A giant cage





# 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?

THIRTEEN YEARS AGO Bill Clinton, then America's president, said that trying to control the internet in China would be like trying to "nail Jell-o to the wall". At the time he seemed 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 shortwave 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

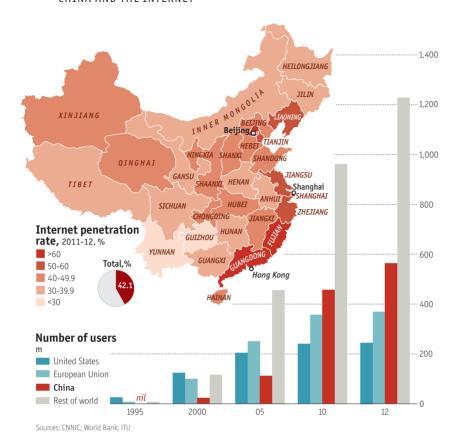
Ironically, the first e-mail from China, sent to an international academic network on September 14th 1987, proclaimed proudly: "Across the Great Wall we can reach every corner in the world." Yet within China's borders the Communist Party has systematically put in place projects such as the Great Firewall, which keeps out "undesirable" foreign websites such as Facebook, Twitter and YouTube, and Golden Shield, which

#### CONTENTS

- 3 The machinery of control Cat and mouse
- 5 Microblogs Small beginnings
- 6 The Great Firewall The art of concealment
- 8 E-commerce Ours, all ours
- 10 Cyber-hacking Masters of the cyber-universe
- 12 Internet controls in other countries To each their own
- 12 Assessing the effects A curse disguised as a blessing?
- 13 Turning off the internet Thou shalt not kill

A list of sources is at Economist.com/specialreports

An audio interview with the author is at Economist.com/audiovideo/ specialreports



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 inter-

net 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 iso-

lated 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-0

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 staterun 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.

### The machinery of control

### Cat and mouse

### How China makes sure its internet abides by the rules

THE HISTORY OF the internet in China is one of give and take, of punch and counterpunch, where the authorities are often surprised by the force and speed of online interactions but determined to keep them under control. The result has been a costly and diverse industrial complex of monitoring and censorship. Central-government ministries have invested in two pillars of control: the Great Firewall, a Western name for a system of blocking foreign websites, starting in the late 1990s, which some believe has cost as much as \$160m (the details are state secrets); and Golden Shield for domestic surveillance and filtering, begun in 1998 by the Ministry of Public Security and estimated to have cost more than \$1.6 billion so far.

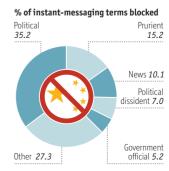
A number of other government departments have their own internet divisions. Many provincial and local governments, too, officially responsible for internet management in their area and keen not to be caught out by local unrest, have invested in their own tailored monitoring systems. More than 100 Chinese companies have made a total of at least 125 products for monitoring and filtering public opinion online, according to a Chinese government register. The most expensive of the publicly disclosed government purchases reviewed by *The Economist* was bought by Beijing's internet-propaganda office for \$4.3m. (One foreign supplier, Hewlett-Packard's Autonomy unit, devised an online public-opinion monitoring system for the Chinese market in 2006 and has had some takers in government.)

One of the suppliers to government, Founder, created by Peking University, describes to potential customers how it helps overworked government staff by monitoring hundreds of domestic websites and overseas Chinese sites. "The early-warning [feature] monitors sensitive information which needs to be dealt with immediately...such as June 4th [the date of the Tiananmen Square crackdown in 1989 and] Charter 08 [Mr Liu's anti-authoritarian manifesto]." The authorities have learned to watch out for ingenious variants of June 4th, including May 35th, April 65th and March 96th. The Founder system also monitors material that may "prompt mass incidents in society and on campus".

### Keep it quiet

Websites and terms blocked by Chinese authorities, latest

Sites tested by GreatFire.org		
Type	Tested	Blocked
URLs	60,111	8,724
Domains	17,144	1,738
Weibo searches	13,130	1,718
Google searches	7,604	1,682
Wikipedia pages	418	223
HTTPs	1,134	213
IP addresses	347	58
Alexa top 1,000 domains	976	34
Google sites	371	27



Sources: GreatFire.org; Jeffrey Knockel, University of New Mexico

In addition, a number of black-market internet companies sell services to individuals, including the deletion of negative articles from websites, using connections in government and at the big internet companies, sometimes at a cost of hundreds of thousands of dollars. Some 60% of the profits of one such company in Beijing, Yage Time Advertising, came from sales to local officials in smaller Chinese cities who wanted to delete negative reports about themselves, according to Caixin, a Chinese financial magazine. The software system for detection and filtering that Yage was offering these officials cost \$64,000. Yage was busted by police in July last year, but the unofficial business of deleting posts—and of planting negative ones and of selling "zombie" followers and retweets of posts—continues to flourish.

### Manual labour

Surprisingly, the machinery of control is far from monolithic, and rife with inconsistencies (especially from province to province: one study found that more than half the microblog posts in Tibet were deleted, compared with barely a tenth in other provinces). It is also much less automatic than might be expected. Academic studies of Chinese censorship show that for all the software and hardware involved in detecting and filtering content, much of the deleting is done manually, blog post by blog post, tweet by tweet. This system requires a substantial investment in people, perhaps as many as 100,000 of them. That includes internet police (20,000 or more), propaganda workers and in-house monitors at thousands of websites, from small discussion forums to behemoths like Tencent and Sina. A recent study reckoned that Sina Weibo, the country's main microblog, currently employs more than 4,000 censors.

This model seems to have a number of drawbacks. Humans make mistakes and can be overwhelmed, as they appeared to be after the crash in 2011 of a high-speed train near Wenzhou, when all of Sina's censors (then numbering only 600-plus) were called in to help, according to *Phoenix Weekly*, a magazine. Such a crisis can put intense strain on these individuals. Some disgruntled or liberal-minded employees clearly view the system as flawed and are providing information about its shortcomings to overseas sites. China Digital Times, a blog run by a dissident exile, Xiao Qiang, from the University of California, Berkeley, regularly publishes transcriptions of propaganda directives under the heading "Ministry of Truth".

For the most part, though, these workers accept the system, and not just because of Communist Party indoctrination and discipline. The party has cells inside most, if not all, of the big internet companies and makes sure that some key posts go to party members. Party leaders have also consistently worked on keeping the big web companies' CEOs loyal. Since 2003, when Hu Jintao became president, the web bosses have been invited on annual "red tours" of historic communist sites. Baidu's co-founder, Robin Li, and Sina's CEO, Charles Chao, have been on many such trips. (Mao Daolin, a Sina CEO before Mr Chao, demonstrated his loyalty by marrying Mr Hu's daughter in 2003.) Disciplinary sanctions also play a part. Internet companies that flout the rules, as some do in an effort to increase traffic, are suspended or shut down altogether. Companies that play by the rules can thrive, but have to budget for employing lots of censors.

