THE INTERNET AND CENSORSHIP IN CHINA. RESISTANCE IS FUTILE

Gudrun Wacker

The global nature of the Internet, the wide geographic distribution of its users and the diverse character of its contents leads many policy-makers to believe that activity in cyberspace is beyond the regulation and control of any single state. With specific reference to China, former United States President Bill Clinton once compared controlling the Internet with 'trying to nail Jello to the wall'.[1] China's own President, Jiang Zemin, drew attention to the dangers of spreading 'unhealthy' information and appealed to the international community to develop common mechanisms for 'safe information management' when he gave a speech at an international computer conference in Beijing in August 2000. Editorials in the *People's Daily* speak of 'hostile' forces at home and abroad trying to infiltrate the country via the Internet.[2]

In light of such apprehensions, it is somewhat ironic that the rapid growth of the Internet in China would not have been possible without the support of the country's political leaders, who stress the importance of ICTs and especially the Internet for future economic development and integration into the global economy.[3] The leadership has even gone so far as to mobilise the Internet for political purposes through projects such as 'Government Online', initiated in 1999 to enhance the presence of ministries, administrative units and local government in cyberspace, furthering transparency and accountability by making more information accessible to citizens, and fighting corruption and fraud.[4] The Internet portal Netease, which

operates in Chinese and English, won several awards for an advertising campaign that it ran on Chinese television in the autumn of 2000 under the slogan 'Power to the people'.[5]

This chapter will attempt to unravel this apparent paradox of a Chinese party-state that encourages the spread of the Internet on the one hand, while believing that it can monitor and censor those aspects of activity in cyberspace that it sees as destabilising, dangerous or 'unhealthy' on the other. To do so, it is necessary to look at the ways in which the party-state mobilises its own resources and co-opts the support of voluntary or involuntary collaborators to make the final outcome of the presumed battle between ICTs and the authoritarian state less predictable than Bill Clinton's comparison with jello suggests. If such efforts can be seen to be in any way successful, then the belief that electronic communication over the Internet cannot be subjected to political control has to be called into question.

THE REGULABILITY OF THE INTERNET

Regulation of the Internet is an issue that has been widely discussed in authoritarian and liberal-democratic states alike, centring on the two questions of whether it is necessary on the one hand and technically possible on the other. While there do exist radical proponents of 'digital libertarianism' who advocate unrestrained freedom of activity on the Internet,[6] it would be hard to find any government in the world that does not see the necessity of regulating certain aspects of electronic communication. While the emphasis does of course differ, all governments accept the need to regulate when ICTs threaten their traditional role of maintaining state sovereignty by

preserving a tax base in the face of cross-border e-commerce, ensuring the security of sensitive data, and preventing cyber crime. Even liberal-democratic states tend to accept the need for control when it comes to issues like the dissemination of (child) pornography, racism, the instigation of violence, rightist extremism, and hate speech. It is hardly surprising, then, that laws to regulate activity in cyberspace have been drafted and passed in just about every country. Needless to say, the terrorist attacks on New York and Washington that occurred on 11 September 2001 have given a new urgency to the debate on 'civil liberties versus national security' throughout the world.[7]

Whether such regulation is technically effective, however, is another question, especially given the changing nature of the Internet under the impact of commercialisation. Although commercialisation does lead to ever more complex architecture and wider connectivity on the one hand, it also creates new possibilities for monitoring the activities of users and revealing their identity on the other. So-called 'geo-location programmes', for example, make it possible to locate users geographically by linking IP-addresses to countries, cities and postcodes.[8] The motives behind such developments are complex, including the growing need to be able to enforce the laws of a particular jurisdiction, target advertising, or ensure that a Website pops up in the right language.[9]

In light of the changes in Internet technology under the impact of commercialisation, a number of observers have begun to develop theories that cast doubt on the assertion that there is something inherent in the nature of the Internet that puts it beyond the control of the state. Lawrence Lessig,[10] for example, identifies four elements that

explain the possibility of shaping behaviour in cyberspace, namely regulations, social norms, the market and the architecture of the Internet itself. It is the nature of the last of these factors, the combination of hardware and software that Lessig calls 'code', that is especially important to grasp if we are to understand the degree of political choice available to states when it comes to controlling the Internet. As Lessig explains, when you go into cyberspace you find some places where you need to enter a password to gain access (online services such as AOL, for example), and others where you do not need to be identified. Sometimes the transactions that you enter into leave traces that link them back to you. In some places you can have privacy through the use encryption, while in others this is not an option. All such features are set by the code writers, and can be used to constrain some behaviour by making other behaviour possible or impossible. It is thus the code that embeds certain values or makes certain values impossible. In this sense, code is a kind of regulation, in just the same way that the architectures of real-space codes are a kind of regulation.[11]

