

The future of dissent: hacking Chinese censorship

Giovanni Navarria

20 October 2005

Should we despair at the power of an authoritarian regime to censor the most democratic force of our time? Giovanni Navarria sees a ray of hope burst through the clouds hanging over Chinese netizens.

Since the spread of the internet in the mid-nineties, privacy concerns have increased exponentially. Cyberspace has often been equated to Jeremy Bentham's Panopticon, or to a new, digital version of George Orwell's Big Brother, capable of seeing and controlling everything and everyone. This rather dystopic vision has rightly generated fear and distrust of the web. Recently, the thickening bonds between authorities and internet companies and the development of the net for political control have given new foundations to those fears. The rapidly evolving situation in China, as observed by Isabel Hilton on [openDemocracy](#), certainly shows how those fears rest upon solid ground.

With an estimated number of total users that this year has crossed the threshold of 100 million, and notwithstanding the assumption that these numbers will continue to rise rapidly, China has already become a dominant presence in the internet world, second only to the United States of America .

Overall, the impressive growth of the Chinese internet is rooted in the long term, state-driven project aiming, with the help of information technology, at the complete renewal of the economy and bureaucracy. It is also a clear attempt to give the government of

Beijing a better infrastructure for controlling the administrative processes of both near and distant provinces.

But the harnessing of information technology, and especially the internet, represents for the party leadership more than a simple economic booster. The web has become an important medium for propaganda and censorship, a powerful ally that helps the party to gain greater and steadier support from the Chinese people. Websites such as [www.xinhuanet.com](#) (the governmental news agency), and [www.chinadaily.com.cn](#) (the online version of *China Daily*), which serve millions of users every day, are perfect examples of how the Chinese authorities use the net for propaganda purposes: the content of these websites is entirely controlled by the Communist Party.

China an expanding digital Big Brother?

But according to Shanthi Kalathil and Taylor Boas, for the Chinese government, rising user figures mean "even greater challenges in balancing economic potential and political control". To defend itself from the democratic and dangerous effects of the internet – namely openness and uncensored information – China has been developing a complex system of electronic surveillance called the Golden Shield. The system is

intended to be a state-of-the-art online database combined with a unique and complex surveillance network that incorporates the whole realm of digital technology, from speech and face recognition, to credit card records, CCTV, as well as advanced internet filtering technologies.

Although the Golden Shield is still a work-in-progress, the government can already count on an estimated force of 40,000 agents allocated to its notorious internet police which has the task to patrol and polish the web, day and night. The Chinese Government seems to have acquired the power to control, oversee, and filter information flow running over the entire communications network.

In September 2002, Chinese internet users had their first taste of this control: for a whole week access to the Google search engine was entirely blocked. As a direct result of the government's new policy and increased efforts to censor the internet, free, anonymous proxy servers that helped users to break through the national firewall have now an average lifespan of just 30 minutes.

As only a small percentage of Chinese have a private connection to the internet at home, internet cafés have been at the centre of the internet revolution, and therefore they have become one of the favourite targets of the government repression. Recently, the censorship belt on the internet cafés has tightened. Swipe cards, for example, have been linked to users' ID Cards. "One café manager", wrote Paul Mooney of the *International Herald Tribune*, "showed me a back room where a police-linked computer, connected to four spy cameras, monitored users."

In the past decade many real, or often simply suspected, dissidents have been caught in the web of the internet police. Their crimes, some of which carry the death penalty, range from circulating emails with alleged top secret information, to posting messages on web forums that criticise Beijing's policy; from viewing forbidden websites, to using the web to advocate the need for a more open and democratic society.

In short, the internet boom is increasingly transforming China into a digital version of Orwell's Big Brother.

The Price of the Chinese cake

In recent years, the fast growth of its internet market – and generally speaking of its overall economy (in a

recent survey, the OECD announced that China could become the largest exporter) in the world by 2010 – has turned China into the new promised land for most internet giants. Companies such as Yahoo!, Google, MSN, and eBay are rapidly increasing their presence on the Chinese market: Yahoo is reported to have already spent more than \$1 billion; Google – with a \$7 billion bag-full-of-cash from their summer-stock sales – is not willing to leave the whole of the Chinese cake free for grab to its rivals. Meg Whitman, the CEO of the world's leading internet auction company eBay, recently said: "Whoever wins China, will win the world".

For watchdog organisations such as Reporters Without Borders "this poses the worrying question of how far those companies will go in complying with Beijing for the benefit of their investments". The recent case of Shi Tao, a journalist of the daily *Dangdai Shang Bao* (Contemporary Trade News) in Hong Kong, has surely set a frightening precedent.

With the compliance of Yahoo! Holdings, Shi Tao was sentenced to ten years in prison when he was found guilty of spreading censored material through the internet. The alleged top-secret material was a message from the Beijing government warning journalists of the "risks resulting from the return of certain dissidents on the 15th anniversary of the Tiananmen Square massacre". In other words it was a request for every journalist to keep a low-key tone – if not remaining totally silent – on the topic of Tiananmen.