For thousands of individual censors to do their jobs willingly and effectively, the system must have a fundamental logic. As it turns out, the party applies the same strict rules online as it has done on the ground since the Tiananmen Square crackdown of 1989: do not jeopardise social stability, do not organise and do not threaten the party. In a study of deletions of Chinese blog posts in 2011 and 2012, researchers at Harvard found that posts which were merely critical of government policies were tolerat-

ed. The ones most likely to get deleted were those that might trigger collective action such as protests. This was true even for posts that appeared to be pro-government.

The authorities have been strikingly consistent in applying this rule. The earliest significant act of domestic internet censorship, in September 1996, was to shut down an online discussion forum at Peking University, "Untitled BBS", when nationalist students began agitating for demonstrations against Japan after a right-wing Japanese group had made a provocative display at the Senkaku, or Diaoyu, islands, Japan's claim to which China disputes. The internet had been commercially available in China only since January 1995, and at the time it had fewer than 80,000 users in the country, but the fear of a "virtual Tiananmen Square" was palpable, writes Xu Wu, an academic.

At about the same time the government started blocking foreign websites, including Voice of America. By July 1997, writes Daniel Lynch at the University of Southern California, Chinese police were looking for advanced filtering software at a conference in Hong Kong. In December 1998 China held its first known trial for a purely internet-based political crime, imprisoning Lin Hai, a software engineer, for sending 30,000 Chinese e-mail addresses to a pro-democracy magazine based in America. Since then China has often jailed activists either for posting pro-democracy messages online or for e-mailing sensitive material abroad, and continues to do so.

In 2005 it took to using "web commentators" and "publicopinion guidance" to supplement censorship and targeted repression. That spring anti-Japanese protests had erupted in cities across China, organised in part through Tencent's QQ chat groups and bulletin boards. In an internal party speech in 2005 Mr Hu gave warning of a "smokeless war" being waged by China's enemies, and of the need to defend the party ideologically. According to Wen Yunchao, a prominent blogger, "the authorities had felt the internet was out of control and they needed to address it immediately. At the end of 2005 they had a meeting in Oingdao to study how to control the internet."

They started to hire online commentators to steer conversations in the right direction, who became known as the "50-Cent Party" because they were paid 50 Chinese cents per post. In January 2007 Mr Hu gave a speech to the Politburo calling for it to "assert supremacy over online public opinion" and "study the art of online guidance". Controlling the internet was not enough; the party also needed to "use" the internet, said Mr Hu.



The arrival of Twitter-like microblogging services in China, and particularly of Sina Weibo in August 2009, forced the authorities and their web commentators to become more active than ever. Officials have tried but so far failed to compel all users to register for online accounts with their real names. Social media also made the government even more concerned about the threat of "hostile foreign forces" online, which it took on with a will. As a white paper on the internet in 2010 put it, "Foreign social-networking sites have become a tool for political subversion used by Western nations." The Chinese authorities reinforced the Great Firewall, their first line of defence against such sites.

#### Control freaks

These days, whenever something happens that the Communist Party sees as a threat to social stability, China's internet managers set in motion a rapid, massive and complex response. The system has evolved with each new technology for online interaction. The nerve centre is Beijing, where most of the big internet companies are based. The Beijing Internet Information Administrative Bureau gets in touch with its contacts at the city's internet portals and microblogs, telling them what is to be deleted from microblogs, blogs and news sites and what approved messages are to be promoted. If the story is very big, celebrity microbloggers (such as entertainers, billionaire entrepreneurs, media personalities and technology icons), each with many millions of followers, may be asked by minders at the internet companies to keep quiet, though most do not need to be told.

In cities around the country, local internet publicity offices will contact internet commentators to feed them the official guidance for their online bulletin boards and discussion forums. And at hundreds of local, provincial and national offices of the various ministries concerned, custom-tailored software helps authorities find "harmful" online postings and get internet service providers to take them down.

Compliance is expected within seconds. When censors at Sina Weibo noticed a flood of posts on a censored New Year's Day editorial at Southern Weekly, a newspaper, they waited a few minutes before deleting them. One censor wrote in an online rant against complaining users that they should have been grateful for the slight delay. The censor's rant itself was quickly deleted, but has been translated and re-posted by Global Voices Online, a free-speech pressure group based outside China. The tardy supervisors had to sit through a pep talk by the authorities,



which deliver such lectures whenever they perceive resistance to "running the internet in a civilised manner"—and then tighten up controls further.

The government constantly worries about losing control when an incident captures the public's attention. This happens quite a lot, despite all the precautions. Examples go back to 1999, when followers of Falun Gong, a spiritual movement banned by the Communist Party, organised protests in Beijing and, having been crushed, used overseas Chinese websites to spread antigovernment propaganda.

In 2003 the authorities tried and failed to cover up the spread of the SARS virus. In 2005 anti-Japanese protests threatened to get out of hand. In 2007 opponents of a proposed chemical plant in Xiamen, in south-eastern China, organised protest "strolls". In 2008 riots broke out in Tibet and in 2009 in the northwestern region of Xinjiang. In 2011 a number of people tried to organise protests inspired by the "Jasmine" revolutions in north Africa and the Middle East. Later that year a high-speed train crashed, killing at least 40 people. In 2012 rumours spread of a coup attempt in Beijing. And so on. Each of these incidents, and many more, prompted new efforts at control. But until the system changes, it will be a never-ending task.

### **Microblogs**

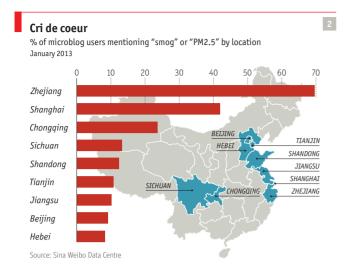
# Small beginnings

### Microblogs are a potentially powerful force for change, but they have to tread carefully

WITHOUT THE INTERNET Pan Shiyi would be just another Chinese billionaire property mogul. But online he has become one of China's most famous microbloggers, with nearly 15m followers on Sina Weibo, the country's main Twitter-like service. He has played a big part in a battle to force the authorities to clean up China's filthy air. In January that battle at last began to turn in the public's favour. Millions of people tweeted in outrage at a dense blanket of pollution that smothered Beijing and many other Chinese cities for days (see chart 2, next page). Chinese newspapers were allowed to give the smog unprecedented coverage. Officials tightened up car-emissions standards in Beijing and ordered an expensive nationwide upgrade of refineries by 2014. But was this a foretaste of the growing power of microblogs or a special case?

Mr Pan is conscious of being a special case himself, positioned somewhere between the public and the government but closer to the government end. He became one of the earliest bloggers when in 2009 Sina invited him to sign up for one of the first 20 accounts on its new service, Sina Weibo (weibo is Chinese for microblog). As a co-founder of SOHO China, one of the country's best-known developers, he belongs to a generally despised group of entrepreneurs, along with coal-mine bosses and corrupt officials; and he attracts some criticism online, especially over property prices, which are out of reach for many in the broadening lower middle class. But he has generally avoided sensitive political issues, and in 2010 he proudly proclaimed that not a single tweet of his had been deleted.

