

Flygtningenævnets baggrundsmateriale

Bilagsnr.:	352
Land:	Kina
Kilde:	Reporters Sans Frontières
Titel:	Enemies of the Internet 2014 – China: Electronic Great Wall getting taller
Udgivet:	12. marts 2014
Optaget på baggrundsmaterialet:	2. juli 2014

[EN](#) | [DE](#)

- **Source:**
RSF - Reporters Sans Frontières
- **Title:**
Enemies of the Internet 2014 - China: Electronic Great Wall getting taller
- **Publication date:**
12 March 2014
- **ecoi.net summary:** Report on governmental restrictions of freedom of expression on the Internet in 2013 [ID 271425]
- **Countries:**
China
- **Original link** <http://12mars.rsf.org/2014-en/2014/03/10/china-electronic-great-wall-getting-taller/>

Recommended citation:

RSF - Reporters Sans Frontières: Enemies of the Internet 2014 - China: Electronic Great Wall getting taller, 12 March 2014 (available at ecoi.net)
http://www.ecoi.net/local_link/271425/386687_en.html (accessed 05 May 2014)



Enemies of the Internet 2014 - China: Electronic Great Wall getting taller

State Internet Information Office

China's leaders realized at a very early stage that the Internet was not just a free speech medium but also a major political challenge. To justify their oppressive censorship and systematic surveillance of the Internet and its users, they stress the need to ensure the country's stability and harmony. Although China's Internet is one of most regulated in the world, it continues to serve as an exceptional vehicle for circulating information.

Since 2011, it is the Guojia Hulianwang Xinxi Bangongshi or State Internet Information Office (SIIO) that drafts the government's directives on the dissemination and censorship of information online. It is attached to the Guowuyuan Xinwen Bangongshi or State Council Information Office (SCIO), also known as Guoxinban for short.

The head of the SCIO, Cai Mingzhao, is a former editor of People's Daily (Renminribao) and former deputy president of the official New China news agency (Xinhuashe). He is also deputy head of the Department of Communication of the Central Committee of the Chinese Communist Party (CCP) and head of the Central Committee's Office of External Communication. His predecessor, Wang Chen, another former People's Daily editor, was elected general secretary of the Permanent Committee of the National People's Congress.

China's leading propaganda agency, the SIIO is also the world's most centralized censorship office. It is in charge of approving the content circulating on the Internet and on related services. It also supervises the online dissemination of information coming from the CCP and the government. The propaganda may be disseminated by means of official blogs or by the so-called "50 Cent Party" (Wumaodang), bloggers who are recruited and paid the derisory sum of 50 cents for every post carrying pro-government information or promoting the party line.

Far from being just a censorship and propaganda office, the SIIO also performs a regulatory function, which includes supervising the allocation of IP addresses to users and the registration of sites and domains, and Internet Service Providers. In western countries, all these different informational and regulatory functions are usually handled by many different administrative entities or by the private sector.

Directives and self-censorship

The government relies heavily on both self-censorship and censorship by Internet companies. The SIIO is empowered to supervise and punish sites that do not follow the "public commitment to Internet industry self-discipline in China," a set of rules drawn up "in collaboration" with the Internet Society Of China (ISOC), an

alliance of 140 leading Internet entities. Thousands of organizations have signed this “self-censorship undertaking,” including Yahoo, Microsoft and Google.

Bloggers and journalists have a general idea of what content is permitted and what is banned, but the “red lines” that must not be crossed can change at any time. Every day, the government sends “[directives](#)” to the media specifying the subjects to be avoided and the subjects to be played up. These directives from the SIIO, or directly from the SCIO, may concern any subject, regardless of how big or small a danger the authorities may think its coverage represents.

Under such conditions, journalists themselves suppress a great deal of content. A recent directive even called for the [Reporters Without Borders press freedom index to be censored](#). While the authorities are aware that a censorship order is not enough to suppress all information on a sensitive subject, it creates obstacles and limits people to what they can find on independent sites or social networks.