It is important to note that Lessig does not deny that there will always be ways to circumvent the constraints imposed by architecture. His point, however, is that we cannot conclude that *effective* control is impossible only because *complete* control is not, any more than the fact that a particular lock can be picked or broken does not prove the total uselessness of locks in general.[12] To find out how cyberspace is regulated, therefore, we need to discover how the code regulates, who the code writers are, and who controls the code writers.[13] From this, it follows that any investigation into the nature of Internet control must extend to the ways in which governments are able to *indirectly* regulate the Internet by *directly* regulating intermediary actors like Internet Service Providers (ISPs) and Internet Content Providers (ICPs).[14]

James Boyle, too,[15] has drawn attention to the ways in which states can regulate the Internet through a combination of privatised methods of enforcement and state-sponsored technologies by appealing to the theories of Michel Foucault concerning the subtle private, informal and material forms of coercion that are enforced through 'surveillance' and 'discipline'.[16] Such a vision is illustrated by the concept of the Panopticon, a prison in which every cell has a window facing a central tower from which an unseen warden just might be watching what any individual prisoner does at any time. The prisoner thus has to act *as if* he is under constant surveillance all the time, even though such surveillance is not physically possible for the single warden. By applying such a model to the kinds of technologies that are being built into the Internet, Boyle argues that effective censorship has indeed become possible.

Take common measures adopted in liberal-democratic states to enable individual Internet users or ISPs to shield people from undesirable content, such as software used to stop children from gaining access to pornographic Websites. SurfWatch, CyberPatrol, NetNanny or CyberSitter, for example, all contain lists with Internet addresses of 'forbidden' Websites and filters to block access when specific words or phrases are detected. Such activity, moreover, is encrypted and thus invisible to the user. Similarly, under the system of self-description known as 'Platform for Internet Content Selection' (PICS), suppliers can build specific information into Websites containing details such as the age group for which specific content is recommended. However, as Boyle argues, the very fact that such systems are claimed to be 'value neutral' means that their political impact will depend on who is using them, because 'The third party filtering site could be the Christian Coalition, the National

Organization for Women or the Society for Protecting the Manifest Truths of Zoroastrianism'.[17]

It is important to realise that such technical solutions enable states to enlist private or commercial parties to carry out tasks that the state itself is either not allowed to carry out for constitutional reasons, or is unable to carry out due to its limited capacities. In fact, commercial ISPs and ICPs are far more susceptible to pressures from states in this respect than are individual Internet users, because they are not so able to operate independently of a geographical base or a real identity. When, for example, ISPs are made legally liable for any copyright infringements committed by their customers, they have to respond by erecting 'digital fences' to prevent unauthorised copying. Similarly, if encryption technology that is developed to enable activities such as online banking might also enable dissidents and human rights organisations to communicate free from state surveillance, states can still normally justify legislation allowing them to gain access to electronic communications on the grounds that encryption can also be used to organise criminal activities.[18]

The kinds of developments indicated by writers like Lessig and Boyle should, then, be taken as warnings that the exercise of state power and control in cyberspace is not always easy to recognize. The methods used by states often appear to be 'natural' and integral parts of electronic communication media themselves, which they do not necessarily have to be. It is certainly premature to write off the ability of states to bring the Internet under control, when efforts to regulate and control cyberspace have been going on in practically every country, and governments have found allies in the form of commercial enterprises developing appropriate technologies. As Qiu points

out, from a global perspective, the kinds of measures imposed by the Chinese government to achieve 'virtual censorship' are not so special, reflecting as they do 'the emerging attempts of legislatures, governments and various administrative organs worldwide to incorporate the cyberspace into their sphere of jurisdiction'.[19] In this light, it is important that we take into account the complex relationships that exist between the kinds of factors of control listed by Lessig and Boyle in any attempt to understand how the Chinese state censors the Internet.

