China's internet

A giant cage

The internet was expected to help democratise China. Instead, it has enabled the authoritarian state to get a firmer grip, says Gady Epstein. But for how long?

Apr 6th 2013 l From the print edition
to be stating the obvious. By its nature the web was widely dispersed, using so many channels that it could not possibly be blocked. Rather, it seemed to have the capacity to open up the world to its users even in shut-in places. Just as earlier communications technologies may have helped topple dictatorships in the past (for example, the telegraph in Russia’s Bolshevik revolutions in 1917 and short-wave radio in the break-up of the Soviet Union in 1991), the internet would surely erode China’s authoritarian state. Vastly increased access to information and the ability to communicate easily with like-minded people round the globe would endow its users with asymmetric power, diluting the might of the state and acting as a force for democracy.

Those expectations have been confounded. Not only has Chinese authoritarian rule survived the internet, but the state has shown great skill in bending the technology to its own purposes, enabling it to exercise better control of its own society and setting an example for other repressive regimes. China’s party-state has deployed an army of cyber-police, hardware engineers, software developers, web monitors and paid online propagandists to watch, filter, censor and guide Chinese internet users. Chinese private internet companies, many of them clones of Western ones, have been allowed to flourish so long as they do not deviate from the party line.

If this special report were about the internet in any Western country, it would have little to say about the role of the government; instead, it would focus on the companies thriving on the internet, speculate about which industries would be disrupted next and look at the way the web is changing individuals’ lives. Such things are of interest in China too, but this report concentrates on the part played by the government because that is the most extraordinary thing about the internet there. The Chinese government has spent a huge amount of effort on making sure that its internet is different, not just that freedom of expression is limited but also that the industry that is built around it serves national goals as well as commercial ones.

Walls have ears

Ironically, the first e-mail from China, sent to an international academic network on September 14th 1987, proclaimed proudly: “Across the Great Wall we can reach every corner in the world.” Yet within China’s borders the Communist Party has systematically put in place projects such as the Great Firewall, which keeps out “undesirable” foreign websites such as Facebook, Twitter and YouTube, and Golden Shield, which monitors activities within China. It has also worked closely with trusted domestic internet companies such as Baidu (a search engine), Tencent (an internet-services portal), Renren (China’s leading clone of Facebook) and Sina, an online media company that includes Weibo, a Twitter-like
microblogging service.

Of all these newcomers, microblogging has had much the biggest impact on everyday life in China. It has allowed the spread of news and views in ways that were not previously possible, penetrating almost every internet-connected home in China. The authorities, having blocked Twitter and Facebook early on, allowed Chinese microblogs and social-media services to develop as trusted and controlled alternatives. They grew exponentially, far beyond anything that Twitter achieved in the Chinese market.

Google, the West’s foremost search company, hesitantly tried to play by China’s rules for a while, introducing a self-censored search engine there in 2006, but eventually withdrew that service in 2010, not so much because of the restrictions imposed on it but because it was being hacked by the Chinese. China’s cyber-hackers continue routinely to break into the e-mails of dissidents as well as into the computer systems of foreign media that report sensitive stories on China’s leaders. They have recently made headlines by stealing the technology of American defence firms and probing critical American infrastructure for vulnerabilities. Numerous hacking attacks abroad have purportedly provided Chinese firms with sensitive commercial information and given the People’s Liberation Army valuable insights into other countries’ defence apparatus.

The party has achieved something few had thought possible: the construction of a distinct national internet. The Chinese internet resembles a fenced-off playground with paternalistic guards. Like the internet that much of the rest of the world enjoys, it is messy and unruly, offering diversions such as games, shopping and much more. Allowing a distinctly Chinese internet to flourish has been an important part of building a better cage. But it is constantly watched over and manipulated.

Sometimes the authorities’ efforts at controlling it are absurd, even ridiculous, but the joke is on the users. Government agencies across the country have invested heavily in software to track and analyse online behaviour, both to gauge public opinion and to contain threats before they spread, and the authorities deal ruthlessly with those who break the rules. In 2009 Liu Xiaobo, a Chinese writer, was sentenced to 11 years in prison for co-writing an online manifesto calling for an end to authoritarian rule and asking for signatures in support. At the time few in China had heard of Mr Liu, a much-jailed democracy activist, and not many saw the declaration. He became famous outside China when he was awarded the Nobel peace prize in 2010 but is still largely unknown within the country because of strict censorship (his name is among a huge and growing number of “sensitive keywords” which are blocked online).
Also in 2009, after riots in Xinjiang, a remote north-western region, the authorities shut off the area’s internet from both the rest of China and from the world. By flipping an internet “kill switch”, they isolated the area for almost a year. And in March 2012, when social media carried rumours of an attempted coup in Beijing, the government temporarily shut down some of the internet’s microblogging services and detained six people.