The Great Firewall

The entirety of the technology used by China to control the flow of information is often referred to as the “Great Firewall” (Fanghuo Changchen), in allusion to the Great Wall of China. Launched under the name of Golden Shield and gradually installed from the late 1990s onwards, this system has benefitted from the technology, material assistance and skills of the US network equipment and security company Cisco Systems.

The censorship is based on very expensive surveillance technology that all website creators must install at their own cost. It enables surveillance of visitors to the site and rapid identification of the authors of all content, comments and messages. It also includes a system that automatically delays posts until they have been geolocated and human censors have vetted subjects and keywords. To understand how such a system works, Harvard University researchers create a pseudo-social network platform and carried out a detailed analysis of the functions and capabilities of the software used. After a supplier revealed to them that, to satisfy the Chinese government, a site must employ two or three censors for every 50,000 users, they calculated that Internet companies in China employ a total of 50,000 to 75,000 censors.

The technology has evolved quickly in recent years and the authorities now have many tools at their disposal for censoring and monitoring the most active online journalists, bloggers and cyber-dissidents.

VPNs and “obfuscated bridges”

Virtual Private Networks (VPNs) are one of the most effective ways to evade Internet censorship and surveillance (as long as you can trust the VPN’s owner). This is also true in China, where the government blocks sophisticated circumvention tools such as TOR. Nowadays, thanks to a system of “obfuscated bridges,” it is still possible to connect to the TOR network and thereby evade censorship anonymously. But few Chinese Internet users seem to be aware of this new software. It is hard for the Chinese government to block VPNs not because of their technical superiority but because they are constantly used by the major western corporations operating in China. Blocking them would cause an outcry and would reduce China’s attractiveness for entrepreneurs and investors. The censors nonetheless often render encrypted connections unusable.

Deep Packet Inspection

The government’s censorship and surveillance policies includes intensive use of Deep Packet Inspection (DPI), a form of filtering that allows closer inspection of user-generated Internet traffic. DPI is not only used to inspect content but also to slow connections to “undesirable” content and platforms such as Facebook or RWB’s website (rsf.org). According to several reports, searching for specific terms on Baidu or Google often causes a connection to slow right down and even become unusable. In 2012, Google’s Hong Kong-based Chinese-language search engine warned users against entering sensitive search strings and advised using alternatives. This advice was removed at the Chinese government’s request.

Depending on the news and the region

Since Xi Jinping became president in 2013, there have been official campaigns against corruption and online rumours. But the conduct of these campaigns is reserved for the authorities. Any lowly journalist or blogger accusing a party member of corruption is severely punished. In July 2013, [the journalist Liu Hu was charged with defamation](#). He was arrested on 23 August on charges of spreading false rumours and defamation and is still facing prosecution.

Many bloggers have been targeted by [the campaign against online rumours](#) that was launched in September 2013. According to a specially-issued legal “interpretation,” any “defamatory” online content that is viewed more than 5,000 times or re-posted more than 500 times could result in a sentence of up to three years in prison under article 246 of the penal code for the person who originally posted it. The same month, [a 16-year-old school student who questioned the actions of the police on his Weibo account](#) was detained for six days.

Internet control is reinforced whenever the authorities are particularly concerned about the possibility of unrest or protests, especially during major political events. There were [crackdowns on bloggers during the Communist Party's 18th Congress](#) in November 2012 and Xi Jinping's installation as president in March 2013.

In November 2012, even Google and Gmail were rendered inaccessible inside China. At the same time, the cyber-dissident Hu Jia's Sina Weibo account was shut down for the third time in the space of two months, while certain keywords such as "18th Congress" (十八大) or homophones were censored in Sina Weibo's search engines.

China's provinces are not all treated alike. The "autonomous regions" of Tibet, Inner Mongolia and Xinjiang are subject to much more intensive and sustained Internet censorship than other provinces. Social networks such as Twitter and Facebook are censored and using proxy servers to evade censorship is much riskier. With Internet speeds that are more than twice as slow as in big cities such as Beijing or Shanghai (less than 1.5 Mbps as against 4 Mbps), content control is much harsher, like the treatment of bloggers.