NATIONAL REGULATIONS

While regulation of the Internet in China is partly based on laws that pre-dated its existence, a series of specific regulations has also been introduced,[20] probably encouraged by the approach of WTO accession. Despite the ongoing streamlining of the state apparatus, formulating this mass of regulations has involved a confusing number of ministries and administrative units.[21] Many are intended to benefit Internet users, such as measures protecting consumers by governing online trading in pharmaceuticals and online educational services, or upholding intellectual property rights and individual privacy. In this respect, regulation in China is not so different from that found in other countries, and such provisions cannot be exclusively interpreted as efforts to stamp out political dissent.

More directly related to questions of control and censorship, however, are various provisions that were included in a raft of regulations that was introduced in the year 2000 to govern telecommunications and the publication of news and electronic information on the Internet. These will be listed below under the categories of

‘forbidden contents’, ‘restrictions on the distribution of news’, ‘licenses’, ‘storage of user data’, ‘surveillance’, ‘judicial liability’, and ‘penalties’:

1. *Forbidden contents*: Since the list of contents that are banned from distribution or electronic publication gives a full overview of the government’s targets in controlling cyberspace, it is worth citing this in its entirety:

> Any information that involves the following is forbidden:
>
> (1) Contradicts the principles defined in the constitution [of the PRC].
>
> (2) Endangers national security, discloses state secrets, subverts the government, destroys the unity of the country.
>
> (3) Damages the honour and the interests of the State.
>
> (4) Instigates ethnic hatred or ethnic discrimination, destroys the unity of [China’s] nationalities.
>
> (5) Has negative effects on the State’s policy on religion, propagates evil cults or feudal superstition.
>
> (6) Disseminates rumours, disturbs social order, undermines social stability.
>
> (7) Spreads lewdness, pornography, gambling, violence, murder, terror or instigates crime.
>
> (8) Offends or defames other people, infringes upon the rights and interests of other people.

(9) Other contents that are forbidden by law or administrative regulations.[22]

It should be noted that this catalogue of prohibited contents is not new. In a slightly more general form, it can be found in the regulations for the publishing industry issued in 1997.[23] Since contents banned on the Internet are nearly identical with those prohibited in other media, it can be concluded that the Internet and electronic information services are basically treated like other means of publication.

2. *Restrictions on the distribution of news*: In principle, the regulations prohibit the distribution of news through the Internet, unless this news has either been published on the Internet by the official state-owned media or the news departments of state institutions themselves, or has already been published by authorised media in another form. If a pure Internet portal wants to publish news via the Internet, it not only has to fulfil specific requirements (such as a professional editorial board, sufficient financial means and technical equipment), but also has to enter into a formal co-operation with one of the state-authorised media. The co-operation agreements have to be filed with the authorities in charge. The source and date of any published news has to be cited in each case. As for the question of whether Internet portals can publish news and articles by their own journalists, contradictory statements were made prior to the regulations and there is still a lack of clarity over this.[24] With respect to links to foreign news sites or the publication of news taken from foreign media – some portals had signed agreements with foreign information services like Dow Jones and others – the

regulations stipulate (§ 14) that the prior consent of the Information Office of the State Council is necessary.

The way in which these rules try to kill two birds with one stone should be noted. On the one hand, they have a political or ideological purpose of containing and directing the proliferation of news material into relatively manageable channels. On the other hand, they aim at securing the economic interests of the official media vis-à-vis pure Internet portals operating in Chinese, such as Sina, Netease or Sohu, which have become very popular due to their early Web presence and timely and attractively presented news services. Faced by such competition, 'traditional' state-owned media such as *People's Daily* and the *Xinhua* (*New China*) news agency formed an interest group as early as 1999. Pointing to the risks created by allowing the Internet portals too much freedom, they protested and appealed for official support from the State to improve their own Web presence. Fighting news piracy was one of the main issues on their agenda.[25] In order to strengthen the competitive position of such official organs, the State Council granted special funds (USD 121 million) to the most influential among them for launching and improving their own Internet presence.[26] One of the tasks of the 'Management Office for Internet Information' (*Guowuyuan Xinwen Bangongshi Wangluo Xinwen Guanliju*) established in April 2000 under the Information Office of the State Council, is to improve the online presence of such media.[27] There is thus a tight relationship between the economic and ideological dimensions of the regulations, since strengthening the presence of the state-owned media also helps to ensure that the supply of Internet news content is in line with what the state wants.