Wobbling Jell-O

Will the Chinese state be able to go on controlling, manipulating and hacking the internet indefinitely? There are reasons to think it will not. When Mr Clinton made his famous remark about nailing Jell-O to the wall, only 20m people in China were online. Now the cage strains to hold in excess of 560m, almost as many as the online population of North America and Europe combined. The fastest growth in internet use is in China’s poorer, more rural provinces, partly because of a surge in users connecting via mobile devices, which now outnumber those connecting from computers. The internet is no longer confined to an urban, educated and relatively well-off public. Most farmers are getting online to listen to music, play mobile games and check the weather, not blog dissent. But even casual users can be drawn into political debates online, and the internet is one place where people can speak their minds and criticise the government relatively freely.

In private they have always grumbled, and families at their dinner tables have scoffed at the propaganda served up on state-run television. But being able to express diverging views collectively online is new. Millions of users are low-grade subversives, chipping away at the imposing edifice of the party-state with humour, outrage and rueful cynicism.

Only those deemed to be threatening the state—on a very broad definition that can include being critical of a leader, or airing some grievance—are singled out for punishment.

Sometimes online complaints do produce results, swiftly bringing offenders to book. When an army political commissar got abusive with a flight attendant, she posted photographs of the incident. Internet users soon ferreted out his name, job title and location and he was eased out of his job. When an official was photographed smiling at the scene of a gruesome accident, the online crowd noticed he was wearing a luxury watch and quickly came up with more photographs of the same official wearing other luxury watches. “Brother Watch”, as he came to be known, was fired.
Small victories like this are becoming increasingly common, to the dismay of millions of Communist Party cadres. Many web users believe that the balance of power has shifted: in a survey conducted in 2010 by a magazine affiliated to the People’s Daily, the party mouthpiece, more than 70% of respondents agreed that local Chinese officials suffered from “internet terror”.

Yet for the party as a whole the internet holds much less terror than it does for local officials. The online mob can gorge itself on corrupt low-level officials because the party leaders allow it. It can make fun of censorship, ridicule party propaganda and mock the creator of the Great Firewall. It can lampoon a system that deletes accounts and allows them to pop up again under a new name, only for the new accounts to be deleted in turn. It can rattle the bars of its cage all it likes. As long as the dissent remains online and unorganised, the minders do not seem to care.

At the same time, though, the more sensitive tweets and blog posts, attacking senior party leaders by name or, most serious of all, calling for demonstrations in the real world, are quickly deleted, sometimes before they even make it onto the web. Activists who directly challenge the central party organisation or attempt to organise in numbers (like Mr Liu) are crushed long before they can pose a threat. (Pornography is also officially censored, though it proliferates nonetheless.) The rest of the chaotic internet that takes up people’s time, energy and money carries on, mostly undisturbed. Dissident activity plays only a small but potent part in the overall mix.

Adaptive authoritarianism

For the party leaders the internet has created more subtle challenges. Collective expression on the web, led by civic-minded microbloggers with millions of followers, is focusing attention on recurring problems such as food safety and pollution, showing up the gap between expectations and performance. That means the authorities now have to try to come up with credible responses to crises such as the huge spike in air pollution in January and February. In short, the internet requires the party centre to be more efficient at being authoritarian.

This is the online blueprint for what scholars call “adaptive authoritarianism”, and there is an international market for it. China sells its technological know-how abroad, including tools for monitoring and filtering the internet. Huawei and ZTE, two big Chinese companies, are leading suppliers of internet and telecoms hardware to a number of states in Central and South-East Asia, eastern Europe and Africa, including Kazakhstan, Vietnam, Belarus,
Ethiopia and Zambia. Many of these would like to increase online access while retaining tight political and technological control. China has aligned itself with these countries and dozens of others, including Russia, in a global dispute with Western democracies over how the internet should be governed.

Dissidents in China say that freedom is knowing how big your cage is. It could be argued that with their internet the Chinese authorities have built one of the world’s largest, best-appointed cages. It could equally be said that they have constructed an expensive, unwieldy monstrosity, a desperate grab for control to buy time for the party. Either way, a careful look at their edifice should throw light on the question whether the internet is an inherently democratising force. This special report will show how they built it and ask if it can last.

From the print edition: Special report