new Decision on Strengthening Network Information Protection. The Decision expressly requires that all ISPs, other business enterprises and non-profit enterprises in China that provide website access services; handle internet access formalities for fixed telephones, mobile

58 Access to the websites of Le monde, The Guardian, Global mail, El País and Süddeutsche Zeitung were blocked in China after they and other international media reported the results of the research by the International Consortium of Investigative Journalists (ICIJ). The report was based on information about the accounts held by members of the Chinese elite in offshore tax havens to conceal the personal wealth that they had amassed. On 21 January 2014, the day that the ICIJ's findings were released Chinese Internet suffered a well-timed massive failure. See further "en.rsf.org/chine-china-censors-reports-about-elite-24-01-2014,45781.html".

59 Id.

60 Id.

61 Id.

phones, and other means of internet access; or provide information publication services to users must require their users to provide real identity information when concluding service agreements or accepting provision of services. According to this Decision all telecommunication companies must now obtain the identity of new customers who register landline, wireless or mobile phone Internet connections. This implies that all activities from the accounts can be directly traced to the account holder. The Decision applies to any Internet site, including micro-blogging sites like Sina Weibo and social chat sites and platform sharing that allow users to post information. Before this Decision was adopted, many netizens created accounts under pseudonyms to protect themselves from state persecution.⁶²

The Decision has been criticized for strengthening restrictions on the use of the Internet and it is feared that the real name requirements will have a chilling effect on the country's netizens use of the Internet to expose corrupt government officials, efforts that appear to have been quiet successful recently. But government response has been that the Decision "will help, rather than harm, the country's netizens". The State Council has previously issued nine regulations on administering the Internet and these regulations and rules will be reviewed and amended in accordance with the Decision.⁶³

7 The Golden Shield Project

In order to monitor Internet use the Ministry set up the "Golden Shield Project" (GSP) in 1998. The GSP, or as it is more commonly known as the "great Chinese firewall" (GFW), is the apparatus constructed by the CPC to censor the Chinese public's ability to access foreign information. The Golden Shield was a direct response from the CPC to the creation of the China Democratic Party (CDP), which was founded in 1998 and was banned that same year. The risk of losing influence in the political and economic arena and the fact that CDP supposedly included former students that had been active in the Tiananmen Square massacre in 1989 posed a threat to the CPC which triggered the prompt banning of the CDP. The Golden Shield is controlled by the Chinese Ministry of Public Security (MPS) and became operational in 2003. Experts have estimated that the cost of fully implementing the Golden Shield Project was UDS 800 million.⁶⁴

Day-to-day operation of the GSP is carried out by the PRC's Internet police. In 2010, approximately 30,000 Internet police officers were actively employed in the PRC. The GSP attempts to effectively screen Internet communications by utilizing five methods: the first one is Internet Protocol (IP) blocking; the

62 Library of Congress, *China: NPC Decision on Network Information Protection*, at "www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403445_text".

63 Id.

64 R. McParland, *The Free Flow of Information: Internet Law In The People's Republic of China*, at "nysbar.com/blogs/lawstudentconnection/2011/08/the_free_flow_of_information_i.html".

second one Domain Name System (DNS) filtering and redirection; the third Uniform Resource Locator (URL) filtering; the fourth packet filtering; and fifth connection reset. IP blocking is a method in which the Internet police learn the IP address of a controversial website and then work to block Internet users within the PRC from accessing the website by blocking its IP. When Internet users attempt to visit a blocked website, their computer's web browser will be rerouted to its homepage.⁶⁵

The DNS filtering and redirection is a method through which the Internet police monitor Internet user's web-based searches and actually block their viewing of certain restricted materials.⁶⁶ URL filtering is utilized by the Internet police to ban URL contact with Internet users. URL contact is third-party contact aimed at targeting the personal computers of Internet users. URL filtering is not censorship orientated, as it is used primarily to prevent malware and spyware⁶⁷ materials from entering the user's computer.⁶⁸

"Packet filtering" controls access to a network by analyzing the incoming and outgoing packets and allows them to pass or stops them based on the IP addresses of the source and destination.⁶⁹ This method is the one most commonly used by the Internet police, as it is the easiest to implement.

The final method implemented by the Internet police is the *connection reset*. This occurs when an Internet user tries to gain access to web information that had been banned. As a result, the police would shut down the user's Internet connection for a predetermined period of time. The length of time that the user's Internet would be shut down would correlate to the web information that they had requested. Logically one can assume that web information deemed more dangerous would trigger a longer shutdown period.

China also has about 50,000 police officers that not only block websites but also monitor the Internet access of individuals.⁷⁰ In addition to its massive firewall and intrusive software the Chinese government employs thousands of paid commentators who act as regular Web users to counter criticism of the government. The commentators are known as the "50-Cent Party" (*wǎngluò*

65 Id.

66 See Entensys, *Internet access control and URL filtering without hardware appliances or proxy servers*, "www.entensys.com/products/gatewall_dns_filter/" (last visited January 10, 2014).