3. *Licenses:* Comprehensive and detailed rules on licenses force providers of Internet services to apply for a range of special permits. These have to be obtained from different authorities, with a separate licence necessary for each category of service. The official registration numbers have to be displayed clearly on the Website in question. It is not permitted to expand the business activity covered by such a licence without prior consent. All Internet cafés have to register with the local Public Security Bureau. Moreover, by requiring businesses to meet certain preconditions in terms of personnel, financial and technical equipment, market entry costs have been raised in ways that leave smaller independent Internet companies that have no official backing in a disadvantageous position compared to the big players. In this way, the 'market' (according to Lessig's categorisation) is brought into play in a legal way as a restrictive factor.

4. *Storage of user data*: ISPs are required to store all user data. This does not only include the registration or customer number of the user, but also which telephone number is used for logging on, which Web addresses or domains are visited during the session and for how long. The data has to be stored for sixty days and be disclosed to the authorities on request. Providers of electronic information services, such as ICPs offering BBS (bulletin board service), chat room and discussion forum services, have to store all contributions published on the Internet, including time of publication and Web address or domain name, and keep such data for sixty days. Postings from users that violate any of the rules on banned contents have to be deleted from the Internet immediately. At the same time, however, they have to be locally stored and reported back to the authorities.[28]

5. *Surveillance*: Reports in the foreign media have claimed that regulations introduced in January 2002 are the most intrusive so far for requiring ISPs and ICPs to screen e-mails.[29] However, it should be noted that the wording of the passages quoted above could also be interpreted as implying that providers are *not* allowed to screen the non-public communications of their customers, such as e-mail.

6. *Judicial liability*: Providers of electronic information services have to notify their users or customers of the legal responsibilities that apply when posting and uploading information or contributions.[30] For the published contents, final responsibility rests with the respective author.[31] This is in contrast to Singapore, where it is ICPs that are made liable for all contents published within their business sphere.[32] The service providers can be held liable in China, though, if they operate without the required business licenses, fail to meet their obligations with respect to the storage of data and notification of the authorities,[33] and also if they fail to protect personal data by passing them on without the prior consent of the respective user (although there are many exceptions to this stipulated by law, of course).

7. *Penalties*: With respect to ISPs and ICPs the regulations provide for reprimand, rectification and fines, and even for the closure of Websites in serious cases. If, for example, the licence number is not visible on a Website, a fine of RMB 5,000-50,000 can be imposed. If the obligation to delete contents violating the regulations and to notify the authorities of the violation is not met, the penalty can be

revocation of the business licence.[34] As for the penal consequences of violations by ISPs, ICPs and individual users, the regulations refer to the 'relevant laws'.[35]

In sum, we can see that this raft of recent regulations constitutes an effort by the Chinese government to make a more pro-active Internet policy and to provide itself with better instruments for influencing activities in cyberspace. This comprises not only content restrictions on the 'ideological' level, but also administrative and economic requirements which strengthen the official media as well as consolidating the advantages of bigger and financially well-equipped Internet enterprises.[36] Through these measures, and by offering more contents through projects like 'government online', the party and the government hope to be able to actively set the agenda for the Internet in China.

INFLUENCING NORMS OF BEHAVIOUR

When looking at the measures taken to enforce regulations by the Chinese state in the realm of the Internet, the number of 'political' cases (as against cases such as breaking into banking networks) with penal consequences has been rather modest so far, with between ten and twenty people arrested and sued as of mid-2001.[37] The first of these to be made public was the case of Shanghai businessman Lin Hai, who in early 1998 sold 30,000 e-mail addresses in China to a New York-based organisation that distributes the pro-democratic newsletter *VIP Reference* (*Dacankao*) via e-mail in China. The involuntary recipients of this service included some high-ranking party officials. Lin, who claimed that his actions were strictly profit-driven, received a two-year sentence, but was released early.[38] Another high-profile case was that of Huang

Qi, who established the Website 'www.6-4tianwang.com' for relatives of missing persons, for which he had even received official praise after clearing up some cases of abduction. However, when contributions to the site began to commemorate the events that occurred in Tiananmen Square on 3-4 June 1989, the authorities closed down the Website and arrested Huang, who was accused of attempting 'to subvert the government and destroy national unity'.[39] Other known cases include that of a teacher in Nanchong who owned an Internet café and was arrested in August 2000 in relation to BBS-contributions criticising the Communist Party.[40] The organisers of the officially closed Website of the 'New Culture Forum' (www.xinwenming.net) were reportedly being sought by the authorities in the autumn of 2000.[41]