Even so, Mr Pan, who has two sons, felt it was appropriate for him to comment on air pollution: "You need to breathe, and so do I. State leaders need to breathe, and so do ordinary people." Thus in 2011 Mr Pan's toothy grin, square glasses and bald pate,



▶ instantly recognisable by the millions who follow him, became the face of "PM2.5", a category of small pollutants, measuring less than 2.5 microns across, that are particularly damaging to the lungs. Until then few Chinese had heard of them. There was no standard for an acceptable level, and most cities did not measure them. But the American embassy did, and was posting hourly readings on Twitter. Chinese officials had asked the Americans to stop, but since Twitter was blocked by the Great Firewall most Chinese were unaware of the embassy's readings—until Mr Pan began to post them daily on Sina Weibo.

"When I first started I thought it would be very calm. I didn't want to start a confrontation, and also I didn't want to be the focus of any confrontation," says Mr Pan. But it came anyway in November 2011 when he asked his followers to vote on their preferences for a PM2.5 air-quality standard: should the government introduce it within one year, two years or not at all? The environmental-protection bureau in Beijing called Mr Pan in for a telling-off. Officials said it would be impossible to enact such a standard even within a decade. Shortly afterwards a Chinese newspaper report on his air-quality campaign was killed off before publication, he says, and propaganda officials ordered a temporary news blackout on him.

But by then the leadership had started taking an interest in PM2.5. On February 7th several Beijing papers ran the same story on their front page: that managing PM2.5 pollution should be the city's priority in 2012. Mr Pan says he later learned that the impetus had come straight from the president at the time, Hu Jintao. Last summer senior party officials invited Mr Pan, along with a panel of public-health experts, to advise them on air pollution; he was greeted by the mayor of Beijing and by the same environmental-protection bureau that had lectured him months earlier. In late January 2012 Beijing began publishing its own PM2.5 readings, and less than a year after Mr Pan's poll the city had a PM2.5 standard. At the start of this year 73 other cities took to publishing PM2.5 measurements, just in time for the ghastly pollution that descended on January 12th.

Since then microblogs have ensured widespread awareness of PM2.5 levels in China. In Shanghai 42% of users who tweeted in January mentioned "smog" or "PM2.5", according to Sina Weibo Data Centre. On January 29th Mr Pan took another online poll, asking whether China should have a clean air act; 99% of his respondents said yes.

This kind of sustained online interest in an issue is unusual. Sina Weibo and rival microblogs are mostly theatres of diver-

sion. Many news events are greeted with banter and critical comment, as they are outside China, and attention moves swiftly from one subject to another. Moreover, the strength of interest can be exaggerated by a flourishing black-market trade in fake "followers" and "retweets" to boost brands, celebrities and sometimes the microblog itself. Sina Weibo, for instance, has more than 500m registered accounts, but many of them are robots employed to generate artificial buzz. Sina itself says that the number of daily active users at the end of 2012 was only 46m.

### Men of few words

Still, popular personalities like Mr Pan can start discussions on microblogs which the authorities take seriously. It helps that although tweets are limited to 140 characters, as in the West, each Chinese character carries a lot of information, so the messages can be more specific and detailed. Occasionally popular microbloggers are asked to behave themselves. Hung Huang, a magazine publisher with 7m followers, says her minder at Sina told her not to tweet on the day of an environmental protest in Dalian, a north-eastern city.

Mr Pan says he was given no such warning, nor did he need it. He is well aware of how much influence he has and how quickly a single tweet of his can spread beyond his intended reach. "Weibo can be used as a tool to participate, to express one's opinions on many things, all kinds of things. However, if you talk about food safety, you will touch on the interest of food manufacturers and that's not safe for you," he says. "It would be even less safe if you talk about Chinese politics, democracy and freedom. Social reform and religious issues are also not safe topics given the current social environment in China."

Despite his political caution, Mr Pan finds it hard to restrain his enthusiasm for his chosen medium. Chinese society before microblogs, he says, picking up your correspondent's iPhone to demonstrate, was "like a cold piece of iron", its atoms inert. Now the iron is hot, he says: the atoms have been activated.

### The Great Firewall

### The art of concealment

# Chinese screening of online material from abroad is becoming ever more sophisticated

ON FEBRUARY 9TH, Chinese New Year's Eve, Fang Binxing, known in China as the father of the Great Firewall, wished his followers on Sina Weibo a happy Year of the Snake. As always whenever Mr Fang tweets, thousands of fellow microbloggers sent messages along the lines of "get lost". They could not reply directly: Mr Fang gets so much abuse for his role in engineering China's censorship technology that the "comments" function on his microblog page had to be disabled long ago. Nor can users easily find the comments on the 35,000 retweets of his new-year post: Sina has blocked access to those as well.

Mr Fang is used to being, in the parlance of the system he helped create, a "sensitive keyword". He is one of the most important figures in the history of the Chinese internet, and perhaps its most reviled. In 2011 several students in Wuhan, in central China, said they threw eggs and a pair of shoes at Mr Fang when he visited their campus to give a speech. There was not a little irony in their spreading the news of their action (and a photograph of one student's shoeless feet) on Twitter, which thanks

to Mr Fang's work is accessible to China's internet users only with special circumvention tools.

Exactly how Mr Fang constructed his wall is a state secret and the subject of much speculation and academic research. Although China's entire system of internet controls is often described under the heading "the Great Firewall" (a term that first appeared in a Wired magazine article in 1997), in reality the Great Firewall is probably the simplest part of a complex effort involving many different agencies and companies. China's cyber-police have their own much larger and more expensive system of domestic filtering and surveillance, Golden Shield, and internet sites employ lots of people to censor their own content and implement government directives.

The Great Firewall that Mr Fang helped build stands separately, guarding a handful of gateways through which all foreign internet content and communications enter the country, sniffing through small packets of data to detect and block access to "harmful" foreign content. It is the world's most advanced na-

Google has been one of China's favourite targets over the years, making it a useful measuring stick for the way that filtering technologies have developed

tional firewall, having evolved from crudely blocking entire web domains (though it still does some of this) to blocking just particular pages within websites (see chart 3).

Mr Fang's work on this system started in 1999, at the National Computer Network and Information System Security Administration Centre, under what is now the Ministry of Industry and Information Technology. It created the modern infrastructure for filtering foreign sites. In the early years China's efforts at blocking web domains had been straightforward. From August 1996 routers filtered out a list of foreign websites, including those of Voice of America, human-rights groups, Taiwan and Tibet independence advocates and some foreign newspapers. But the early blocks did not take account of the content of individual web pages, and savvy users could easily get round them.