The persecution of Ilham Tohti, a prominent Uyghur academic and editor of the Uygurbiz.com website, is emblematic. The target of constant police surveillance, he was held for more than a month in [2009](#), at a time of rioting in Xinjiang. Arrested again in January 2014, [he has been held incommunicado](#) ever since on a charge of separatism, which carries a possible life sentence.

Uyghur-language sites are often blocked and, at times of unrest or rioting in Xinjiang, almost all of the most popular sites, such as [Diyarim](#), [Xabnam](#) and [Ulinix](#), are inaccessible. In a survey of websites dedicated to the Uyghur community in 2009, Reporters Without Borders found that the authorities blocked 85 per cent of the tested sites. Most displayed "connection expired" or temporary error messages, masking the fact that they had been permanently blocked.

In Tibet, filtering and surveillance software has been installed in all public places and companies with Internet connections. The Communist Party boss in Tibet, Chen Quanguo, often steps up content surveillance and censorship. In March 2012, the monitoring of phone and Internet networks was intensified and access to many Tibetan exile blogs and media websites such as [Sangdhor.com](#) and [Rangdrol.net](#) was blocked. Chen announced in November 2013 that the government would do its utmost to ensure that "only its voice is heard" and that no one received the Dalai Lama's propaganda on the Internet, TV or any other medium.

The world's biggest prison for netizens

China, which has the most sophisticated Internet censorship system, continues to be the world's biggest prison for netizens. At least 70 online information providers are currently in prison because of their Internet activities. They include Nobel peace laureate Liu Xiaobo. And at least three of the 30 currently imprisoned journalists were convicted for what they posted online.

The arrest of Liu Hu, a journalist with the daily Xin Kuai Bao (Modern Express), on 23 August 2013 is indicative of how media personnel are hounded in China. He was charged with disseminating false rumours because he used his Weibo account to urge the authorities to investigate an official for suspected corruption.

Even after release from prison, cyber-dissidents such as Ai Weiwei and Hu Jia are subject to constant harassment and surveillance, and sometimes house arrest. Hu Jia was arrested on 25 June 2013 while celebrating his birthday with friends, some of them influential bloggers. Chen Guangcheng's family has been hounded ever since he fled to the United States. Chen announced in Washington on 5 March 2013 that his jailed nephew, Chen Kegui, had been tortured in detention. Two days later, the police tried to kidnap Chen Kegui's son from a kindergarten but were prevented by Chen Guangcheng's elder brother. Liu Xia has been under house arrest ever since her husband, Liu Xiaobo, was awarded his Nobel in December 2010. Her brother, Liu Hui, was sentenced to 11 years in prison in June 2013 on a trumped-up real estate fraud charge.

The Chinese authorities try to get Internet firms to help them censor and track down dissidents. Shi Tao, a journalist and poet, paid the price in 2005. [He was sentenced to ten years in prison](#) on a charge of divulging state secrets after Yahoo's Hong Kong office provided the information that allowed the authorities to identify him as the person who had circulated an email about Tiananmen Square censorship. Since then, Yahoo's collaboration with the regime has been linked to three other cyber-dissident arrests. Yahoo said it had no choice but to comply with China's law. Unfortunately, it is not alone.

Cracks in the Great Wall?

China is constantly trying to introduce ever stricter controls on Internet use and access to international content but the exponential growth in the number of Chinese Internet users and the steadily expanding volume of content available online is stretching this censorship model to the limit. In particular, social networks such as Sina Weibo, which function as very efficient real-time information tools, are hard to censor effectively with today's resources.

President Xi Jinping was “appointed” head of a cyber-security committee on 26 February 2014. He said he wanted to turn China into a “cyber-power” but stressed that there would be no national security without cyber-security. As long as social networks keep on mocking and embarrassing officials, even questioning their position in the party, the regime will continue to adapt its technological arsenal and human resources to its censorship needs.

published on  **ecoi.net**
European Country of Origin Information Network