The Falungong spiritual movement has become the most prominent example illustrating the subversive potential of using the Internet from the perspective of the Chinese government. It has been claimed that electronic means of communication like e-mail played a central role when its members secretly planned and organised a mass demonstration in April 1999, right in front of the CCP's headquarters at Zhongnanhai, Beijing, which seems to have caught the Chinese leadership completely by surprise. The group, whose spiritual leader lives in the United States, certainly propagates its ideas on a number of Websites outside China. When the movement was declared illegal after the demonstration in Beijing, a fairly orthodox campaign to criticise it was accompanied by the transformation of cyberspace into something of an electronic battlefield as the authorities sought to paralyse servers housing the group's Websites through measures such as 'email bombs', flooding them with large amounts of meaningless data. Access from China to the IP addresses of the group's Websites in the United States, Canada and the United Kingdom was also blocked.[42] In fact, the

majority of charges for 'political' offences in cyberspace might well be in relation to Falungong. For example, several students of Beijing's Qinghua University were reportedly charged in 2000 and 2001 and sentenced to long jail terms for posting articles criticising government policy with respect to Falungong and for downloading and distributing material related to the movement.[43]

In general, this kind of censorship can be divided into proactive and reactive measures. The blocking of Websites is an obvious case of proactive censorship, and is applied mainly for Websites operated by foreign news services like CNN, the BBC or international human rights organisations. Judging from available reports, such blocking seems to be rather erratic and unsystematic. The *New York Times*, for example, was blocked until it published a lengthy interview with President Jiang Zemin.[44] It is sometimes possible to access the *International Herald Tribune*, the *Far Eastern Economic Review* and even *Human Rights in China*, but not always.[45] Blocks are sometimes temporarily lifted on special occasions. One such event was the October 2001 APEC summit in Shanghai, when foreign media sites were unblocked during a phase of (nearly) 'total digital freedom'.[46] It should also be noted that certain IP addresses have become unreachable at times due to bottlenecks in international data traffic. While bandwidth capacity has been enormously expanded during recent years, the number of Internet users in China has grown even faster.[47]

The phenomenon of Internet cafés also poses a problem for state control as they have become increasingly popular, especially in China's cities. During the sessions of the National People's Congress and the Chinese People's Political Consultative Conference in Spring 2001, some delegates motioned for closing down all of these,

arguing that they are harmful for children and young people. The discussion centred mainly on the 'online poisons' of pornographic material and online gambling.[48] Internet cafés have been raided several times by security forces, with crackdowns aimed at identifying places that are operating without a proper business license on the one hand, and at stopping access to 'unhealthy' Websites on the other, especially for the young.

In this respect, it should be noted that Internet cafés are not only required to apply for a business licence and register with the local Public Security Bureau, but also to hire appropriate personnel to monitor the activities of users, who themselves are supposed to show an ID and register their details.[49] Following a decree from the State Council for a 'cleansing' campaign of Internet cafés between April and June 2001,[50] it was reported that some 8,014 institutions were closed, with about 2,000 of them permanently shut down and 6,000 temporarily undergoing 'rectification'. All in all, 56,800 Internet cafés were inspected on a national scale.[51] According to new rules issued in May 2001, Internet cafés are now required to keep a minimum distance of 200 metres from government offices, army units and party organisations, as well as from primary and middle schools.[52]

Surveillance of the activities of ISPs has also begun to be more systematic. In March 2001, reports began to appear on sample checks conducted among four large ISPs in Shanghai to see if their customers held the necessary licences for their Internet presence. The result of the survey was declared to be satisfactory, with between 80 and 95 per cent of the Internet services registered as required.[53] The ability of the state to carry out such exercises is steadily being increased by beefing up the relevant

personnel required to meet the challenges of the digital age. This includes the creation of special police units, which first appeared in Anhui province in August 2000, and have since spread to other regions and cities. These forces are charged with the central tasks of fighting cyber crime, ensuring IT security through work such as providing information and consultancy on computer viruses, and 'keeping order' in cyberspace.[54]