Now the firewall is far more capable. If users try to get on Facebook, Twitter or thousands of other websites, or if they search for a banned keyword such as "Falun Gong" or the name of one of the many jailed Chinese dissidents, they are taken to a dead end with an error message (such as "web page not available"). The system can intercept messages containing banned terms sent across China's borders on chat software. It can also block access to many circumvention tools, and in December last year it began more intensive disruption of private commercial services, called VPNs, that are widely used to "tunnel" under the firewall. It also subtly and intermittently "throttles" websites such as Google's search engine to slow them down.

### Degoogled

Google has been one of China's favourite targets over the years, making it a useful measuring stick for the way that filtering technologies have developed. In September 2002 the firewall blocked Google entirely, using a technique called "DNS poisoning" that intercepts requests for web pages. The blocking made global headlines. The service was restored after nine days, but Google's "cache" pages (snapshots of web pages stored and delivered by the company), which had been a convenient way for Chinese users to find banned content, remained blocked. The Great Firewall was getting smarter. Today searches for banned keywords on Google will take users to a dead end and leave

them in a virtual sin bin, blocking access to the search engine for about 90 seconds, though other parts of the internet will remain readily available.

The centrepiece of this sophisticated filtering effort had been the National Information Security Management System, named Project 005 after its starting date in May 2000. Mr Fang and other engineers worked on it until 2002. The project won a national prize for science and technology in 2003. It had cost \$60m to build and is believed to be the most critical and most expensive component of the Great Firewall.

Mr Fang, who in 2007 became president of Beijing University of Post and Telecommunications, has sometimes played down his involvement in such efforts, but he has clearly had a big part in them. For example, he helped develop filtering technology used for domestic search engines, according to the summary of a study (itself not in the public domain) he co-wrote in 2005. The system "has yielded good results", the summary states, and will help in "purifying the domestic internet space".

Many Chinese internet users are less keen on these advances. In January Han Weili, a professor at Fudan University in Shanghai, was attacked for inviting doctoral students to conduct research on China's Great Firewall (GFW, as Chinese users abbreviate it). His notice on the university's online bulletin board read:

"Anyone interested in improving the GFW. Their team is recruiting PhD students. If interested, get in touch with me."

Mr Han felt compelled to defend himself. "So in your opinion the scientists who studied nuclear bombs should be ashamed of themselves throughout history? The launch button for nuclear weapons is controlled by the politicians of a country," Mr Han wrote in a reply that was later deleted. "As for how to use [the GFW], it's not something scientists can handle. You can be the king of morality and refuse to do it, but you don't have to condemn those who try to improve it." Mr Han later wrote that he has not worked directly on the firewall. His last word on the matter was that authorities had asked to meet him: "Both sides hate me. Damn it." That comment too was deleted.



Sources: CNNIC; World Bank; news reports

### SPECIAL REPORT

CHINA AND THE INTERNET

Mr Han has a point. It is generally senior bureaucrats, not engineers like Mr Fang, who decide what foreign sites are unfit for Chinese users, such as YouTube (blocked permanently in 2009), Facebook and Twitter (blocked since riots in Xinjiang in 2009) and Bloomberg and the New York Times (blocked in 2012, after publishing detailed reports on the finances of Chinese leaders' families).

The engineers' job is to fine-tune the instruments. Michael Robinson, an American network engineer who in 1996 worked on some of the early infrastructure of commercial internet access in China, says that "most of the development of the technical capabilities of the Great Firewall over the past 15 years has been toward an ability to minimise the impact of the government's content-control policies through more precise mechanisms." Such improvements often aim to minimise not the censorship itself but the sense of being censored. One technique is to leave tweets that have been removed from public circulation visible to those who posted them.

To most Chinese internet users, though, exactly who is responsible for what in the machinery of censorship matters much less than the idea of censorship itself. Mr Fang is a symbol, and the term GFW has become a hated archetype. It is shorthand for the restriction on their experience of the internet and for the increasing number of Chinese words that have become too sensitive to use, including many innocuous ones that happen to be homophones for sensitive ones. This prompted one user to write a science-fiction parody in which a new project, GFW Turbo, becomes self-aware and runs out of control, banning almost the entire Chinese language. The parody looks ahead to 2020 when a "National Anti-GFW Ministry" adds "2,000 more Chinese characters to meet the people's ever-increasing needs for means of production, only to find them censored within two seconds." Finally, in 2025, there is only one phrase left in the Chinese language: "sensitive word". ■

### E-commerce

### Ours, all ours

# A wealth of internet businesses with Chinese characteristics

SINCE THE EARLY days of China's web, internet cafés have been seen as modern-day opium dens where the addicted users, mostly young males, play online games. This generally remains true today. Walk into an internet café outside one of the Chinese factory complexes of Foxconn, an Apple supplier and the country's largest private employer, and you will see hordes of assemblers of iPads and iPhones on their breaks, playing multiplayer online games.

The one thing that has changed is the games they are playing. Less than a decade ago foreign games, such as South Korea's "The Legend of Mir II", accounted for 70% of China's online gaming market; now they make up just one-third. Instead, players are choosing home-produced fare, such as "Fantasy Westward Journey" or "Dream of Three Ancient Kingdoms". At the same time the market has surged from below \$160m in 2003 to an estimated \$9 billion in 2012, more than a third of the global total. By 2016 it is expected to be worth \$20 billion.

The online gaming industry illustrates two striking things about the Chinese internet as a place to do business. The first is



that the number of consumers and their spending have grown extraordinarily fast (see chart 4, next page). Far more people are online to shop, play games, search, watch videos and use social media in China than in any other country. Astonishingly, the number of online shopping transactions is expected to surpass America's this year.

The second is that those consumers are spending almost all of that time and money on Chinese internet platforms. The Communist Party has the internet industry it wants, a thriving sector served by Chinese-led companies that it can trust to be politically reliable, rather than by unpalatable foreign ones (even though on paper many of the Chinese companies are partly foreign-owned through private-equity and venture-capital investors). Not coincidentally, though, this politically sheltered industry is also devoid of significant technological advances. The chase for users and revenues means cut-throat competition and incremental innovation, but no leaps of invention.

Economics has played a big role in creating this walled-off Chinese ecosystem. Many early founders cloned Western services with the enthusiastic support of foreign (mostly American) investors who understood that the market would be large enough to support distinctly Chinese companies. So instead of visiting Western internet portals, users go to Sina, Sohu and Net-Ease. Instead of eBay, they shop at Taobao and pay not with Pay-Pal but with AliPay, an affiliate of Taobao within the Alibaba Group, China's dominant online shopping business. Instead of Google, users search on Baidu. Wang Xing, a talented engineer trained at Tsinghua University, China's Massachusetts Institute of Technology, created four successive clones in China: of Friendster, Facebook, Twitter and Groupon. Mr Wang's Twitter clone, Fanfou, stumbled when he failed to censor it strictly enough. But he sold the Facebook clone (which became Renren) for several million dollars, and his Groupon clone, Meituan, is now one of the market leaders. Groupon itself failed in China, and its joint venture was swallowed up last year by a clone owned by its own Chinese business partner, Tencent.