In order to "spread" the top-secret material, Shi Tao sent a message to a foreign-based website through his personal – supposedly anonymous – yahoo email account. Following the recent publication of the sentence of the trial, it is now clear that Yahoo! Holdings (Hong Kong) Ltd. played a major role in Mr. Tao's conviction. The internet company provided the Chinese prosecutors with the account details of the email address (huoyan-1989@yahoo.com.cn) responsible for sending the forbidden information to the foreign website, and the IP addresses linked to both that email account and Shi Tao's computer. Without such supportive compliance by Yahoo!, it would have been impossible for the Chinese government to convict Shi Tao.

For many commentators the Shi Tao case represents the rising price Western companies are learning (and willing) to pay to increase their portion of the highly desirable Chinese cake.

Cracks in the System

So is the future of our expanding network society a bleak one? Given certain conditions – namely threats and authoritarian regimes – we might be tempted to conclude that the internet is nothing but a strong amplifier of pre-existing patterns of domination that has turned governments in an even more powerful digital Big Brother. Corroborating evidence comes from the censorship regimes of other authoritarian regimes such as Burma. From this standpoint, the network can be seen as a new infrastructure of power, rather than the handmaiden of a more democratic future.

Upon more careful examination, the reality appears to be rather different. As Hannah Arendt remarked in her 1969 essay *On Violence*, when a government starts losing control, *that* is the proof that legitimacy (people's support) has vanished. An outburst of violence or an attempt (even a successful one) to tighten further the web of censorship signals a crack in the structure of power.

The eleven commandments for the perfect internet user announced recently (see box) might be one of these cracks in the fortress of power. There is nothing really new in those rules, as Reporters Without Borders commented “[they] are certainly more intended to frighten internet-users than to codify the use of the net.” However, the watchdog organisation added that “these moves to filter the internet are a sign that the internet frightens those in power, in particular during a period of ever greater social unrest. It's noticeable that the only new elements in the text relate to banning the calling of strikes or gatherings though the net.”

Reporters Without Borders has stressed an important point. In fact, while geographical boundaries grow thinner and fade, the growing number of internet users, the sheer complexity of the global network, the intrusion of external actors and the development of new software and technology all pose a major threat to the future of any digital Big Brother.

The true problem is to understand how to multiply the quantity of those cracks in the systems.

Political Activism: Davids vs. Goliath

As a network of networks, the internet is highly resilient to any attempt of control. Clearly in the case of the single-party state of the People's Republic of China we see the strong will of a government trying to exploit the internet as a system of total control and censorship. However, that network itself becomes a

system – an unprecedented opportunity – for *breaking through* control.

In fact, the Chinese government's strong policy of protecting its network from external intrusion by using firewalls and e-police to patrol it, coupled with the growing compliance of IT companies, *still* cannot cope with the increased volume of internet traffic and with the interference of external actors. Thanks to groundbreaking software such as Ultrareach Internet, Roaming without Borders – easily available even on the Chinese internet – and proxy networks such as DynaWeb that allow users to bypass government censorship and to have secure and full access to the world wide web, China's great firewall has started losing strength. It has become *hackable*.

For instance with the help of Roaming Without Borders, millions of emails are delivered unfiltered to users in censored areas. And since 2002, when DynaWeb started operating as a free web portal for Chinese users, each day more than 20,000 unique web-surfers have gained regular, unblocked access to the internet.

Reporters Without Borders recently published a handbook for bloggers in countries such as China with heavy censorship. In it, they point out that “bloggers are often the only real journalists in countries where the mainstream media is censored or under pressure”. The idea behind the handbook was to give them “handy tips and technical advice on how to remain anonymous and to get round censorship, by choosing the most suitable method for each situation”

These advanced technologies let new forms of political activism find ways to swim through the net of Chinese censorship. “I can get any information I want” – a political dissident told the *International Herald Tribune*, smiling broadly – “A few months ago, he said, he was unable to access sensitive sites, relying on foreign friends to give him news about China.”

The work of UltraReach Internet, DynaWeb, and Reporters Without Borders represents only a fraction of the support available to political activism on the internet.

Taken one by one, these efforts could pessimistically be seen as a no-contest battle between the mighty force of the Chinese state and a microscopic, insignificant resistance. But if placed within the context of a growing network society, the perspective radically changes. One might finally see in the web a new battlefield where a giant Goliath faces a rising army of brave and bold Davids. The outcome of such a battle is everything but certain.

Being part of the network society has its price: everyone must pay it. That price is a lack of total control; it carries with it an embedded condition of weakness or openness to attack. In fact this rule applies even to a government – regardless of its powerful army and notorious e-police. Once it has fully entered the network it becomes one-among-many; in other words, a user of the network which is exposed or *hackable*. This condition of weakness or openness to

attack is the most important characteristic of the technological revolution of the last decade and it represents the growing strength and the future of political activism.

It is surely an expensive price to pay for any authoritarian regime, but indeed a welcome fee for the many supporters of democracy worldwide.

Giovanni Navarria graduated in Philosophy from the University of Catania, Italy. Since October 2003, he has been undertaking a PhD at the Centre for the Study of Democracy (CSD) at the University of Westminster, London. His research centres on the future of democracy in the digital age. His interests include the public sphere, civil society, group theory, social networks, activism, china and the network society.

This article is published by [Giovanni Navarria](#), and [openDemocracy.net](#) under a Creative Commons licence. You may republish it free of charge with attribution for non-commercial purposes following these guidelines. If you teach at a university we ask that your department make a donation. Commercial media must contact us for permission and fees. Some articles on this site are published under different terms.