The physical ability of the state to surveil and punish is not necessarily the most important factor when it comes to maintaining 'security' in the realm of information technology, however. As Winkel points out, the concept of security in this field must be understood in terms of the 'objective security' that is derived from the reliability of social and technical functions, and the 'subjective security' that arises from the state of consciousness that is determined by individual perception and social communication. This becomes crucial in relation to the use of the Internet for political dissent, when we realise that 'The development of trust in a technology is a precondition for its acceptance, that is, for its being embraced and used by the people concerned'.[55]

The issue of trust may not be such a salient concern in liberal-democratic societies, where the monitoring activities of non-state actors are less likely to be associated with state intervention or coercive measures in the minds of users, and therefore ignite little protest. Most Internet users in the United States or Europe have probably never given much serious thought to the kinds of technological capacities for storing user data and carrying out surveillance that are available. They most likely do not care too much so long as there exists a significant degree of 'trust capital' in the operation of modern

information technologies. Even if the individual user does wonder about what happens to the electronic traces he or she might leave in cyberspace, one would normally assume that these traces will not have any legal, let alone penal, consequences.

In an authoritarian state, where citizens have lived with censorship for decades, the issue might present itself in a different light. Doubts with respect to 'availability', but even more so with respect to the 'confidentiality' of electronic information, would suggest a lack of 'trust capital' and a good amount of insecurity concerning the capacities of the state (and its helpers) to watch what is going on in cyberspace. Just as in the Panopticon cited by Boyle and Foucault, the perception that one just might be under observation is likely to be more important in ensuring conformity with the rules of behaviour than whether one is actually being observed at any specific point in time. Such a vision could explain why the majority of censorship measures in Chinese cyberspace are in fact rather limited. Police forces and courts only need to become active sporadically if high-profile arrests and sentences can be made to constitute an effective deterrence by demonstrating the risks associated with dissident behaviour. The trick for the state is thus to nurture an attitude of 'voluntary' self-control and self-censorship among users, a 'firewall within one's head' as the *People's Daily* puts it.[56] The regulations need not necessarily be enforced in a strict sense to achieve this. In fact, it may actually be to the benefit of the state to leave a degree of vagueness in the terminology it uses, interpreting regulations in as loose or as strict a sense as is necessary to ensure that users and providers will always err on the side of caution when it comes to assessing the risks of dissent. For example, practically any kind of information can be declared to be a 'state secret' in China, even seemingly harmless

statistical data on the last grain harvest.[57] In this way, laws become a mere supplement to much more subtle means of psychological control.

THE ROLE OF THE MARKET

Another factor that plays a crucial role for exerting control over the Internet is the emerging alliance between the state on the one hand, and the official media, state-owned enterprises and financially strong investors on the other. Qiu describes the emerging relationship well when he explains how China's Internet industry has become characterized by the rapid formation of an authoritarian-capitalist coalition that has seized the central spot that used to belong to small-to-medium sized enterprises. The new arrivals are not only strengthened by traditional media conglomerates that serve as the mouthpiece of the party-state, but also by the close networking that takes place between wealthy investors and powerful political figures from both inside and outside the country that has developed in the context of commercialization without political democratization.[58]

The support of the state for the official media and large enterprises like Legend Computers in the IT sector, in addition to legal requirements that are imposed with respect to finances and personnel, leads to the marginalisation of smaller providers. Moreover, Internet firms that do not want to endanger their market position are well advised to play by the rules set by the state. Managers of Internet portals have thus expressed no surprise over the raft of regulations that were introduced in 2000, with one operator explaining the bottom line as being that, '[T]he new regulations don't make anyone happy, but they're completely expected and in line with other Chinese

government policies. Anyone who was not already in de facto adherence with the policies was being very naïve'.[59] In fact, Internet providers had hurried to comply with draft versions of the regulations before they even came into force, revealing how they have to walk a tightrope between the interests of their customers and the demands of the state when operating in China. As an American representative of the Chinese-language portal Sina.com puts it, 'We are playing that role, to let people talk about sensitive issues but also to help the government manage the flow of ideas'.[60] Due to the vague wording of the regulations and their incoherent or arbitrary enforcement, Internet providers have to err on the side of caution when trying to decide what the authorities are prepared to tolerate.