Many of the victors are now among China's wealthiest entrepreneurs, business heroes if not heroes of innovation. The creator of Taobao, Jack Ma, a former English teacher, first shot to fortune with Alibaba.com, an online platform for importers and exporters. Robin Li, co-founder and chief executive of Baidu, proudly displays his patent for a search algorithm at his head-quarters in Beijing—which predates, his employees note, the one awarded to Larry Page, Google's CEO (though Mr Li's business

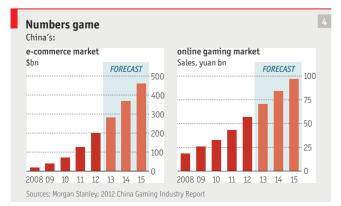


was closely modelled on Google). In 1999 Ma Huateng used a precise copy of AOL'S ICQ instant-messaging service to launch Tencent, but had to rename it QQ after AOL complained.

The spoils have been substantial. In 2012 China had more than 200m online shoppers who spent going on \$200 billion (not counting food and travel), ten times as much as in 2008. This market is dominated by Taobao, which is responsible for almost 60% of the parcels delivered by courier in China. More than 370m people watch online video, a medium that has special appeal, even with censorship, because the rules are looser than for traditional TV and cinema. Youku Tudou, which may turn profitable next year, has a market capitalisation of \$2.8 billion. Baidu owns more than 70% of search in China and has a market capitalisation of \$30 billion (compared with Google's \$267 billion).

Tencent, the leader in online games, is the most profitable internet business in China, earning more than \$2 billion in 2012 (see chart 5). The company has excelled at converting its hundreds of millions of social-media users into paying customers, mainly for virtual items in games. From being an AOL clone, it has evolved dramatically. Its elegantly designed WeChat social application, which has more than 300m registered users, is one of China's best examples of product innovation and may help the company gain business overseas. In February Tencent said it would expand its presence in America.

Each of the foreign companies that failed in China tells a different tale. Sometimes it is merely one of incompetence or a nimbler competitor. Quite a few foreigners lost out to the hordes



The Economist April 6th 2013

of Chinese entrepreneurs who copied fast and understood their customers better. But the playing field has not been level. Western companies have been blocked by the Great Firewall (as happened to Twitter, Facebook and You-Tube) or slowed down unacceptably (as is still happening to Google), examples of political protectionism translating into the economic sort.

More subtly, many foreign companies have found it **Hubs of commerce** Chinese internet companies Market Net cap. (latest) Revenue profit 7.0 Tencent 59.2 200 Baidu 295 1.68 NetEase 7.2 1.3 0.58 Sina 3.2 0.5 0.03 Yukou 28 0.3 -0.07

Sources: Thomson Reuters; company reports

hard to play by Chinese rules, both written and unwritten, either because they conflict with values or practices back home or because they explicitly favour domestic companies. Even companies that readily agreed to self-censorship, as both Yahoo and Microsoft did with their search and content-hosting services, encountered obstacles if they looked likely to gain too much market share. This has been especially obvious where the party has a political interest in the services offered: in news and information, social media and search, but also in online games. The multiplayer gaming market shows how politics helps shape a distinct Chinese internet even without the Great Firewall.

### From heroin to heroes

Until 2003 Chinese propaganda had consistently attacked online games as "opium" or "heroin" for the country's young people. The spectre of internet addiction is a recurring theme in the Chinese press, as are boot camps for curing it. But that attitude shifted abruptly, writes Hongping Annie Nie, an academic at Oxford University, as the party recognised both the cultural power and the economic potential of massively multiplayer games, which made money in part by telling compelling stories. "Long scorned and labelled as electronic heroin, online games now teach people history and culture in China," declared People's Daily in 2003.

Regulators helped by toughening the rules for foreign games, thus favouring joint ventures that would transfer game technology to domestic national champions, a familiar technique in other industries. The Ministry of Culture classified online games as "cultural products". The party wanted the stories told by online games to be Chinese ones, not South Korean or American, and especially not Japanese.

It got what it wanted. The gaming market is now dominated by big domestic companies including Tencent, NetEase and Shanda. The Communist Youth League helped fund "red" games like "Resistance War Online" in which users can play Red Army soldiers killing Japanese invaders. Meanwhile many of the more advanced foreign games are kept out by regulatory barriers or, like "World of Warcraft", are hassled and censored. And as online games played on social-media sites rapidly become more important, so too does the Great Firewall, as only the trusted domestic social-media channels can carry those games.

Some would say this is no way to run an internet. The Chinese model of copying Western web successes and raising barriers against foreign companies is so appealing and potentially profitable that it discourages risk-taking. What this model requires is competent and politically reliable engineers, not rebels, iconoclasts or dreamers. It is a metaphor for how China works.

Kai-Fu Lee, a Taiwanese-born former executive at Apple, Microsoft and Google, now funds start-ups in China, where he is a tech celebrity with more than 30m followers on Sina Weibo. In

February his account was briefly suspended when he blogged about the troubles of a party-sponsored search engine, Jike, which has hardly any users. Mr Lee believes that China's rote education system and its blocking of Facebook, Twitter and other creative influences will delay true innovation for generations.

"The out-of-box thinkers like Steve Jobs and Larry [Page] and Sergey [Brin], if people like that were born in China, they might not blossom to be the great people that they became, because they're maybe too radical, too cowboy-like," says Mr Lee. "When you go in to get funding in China, lots of teams will say, 'Who's done something like that in the Us, who are you analogous to?" Mr Lee says Innovation Works, his fund, does not invest in clones, but some of his competitors (a jealous crowd) call him the "King of Clones" for funding replicas of such businesses as Tumblr and Quora. In 2011 one wag created a mock-up of the Innovation Works website and called it "Copy Works".

One of Mr Lee's great laments was Google's withdrawal in 2010 of its China-based search business, which he had left months earlier. Google's attempt to operate in China was based on the idea that engagement even at the price of censorship was a net gain for the Chinese people. But this was bound to deepen the Chinese leaders' hostility towards the company. Mr Brin, Google's co-founder, who spent his childhood in the former Soviet Union, had always been uneasy about the China experiment. Once in the country, Google endured state-led media attacks accusing it of helping users find pornography, along with growing demands for self-censorship. But in the end what tipped the balance was not the public hostility but a secret and relentless campaign to hack the company.

### Cyber-hacking

# Masters of the cyber-universe

### China's state-sponsored hackers are ubiquitous—and totally unabashed

CHINA'S SOPHISTICATED HACKERS may be the terror of the Earth, but in fact most of their attacks are rather workaday. America and Russia have hackers at least as good as China's best, if not better. What distinguishes Chinese cyber-attacks, on anything from governments to Fortune 500 companies, defence contractors, newspapers, think-tanks, NGOs, Chinese humanrights groups and dissidents, is their frequency, ubiquity and sheer brazenness. This leads to an unnerving conclusion.