67 *Malware* is short for malicious software and used as a single term to refer to virus, spyware, worm etc. Malware is designed to cause damage to a stand-alone computer or a networked pc. So wherever a malware term is used it means a program which is designed to damage your computer it may be a virus, worm or Trojan, see more at "www.symantec.com/connect/articles/what-are-malware-viruses-spyware-and-cookies-and-what-differentiates-them" (last visited Jan 8, 2014).

68 See *Blue Print Data, Architecting a Safer Internet*, "www.blueprintdata.com/glossary.html". (last visited Jan 8, 2014).

69 See OpenBSD, *PF: Packet Filtering*, "www.openbsd.org/faq/pf/filter.html". (last visited March 31, 2011).

70 "www.hjalmarsonfoundation.se/2012/03/china-40-000-police-officers-monitor-the-internet"..

pínglùn yuán) as they are said to be paid 50 cents for every post that steers a discussion away from anti-party content or that advances the CPC-line.⁷¹

8 Circumventing Censorship – Virtual Private Networks (VPNs) and The Onion Router (TOR)

In the PRC, many netizens have been using a Virtual Private Network in order to access certain censored websites outside China. A VPN ensures that the citizen's communications are kept private and out of the reach of the Internet police. This method has allowed netizens within the PRC to achieve a certain degree of freedom while using the Internet.⁷² But the Great Firewall (GFW) has tightened its control of Internet services that are able to secretly by-pass censorship mechanisms, which prevents citizens in China from assessing overseas content.⁷³ Both companies and netizens have become aware of the new technology deployed by the Chinese government to control the flow of information inside the country. A VPN encrypts internet communications between two points so that even if the data being passed is tapped, it cannot be read. A VPN connection from inside China to outside implies that the user's internet connection effectively starts outside the "Great Firewall" – in theory giving access to the vast range of information and sites that the Chinese government blocks. That includes many Western newspaper sites as well as resources such as Twitter, Facebook and Google. In late 2012 the Chinese government was able to discover and block the encrypted communications methods used by a number of different VPN systems. China Unicom, one of the biggest telecoms providers in China, can now shut down connections where VPNs are detected. However, VPN providers for users inside and outside of China are continuously trying to find ways to circumvent censorship by trying to stay ahead of the censors. What is going on between VPN providers and the GFW in China is often described as a cat-and-mouse game.⁷⁴

The Onion Router (TOR) anonymity network enables one to send email and instant messages, surf websites, and post content online without disclosing IP address or location. Consequently, it is widely acknowledged as an important tool for freedom of expression. TOR makes it difficult for anyone to trace internet activities back to the end-user and is designed to protect Internet privacy online. All the traffic that passes through these relays – electronically operated switches – within the TOR network gets encrypted and re-encrypted

71 See "www.newstatesman.com/politics/politics/2012/10/china%E2%80%99s-paid-trolls-meet-50-cent-party".

72 See, e.g., Thomas Crampton, Best VPN to leap China's Firewall, "www.thomascrampton.com/china/poll-result-best-vpn-to-leap-chinas-great-firewall/", (last visited Jan 11, 2014).

73 A. Charles, *China Tightens "Great Firewall" internet control with new technology*, "www.theguardian.com/technology/2012/dec/14/china-tightens-great-firewall-internet-control".

74 P. Winter and J.R. Crandall, *The Great Firewall of China: How it Blocks ToR and Why it is Hard to Pinpoint*, "www.cs.kau.se/philwint/pdf/usenix-login-2012.pdf".

multiple times until it reaches the exit node (the last computer in the TOR network). At the exit node, the last layer of encryption gets decrypted and the data is sent to the destination without revealing who the sender is.⁷⁵

According to the TOR website, TOR helps to reduce the risks of both simple and sophisticated traffic analysis by distributing transactions over several places on the Internet, so no single point can link to the user destination.⁷⁶ But the GFW has found ways to actively block access to the TOR network.⁷⁷ As the case is with the VPN, the TOR network has also been a cat-and-mouse game with the GFW where providers and users are trying to stay ahead of the censors. The first documented attempt to block TOR occurred back in 2008. But ways of circumventing censorship develop all the time, like when the TOR website is blocked when accessed over HTTP but is reachable over the HTTPS which makes it possible for users to download the TOR Browser Bundle without needing to install any software.⁷⁸ The TOR network has created a list of approximately 3,000 public relays but only few of them remain accessible today. But there are also bridges that are non-public relays, but censors continuously find ways to block TOR even when clients are using these bridges. A current method is by installing boxes in ISPs that peek at network traffic and detect TOR; when TOR is detected they block the traffic flow. To circumvent such sophisticated censorship TOR introduced obfuscated bridges.⁷⁹ These bridges use special plugins called pluggable transports which obfuscate the traffic flow of TOR, making its detection harder. To connect to obfuscated bridges you need to use the Obfsproxy Tor Browser Bundle. The bundle includes some pre-configured obfsproxy bridges but more bridges are accessible from BridgeDB.⁸⁰ This illustration indicates how dynamic and innovative this cat-and-mouse game is in reality and how likely it is that the GFW will continue to adapt their censorship technology as TOR adapts to them.