This situation means that ICPs offering BBS services or chat rooms have to use the whole array of methods described by Boyle to indulge in self-censorship. Filter software that can block access to a certain Website or sound the alarm if it contains the word 'nipple' or one of its synonyms can also be programmed to do the same for the name of Taiwan's President or the word 'Falungong'. Such is the nature of 'neutral' technology, much of which is supplied by Western firms eager to supply the Chinese market with software and technology. Among others, Cisco Systems, Sun Microsystems, Nortel Networks (Canada), Dupont, and Daniel Data Systems (Israel) are known to have displayed their products at the trade fair 'Security China 2000', organised with the cooperation of the Ministry of Public Security. The advanced firewall software and other technical solutions offered by such firms is not only useful for protecting police networks from hacker attacks, but also for screening millions of electronic messages for key words. In fact, the focal point of the fair was a government project called 'Golden Shield'[61] that aims to safeguard the security of

computer networks and fight cyber-crime by connecting together the databases and surveillance systems of national and local police stations. It is ironic, therefore, that while the Western media frequently criticise China for obstructing the development of the Internet, it is Western firms that are supplying the technological means which enable China to carry out surveillance. In the meantime, Chinese companies have also started to develop special monitoring and filter software for themselves.[62] Early in 2001, for example, the Ministry of Public Security introduced an 'Internet Police 110' software package to be supplied in various versions for schools, individuals and Internet cafés that is supposed to filter out 'unhealthy' information, including not just violence and pornography but also anything positive about the Falungong or Tibetan exile and human rights groups.[63]

ISPs and ICPs employ special personnel, or 'big mamas', to look closely at the postings and contributions that filter software identifies as suspicious, in order to either delete them or clear them as being appropriate for the Internet. The personal decisions of Webmasters are thus a key element among the series of factors deciding on what gets onto the Internet and stays there.[64] One important form of 'punishment' for those who break the rules is simply to be eliminated from the Net, with no explanation necessary. Webmasters and system administrators can, moreover, criticise or reprimand authors for posting controversial contributions. If an author repeats his behaviour, then his IP address or registered name can be permanently blocked, amounting to the termination of their virtual existence.[65] While such punishments can be meted out in cyberspace, additional deterrence credibility is gained from the possibility of harsher 'real-world' sanctions in cases of what are considered to be grave violations.

The Internet branches of the important official media probably enjoy more freedom than Internet portals whose position is politically uncertain when it comes to deciding on the borders of what is allowed precisely because their censors know what the government line is. This goes some way to explaining why a particularly popular forum for debate is the *Strong State Forum* (*Qiang guo luntan*) on the *People's Daily* Website.[66] While BBS s and the chat rooms of university networks or Internet portals seem to be closed down as a precaution when a sensitive anniversary such as 4th June, the date of the Tiananmen Massacre, or when a new event triggers a fierce online debate, this has not so far happened to the *Strong State Forum*. An explosion at a school in Jiangxi province, for example, led to an intense discussion in cyberspace, with many postings calling into question the official government version of the incident, which blamed it on the actions of a lunatic. When too many comments with critical undertones appeared on Sina.com's online discussion forum, however, it was temporarily shut down.[67] Another method reported to have been used to stifle debate is to reduce data transfer speed before sensitive dates approach,[68] although this has the drawback of affecting state-run Websites as well.

Topics banned from public discussion include the Tiananmen Square events of June 1989, the Falungong movement and any explicit criticism of China's leaders. As for current events like scandals concerning official corruption, decisions are made on a case-by-case basis.[69] That there seems to be more toleration for comments on international incidents than on domestic affairs indicates that the Internet provides a welcome and officially tolerated outlet for nationalistic sentiments,[70] as long as the postings are not directed against the Chinese government and do not challenge state

policies. The collision of the American EP-3 reconnaissance plane and a Chinese F-8 fighter off the Chinese coast in April 2001, for example, triggered a deluge of commentaries and personal statements in Chinese cyberspace. The overwhelming majority of these postings expressed a clear-cut anti-American attitude and most of them supported the position of the Chinese government. Within this context, one online comment pointed out that censorship measures were responsible for this nearly complete uniformity of opinions on the Net.[71] One analysis of postings made during this incident seems to corroborate the impression of uniformity, but also notes that a few critical contributions did appear, especially on the popular Chinese Internet portals Netease.com and Sina.com.[72]

As was to be expected, the terrorist attacks of 11 September 2001 in the United States sparked a hot debate in China as well. In the days directly following the attacks, the majority of the postings on *Strong State Forum*, despite deploring the death of so many people, expressed the view that these attacks were the logical result of the unilateral and 'hegemonistic' policy of the United States and that terrorism was nothing but the reverse side of hegemony and power politics. Others argued that the terrorist attacks were the outcome of a type of globalisation that, under the leadership of the United States, had widened the gap between rich and poor in the world.[73] That appeals for people to refrain from downright anti-American postings began to appear after a few days should be understood in the context of the Chinese leadership's decision to interpret the formation of the United States-led anti-terrorist coalition as an opportunity to improve Sino-American relations, making a wave of anti-American sentiment within the population less desirable than before.