"They don't care if they get caught," says Dmitri Alperovitch, who used to work at McAfee, a computer-security firm, where he helped analyse several Chinese hacking operations in 2010 and 2011, and is a co-founder of CrowdStrike, another cyber-security firm. The indiscriminate tactics of China's 2010-11 campaign made it relatively easy to track. His team identified more than 70 victims (among many more unidentified ones), dating back to 2006, and found that the average time the hackers stayed inside a computer network was almost a year. "They'll go into an organisation and then stay there for five, six years, which of course increases the chances that they get caught."

Mr Alperovitch offers two reasons for the careless abandon of China's hackers. The first is that their attacks are on an industrial scale—"thousands of continuous operations"—so they could hardly be expected to go unnoticed. The second is that "they don't see any downsides to being caught. They have so far

not suffered economically or politically for being caught."

It is true that most victims are unwilling to remonstrate openly with the Chinese state. Except for Google, hacked companies have tended to keep quiet. Most governments have chosen not to confront China publicly, though American officials have recently started doing so. NGOs working in China have said nothing. Companies fear reprisals from customers and shareholders for failing to secure their networks. And perversely many victims do not want to antagonise their attackers. Even security companies, though obviously keen to capitalise on the threat, are wary of pointing the finger because they want to sell their antivirus products in China too.

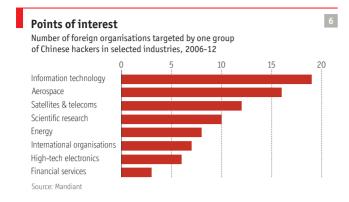
This culture of secrecy and shame makes it harder to confront the problem. It also helps Chinese officials, who consistently and emphatically deny allegations of state-sponsored hacking. They rely on the hope that in such a murky field the evidence is always wanting. Yet in reality it is often fairly plain, and attitudes may at last be hardening. That could mean growing suspicion of the big Chinese technology companies, including Huawei, which is already politically unwelcome in America, and Tencent, which is trying to expand its social-media services abroad. But it is not clear what, in practice, America and other Western countries can do to restrain Chinese behaviour, other than becoming better at hacking themselves.

### Whodunnit?

Security experts outside China have learned how to reverse-engineer methods of attack and trace attackers' internetprotocol addresses back to their physical origins. They have identified up to 20 "Advanced Persistent Threat" teams operating in China, including one that stole valuable commercial secrets from Google, Adobe and other Silicon Valley companies; another that for years targeted a number of global energy companies; and yet others that have hacked hundreds of companies, government agencies, think-tanks and NGOs the world over. The victims have included global steel companies; a firm that supplies remote-control systems for American oil and gas pipelines and power grids; a hotel computer system that provided access to data for important guests; a tech-security firm, RSA, that opened the way to hacking Lockheed Martin and defence subcontractors producing America's F-35 Joint Strike Fighter; and even NASA. Some of the attacks have been highly sophisticated, but many more have begun with a simple "phishing" e-mail fooling the recipients into clicking on a link.

The organisation and scale of these attacks, involving large teams of hackers and thousands of computers, strongly suggest





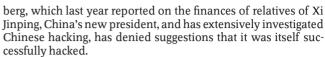
• that the Chinese party-state has played a guiding role. American experts point to the People's Liberation Army's 3rd Department, which according to the Project 2049 Institute, an American thinktank, is roughly equivalent to America's National Security Agency. Project 2049 describes an apparent fixation with North American targets at the Shanghai headquarters of Unit 61398, part of the 3rd Department. In February Mandiant, a security firm, identified Unit 61398 as the likely base for thousands of attacks on North American corporate and security targets.

The choice of targets also clearly points to China's government as the perpetrator. The Google hack, at a time when the company was facing increasing hostility in China, appeared to leave little room for doubt; one Chinese source actually told officials in America's State Department that two members of the elite Politburo Standing Committee ordered the attack, according to a State Department cable that was released by WikiLeaks. Other victims of hacking attacks included the International Olympic Committee and the World Anti-Doping Agency after the 2008 Beijing Olympics; Tibetan and Uighur activists and Chinese dissidents; think-tanks that analyse China (including its hacking capabilities); and NGOs operating in China. None of these seemed to have any commercial value.

For an individual caught up in such an attack the effect can be creepy. One day in early 2010 an American working for an environmental NGO in China noticed something odd happening on his BlackBerry: it was sending an e-mail from his account without his doing. He watched, dumbfounded, as the e-mail went out to a long list of Us government recipients, none of which was in his address book. Seconds later he saw the e-mail disappear from his sent folder. Eventually he heard from the fbi

that his e-mail account and those of several colleagues had been compromised by hackers from China. All the victims had attended a climate-change conference in Copenhagen in December 2009 where America and China had clashed.

Another obvious target was David Barboza, a journalist on the New York Times. In October 2012 he reported that relatives of Wen Jiabao, then China's prime minister, had amassed assets of \$2.7 billion. After the story was published, said the newspaper, Chinese hackers compromised its networks to get at Mr Barboza's work e-mail account. Following the newspaper's disclosure in January, other news organisations, including the Wall Street Journal and Reuters, noticed similar Chinese intrusions. But Bloom-



The Chinese authorities, which since the report on Mr Wen have blocked the *New York Times*'s English and Chinese-language websites, angrily denied the newspaper's hacking allegation. Wan Tao, one of China's first "patriotic hackers" (nationalists who in the early days of China's internet hacked into websites of foreign governments on their own initiative), offers a convenient alternative culprit: "underground hackers", or blackmarket operators who either sell their services or strike out on their own in hopes of finding a buyer. "Their business model is to sell," Mr Wan says, sitting in front of a ThinkPad in a coffee house in Beijing. The price of access to a target's e-mail box starts at less than \$1,000, he says.

But Mr Wan's explanation is unconvincing. His own story offers evidence that what may have started as independent hacking has evolved into a state-supported enterprise. He is now a cloud-security consultant but was an "angry young man" in the 1990s, he says. In 1997 he joined China's first hacking group, "Green Army", leading attacks on foreign websites. His first (solo) patriotic hack, in 1997, was to crash the e-mail box of the Japanese prime minister's website; in 2001, after an American spy plane collided with another plane, he and fellow patriotic or "red" hackers conducted various attacks on American websites in what they quaintly called a "cyberwar".

### The quick and the dead

The authorities gave Mr Wan and other hackers free rein. Police did not worry about hacking of targets outside the country, and still do not appear to. China has so far failed to sign an international cybercrime convention. Although hacking has been a criminal offence in China since 1997, the authorities have enforced the law only when the perpetrators were targeting things like state secrets and assets. The first publicised hacking trial in China, in 1998, was of two men who got into the website of a state-owned bank in Jiangsu province, stealing less than \$100,000. One of them was executed.