9 Conclusion

Freedom of expression is not only a Western phenomenon. It was also advocated by Confucius (551–479 BC) who did not recommend blind obedience to the ruler (the state). When Zilu asks him “how to serve a prince”,

75 *HotspotShield* by *AnchorFree*, at “www.hotspotshield.com/learn/tor-vs-vpn”.

76 See “www.torproject.org/”.

77 *Torproject.org Blocked by the GFW in China: Sooner or Later*, “blog.torproject.org/blog/torprojectorg-blocked-gfw-china-sooner-or-later”, *How China Blocks the Tor Anonymity Network*, “www.technologyreview.com/view/427413/how-china-blocks-the-tor-anonymity-network/”.

78 See *supra* note 74.

79 T. Wilde, *Great Firewall of China probes Tor SSL Sessions*, “www.zdnet.com/great-firewall-of-china-probes-tor-ssl-sessions-4010025171/”, also by the same author, *Knock Knock Knockin’ on the Bridges Doors*, Jan 7, 2012 at “blog.torproject.org/blog/knock-knock-knockin-bridges-doors”.

80 “www.cs.kau.se/philwint/pdf/usenix-login-2012.pdf”.

Confucius replies: “Tell him the truth even if it offends him.”⁸¹ It is not at all surprising that the Chinese edited version of the Analects, bought in Beijing in 2010, has omitted section 14.23, where freedom of expression is rooted. State control, censorship, limiting freedom of expression and information has been a characteristic of the CPC’s regulation since the foundation of the People’s Republic in 1949. Today, 65 years after the establishment of the PRC it appears as if the CPC is putting more emphasis to control the flow of information than trying to find ways to explain to the public why China is not complying with recognized international human rights standards. There is an overwhelming consensus today that there should be as little restrictions as possible to the flow of information and freedom of expression via the Internet. Restrictions are only permissible in a few exceptional cases, and in limited circumstances prescribed by international human rights law. The full guarantee of the right to freedom of expression must be the norm and any limitation considered as an exception, and this norm should never be reversed.⁸² When the Chinese government limits freedom of expression, decides to block a website or two, it is under no legal obligation to offer any explanation for its actions.⁸³

The 2010 White Paper on the Internet clarifies that Chinese citizens fully enjoy freedom of expression on the Internet. Likewise, the 1982 Constitution of the PRC confers on Chinese citizens the right of freedom of expression. With their right to freedom of expression on the Internet protected by law, they can voice their opinions in various ways on the Internet. It is also maintained that the Internet is an important infrastructure facility for the nation and that it is “under the jurisdiction of Chinese sovereignty”. The foreword of the White Paper on the Internet opens up grandly by describing the Internet as “[a] crystallization of human wisdom ...” , but apparently the Chinese government is not in a position to fully disclose that wisdom to the Chinese people without being able to first control the flow of information.

The view that the government intends to maintain its tight control over the Internet is also strengthened by the Chinese government’s own internal narrative in the above mentioned report “Concerning the Development and Management of Our Country’s Internet”. The incident with the two versions of the same narrative further reveals the government’s lack of transparency and the obvious intentions to not disclose to the Chinese public how they planned to control the Internet.⁸⁴

A last example disclosing the government’s intention of maintaining a tighter control over the Internet is the 28 December 2010 Decision on

81 See Analects 14.23. The Chinese edited version of the Analects, bought in Beijing in 2010, has omitted section 14.22, censorship in China has no limits.

82 Report on the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/17/27, 16 May 2011, para. 68.

83 *Internet Filtering in China in 2004-2005: A Country Study*, Opennet Initiative, “opennet.net/studies/china”.

84 See supra note 32.

Strengthening Network Information Protection.⁸⁵ As discussed earlier, although the name of the Decision implies that it aims to protect net information, it rather reveals something else. In addition to expressly requiring ISPs to obtain real-name identity information when providing internet access services and information publication services, the Decision provides that whenever ISPs find that prohibited content is being transmitted, they must stop transmitting that information, erase it, keep a record of it, and then report the incident to the government. The government response to critique that the Decision strengthens restrictions, rather than being protective, was that the Decision “will help, rather than harm the country’s netizens”. But it appears to be the other way around, that the Decision will harm the netizens rather than help them because they will not be able to create accounts under pseudonyms to protect themselves from state persecution. Real name registration requirements allow Chinese authorities to more easily detect online commentators or tie mobile use to certain individuals and by doing so eradicate anonymous expression.⁸⁶

The most obvious conclusion after this brief presentation is that the way the Chinese government deals with freedom of expression and access to information, reflects the government’s true human rights and rule of law related intentions.

85 *See supra* note 56.

86 “www.ebeijing.gov.cn/Beijinginformation/BeijingNewsUpdate/t1292298.htm.”

**The Role of European
Institutions for Promoting
Rule of Law and
Development**