In contrast, patriotic hackers like Mr Wan were sought out for their advice and expertise. In 1998 the cyber-police, then quite newly formed, approached Mr Wan at a security conference in Guangzhou. They wanted him to help them find out who had written anonymous subversive postings on bulletin boards. In response he designed a software system in 1999 that could analyse posts about sensitive subjects such as Falun Gong or democracy, compare them with other online content and find out who had written them. He believes it was the first of its kind in China. "I'm a security expert," he explains. "They had the need."

Later, after his hacks against America, says Mr Wan, he was asked for help by the People's Liberation Army (PLA). He did not want to work for them but agreed to introduce them to other hackers. Since then the PLA has openly recruited hackers, sponsoring contests at universities and posting job advertisements.

The Chinese army's doctrine of cyber-warfare (like that of a number of Western counterparts) is to knock out the enemy's information infrastructure, and its doctrine of cyber-security is to go on the offensive to defend itself against attacks. The Chinese authorities often point out, correctly, that they are the victims of frequent cyber-attacks from America. Thousands of such attacks are also carried out from Russia and Brazil every year. But more of them originate from China than from anywhere else in the world, and at least some of them are undeniably linked to the party-state. That Chinese model may well prove attractive to other countries.



#### Internet controls in other countries

### To each their own

### China's model for controlling the internet is being adopted elsewhere

AT A UNITED NATIONS conference on telecommunications governance in Dubai last December representatives of most of the world's countries argued furiously over the way the internet should be managed. The debate established a clear divide over how much control a country should have over its own internet. On one side were America, the European Union and other developed countries that broadly back internet freedom; on the other were China, Russia, Saudi Arabia, Sudan and a number of other authoritarian states. A significant majority of these seem to favour China's approach to control (or a Russian variant), which involves allowing more access to the internet and reaping the economic benefits, but at the same time monitoring, filtering, censoring and criminalising free speech online.

Many Asian and African countries are using Chinese technology both to deliver access to the internet and to control its use, and some Central Asian republics are believed to use Russian surveillance technology as well. A very few, such as Turkmenistan, prefer the North Korean model, in which hardly anybody is allowed to go online, and a few others, including Azerbaijan, do little to encourage use of the internet. Katy Pearce, of the University of Washington, explains that Azerbaijan has run an effective campaign against the evils of the web, linking it to mental illness, divorce, sex-trafficking and paedophilia. She says that only a quarter of Azerbaijan's population has ever been online, which puts it behind poorer neighbours; and only 7% are on Facebook.

But most authoritarian regimes have allowed the use of the web to grow rapidly, noting that China has found it perfectly possible to embrace the internet while keeping it under close control. In Kazakhstan, for instance, some 50% of the population is now online, compared with 3.3% in 2006, though access is tempered by some Big Brotherish constraints.

### What's your weapon?

In Russia, Nigeria, Vietnam and elsewhere the government is paying people to blog and comment in support of government priorities, a tactic China started in 2005 with its "50-Cent Party" of web commentators for hire. Belarus, Ethiopia, Iran and many others are believed to use "deep packet inspection" to look into internet users' communications for subversive content, aided by hardware from, among others, China's Huawei and ZTE. Obligingly, internet users who know they are being watched are more likely to exercise self-censorship in the first place.

In addition some authoritarian states selectively block access to foreign websites that carry politically sensitive content, along with shutting down or harassing domestic opposition websites. In some countries opposition websites are subjected to massive denial-of-service attacks. Another technique, borrowed from Russia, is to accuse troublesome website operators of extremism or defamation, which in some countries are criminal offences. This method is employed by Kazakhstan, which also blocks some sites without acknowledgment, much less an explanation, in the same way as China does. Kazakhstan officials say they have a completely free, lively internet and block only extremist content. But that sounds doubtful in a country



that also cracks down on its opposition press and where the president, Nursultan Nazarbayev, regularly claims more than 90% of the vote in elections.

A growing number of such countries have an internet that each of them can call their own, walled off as much or as little as suits them. They argue that Western governments also manage the internet, censoring it and shutting down objectionable websites, so they should let others do the same. This was the crux of the debate at the telecommunications conference in Dubai. Russia, China and 87 other states insisted that all countries should recognise each other's sovereign right to connect to the internet in their own way. That resolution failed, but China's internet model is clearly attracting plenty of followers.

### Assessing the effects

# A curse disguised as a blessing?

### The internet may be delaying the radical changes China needs

ONE OF THE world's most widely read bloggers, Han Han, who is based in Shanghai, once explained to your correspondent why he did not think much of the shorter forms of microblogs, which he uses only sparingly. It was not long after the high-speed train crash in July 2011 that had been a big moment for social media. Outrage at the accident and at the government's slow and bumbling response spread rapidly on Sina Weibo, overwhelming the censors. It seemed a rare case of the public shouting down the authorities. Urban intellectuals, including some hardened sceptics, saw this as a turning-point in the history of the internet, perhaps of China generally. But Mr Han was not impressed. "You feel everyone's really angry, you feel like you could go open the window and you would see protesters on the street," Mr Han said. "But once you open the window, you realise that there's nothing there at all." Microblogging, he said, encouraged people to tune into a big story briefly, almost as entertainment, until the next big story comes along. It did not bring about "any real change or progress".

And yet microblogging has already transformed Chinese society and the way it is ruled. It has fundamentally altered the relationship between the people and the state, allowing the public to demand more accountability from officials, even if it is of-

be ten disappointed. In another era the authorities would surely have kept the details of that train crash secret, lied about its cause and understated the death toll. As it was, official orders kept it off the front pages the following day. Even so, microblogs quickly spread the news, along with lots of photographs, before officials could control them. When a spokesman failed to provide convincing answers, he was pummelled online and lost his job. Anger continued to rise at his employer, the powerful railway ministry, which is now being reorganised.

This special report has argued that by building a better cage, the Communist Party has reaped the economic benefits of the in-

ternet while absorbing and controlling its political impact, and that other countries have adapted China's blueprint to their needs. The high-speed crash posed a challenge to this state of affairs, a demonstration of the power of weibo to rattle the cage. So is that cage built to last or will it fall apart, shown up as an increasingly desperate and ultimately doomed effort to control the uncontrollable? Recently it has become fashionable to suggest that the cage is being rattled so much it will eventually break, heralding a Beijing spring. This special report, in contrast, has argued that if such a spring were to be on its way, the internet may well be delaying its arrival, not hastening it.

### Thou shalt not kill

### Turning off the entire internet is a nuclear option best not exercised

IN A CRISIS, might China flip the "kill switch" on its internet and disconnect its 564m users? It may sound unthinkable, but the idea is not altogether outlandish. The Communist Party has already given it a trial run in an entire province.

In July 2009, after ethnically charged riots left hundreds dead in Xinjiang, a remote north-western region with a sizeable Muslim Uighur minority, the authorities put the province on electronic lockdown. More than 6m internet users were cut off from the rest of China and from the world, and long-distance calls and text messages on mobile phones were disabled. Xinjiang residents could not use these telecoms services for many months and were unable to use any of the outside internet, even most of the scrubbed Chinese version, until the following May, leaving a gap of more than ten months.

By the party's criteria it seemed to work. The combination of online repression and ruthless security on the ground enabled the authorities to quell the riots and prevent further disorder. This did not seem to cause any great harm to China's reputation abroad, but there was an economic price to pay. Xinjiang's exports in 2009 plummeted by 44%, compared with a less devastating drop of 16% in a difficult year for the global economy.

Technically, shutting down Xinjiang was relatively easy because it was already isolated both geographically and technologically. It required nothing more than blocking all internet-protocol addresses outside Xinjiang at the border so people were stuck in a Xinjiang "intranet", a rather dull place. Some users used long-distance calls to hook up to the internet by modem, though access numbers would get blocked. Others travelled long distances outside the province to get connected.

Cutting off the whole country would

be a different matter. In December Renesys, a network-research firm, ranked more than 200 countries by how easy it would be to disconnect them from the internet. It reckoned that for 61 of them, with only one or two internet service providers at their borders (eg, Tunisia, Ethiopia and Yemen), it would be fairly simple, and for another 72 (including Rwanda, Kyrgyzstan and Iran) it would not be too difficult. China, with its well-developed internet backbone, was not on either of those lists. Renesys thought that given a "determined effort", its internet could be shut down over a period of time, "but it would be hard to implement and even harder to maintain."

The party has often proved itself capable of making a determined effort when it comes to security. The Great Firewall could easily block the foreign internet for most users in China; an unexplained glitch actually made this happen by accident one day last year for a couple of hours. Some large enterprises, banks and foreign companies have leased their own lines out of China, which might need to be shut down separately. As for the domestic internet, which would be of most concern to the party, shutting down the country's homebased internet service providers, and with them access to microblogs, video sites, bulletin boards and the rest, should be within its capabilities.

But would the party dare? In the Arab spring flipping the kill switch was no help to the dictators of Egypt, Libya and Syria. For China, even if its big cities were torn by riots, turning off the internet would seem to run counter to its operating logic: adjust the machinery, intensify filtering, round up far more than the usual suspects, but do not give the people added reason to go out into the streets. The kill switch may be necessary as a last resort, but using it would be an admission of system failure.



China's problems in the real world are mounting. Admittedly the economy remains one of the world's best-performing, with GDP expected to grow by 7.5% this year. Hundreds of millions of Chinese people have become middle-class or even rich, whereas the number of those in abject poverty continues to decline. But corruption, income inequality, pollution and foodsafety scares are far worse now than they were before the internet arrived. Incidents of mass unrest have risen dramatically in the past two decades.

Even among some of the most prosperous Chinese, who have little reason to protest, a more subtle but palpable unease has taken hold. Some of them, including entrepreneurs and government officials, have hedged their bets by obtaining foreign passports and residence permits, buying properties overseas, sending their children to study abroad and sometimes getting their spouses to go with them (the term used for such officials is "naked", meaning there is nothing to hold them in China). Such moves have been spurred by concerns about things like smog, tainted milk and the quality of education, but also by a vaguer sense that the current gilded age cannot last. For some people the train crash was a metaphor for years of unrestrained high-speed GDP growth propelling the country towards a social, environmental and political reckoning.

### Of mice and Chinamen

So far the party's heavy investment in the internet has paid off, allowing the government to acknowledge the problems but keeping things under control. Outsiders often describe China's internet as an ever-evolving game of cat and mouse in which both parties keep getting cleverer. The metaphor is useful up to a point, but ultimately misleading. The Chinese government has a strong interest in catching and silencing the troublemakers among the mice, and this special report has shown how much effort and ingenuity it is putting into achieving this. But it has just as much interest in providing a roomier and more attractive cage for all the mice so that they might make less trouble. To this end it has allowed a distinctly Chinese internet to flourish, with more people getting online-and more of them shopping, watching videos, gaming and chatting with each other, all on trusted Chinese platforms—than in any other country. This customisation of the internet is an important part of building a better cage.

This special report has also shown that the internet is not just a forum where citizens can vent their concerns, it is also a place where the party can listen to them and take part in the discussion. The authorities have come up with serious responses to

events such as the train crash and the recent air pollution. One reason that the train crash has had no further repercussions is that the authorities have heeded people's concerns about safety, reducing the number of trains and their maximum speed so that they are now running smoothly and on time.

If the internet makes the government more responsive to people's everyday concerns, does it matter if the party quickly crushes attempts to organise protests, as it did during the Arab spring? (China's top security official urged at the time that any such efforts be snuffed out "in the embryonic stage", and so they were.) Does it matter that the party continues to stamp on dissidents online, just as it does offline? Some will say that a few human-rights concerns hardly detract from the massive

Microblogging has already transformed Chinese society and the way it is ruled

success story of the Chinese internet. But this misses the point.

The government has indeed provided a roomy and attractive cage, with helpful offitending to it. meanwhile the systemic issues that have contributed to the problems in the real world-such as corruption, unaccountability and a total lack of transparency-continue to fester, destabilising the foundations of authoritarianism.

It is not inconceivable that the entire authoritarian edifice may eventually founder, hastened perhaps by some huge domestic crisis. If the economy were to go into a deep slump, causing massive unemployment, or if some catastrophe were to befall the country that seriously undermined party's legitimacy, the internet could play a dramatic and unpredictable role. Flipping the kill switch to turn it off could have equally unpredictable results (see box, previous page). Until such a moment the authorities

Offer to readers

Reprints of this special report are available. A minimum order of five copies is required. Please contact: Jill Kaletha at Foster Printing Tel +00(1) 219 879 9144 e-mail: jillk@fosterprinting.com

#### Corporate offer

Corporate orders of 100 copies or more are available. We also offer a customisation service. Please contact us to discuss your

Tel +44 (0)20 7576 8148 e-mail: rights@economist.com

For more information on how to order special reports, reprints or any copyright queries you may have, please contact:

The Rights and Syndication Department 20 Cabot Square London E14 40W Tel +44 (0)20 7576 8148 Fax +44 (0)20 7576 8492 e-mail: rights@economist.com www.economist.com/rights

**Future special reports** 

Cars April 20th International banking May 11th Myanmar May 25th Germany June 15th

Previous special reports and a list of forthcoming ones can be found online: economist.com/specialreports

will try to fill in cracks in the edifice of power as the internet exposes them. By doing so they may be able to buy themselves more time, possibly a lot more.

The old way of doing things will not be viable indefinitely; but for now the party is still very much in charge, deciding on the new way of doing things. In that sense Mr Han was right to be sceptical about social media. When, many years from now, history books about this period come to be written, the internet may well turn out to have been an agent not of political upheaval in China but of authoritarian adaptation before the upheaval, building up expectations for better government while delaying the kind of political transformation needed to deliver it. That may seem paradoxical, but it makes sense for a party intent on staying in power for as long as it can.