COUNTER STRATEGIES

It would be unrealistic to claim that the array of methods used by the state to ensure its control over the Internet provide a watertight system, when spaces for the development of counter strategies certainly do exist. For example, it is common in China for regulations to be only loosely enforced. Some Internet cafés also operate without the required business licenses, making them less likely to insist on the proper identification and registration of their customers. Moreover, Internet users can and do find ways to outsmart government blockades and restrictions through methods such as using proxy-servers outside China to access banned addresses.[74] Lists of the IP addresses of proxy-servers are reportedly distributed among Internet users in China, sometimes via e-mail. Members of the Falungong movement are also supposed to have learned how to circumvent blockades and protect their electronic communication using encryption programmes.[75] There has been at least one occasion on which commercial interests appear to have weakened the hold of the state, when the government tried to gain control over the usage of encryption by passing a new regulation in December 1999. Strong objections from Western firms like Microsoft led to the measure being considerably watered down.[76]

However, the state has so far also proved resourceful in its attempts to close such gaps. The IP addresses of proxy-servers can themselves be blocked, for example. Security agencies are even said to circulate false IP-addresses for such servers, so that attempts to get round blockades might end up being routed directly to the Public Security Bureau.[77] Moreover, the international priority given to strengthening

surveillance of the Internet following 11 September does not seem to be encouraging such challenges to state control by foreign commercial actors. This point is well illustrated by the case of SafeWeb, a United States-based software company that developed 'Triangle Boy', a method for maintaining anonymity in cyberspace. In August 2001, it was reported that International Broadcasting Bureau, the parent company of Voice of America, had entered into negotiations with SafeWeb to finance a project to undermine China's efforts to censor the Internet. [78] Soon after 11 September, this venture ran into problems as the atmosphere in the United States became far more sympathetic to efforts to strengthen online surveillance, although SafeWeb is reported to be keeping its services for Voice of America going on a trial basis.[79]

An additional advantage for the state is that a certain level of technical knowledge and sophistication is necessary for employing the methods of circumvention described above, and even users with the requisite expertise have to ask themselves whether they are willing to take the risk involved in actually using such skills. According to official statistics, the vast majority of Internet users are young male urban citizens with more than average education and more than average income.[80] Their main motives for accessing the Internet are to gather information, access educational services and for entertainment. Although surveys on Internet usage in China that have been conducted since 1997 used to reveal that lack of Chinese-language information on the Internet was one of the most frequently mentioned complaints, this problem has now gone down in importance, not least due to state-sponsored initiatives such as 'government online' and the development of a significant Web presence for the 'traditional' state media. This expansion and improvement of information and

entertainment offered in the Chinese language, largely provided on the Internet by organisations with strong links to the state, clearly reduces the need to look for alternative sources and activities in cyberspace. [81]

It remains far from clear just how interested the average Chinese Internet user is in accessing information and activities that could be deemed politically subversive, with empirical evidence still very sketchy. At least two surveys have been conducted on opinions in urban areas,[82] but many more in-depth analyses will be necessary to get a clearer picture of online behaviour in China and of how the different forms of electronic communication are used and how this relates to the off-line world. Statements made by young people and students suggest that they see accessing blocked sites as a kind of game, with politics not being their core interest.[83] A strong enough motivation to seriously risk not only one's 'virtual' existence, but also one's real existence, by engaging in dissenting activities on the Internet can only be readily assumed for groups like the Falungong, which operate outside the law anyway. There is thus a real danger that the impression generated by the Western media of Chinese cyberspace as the stage for a battle between a repressive state and Internet users ceaselessly posting and hunting for politically subversive information restricts our perspective to a very small and possibly insignificant aspect of the overall situation. The majority of observers who have followed and analysed the development of the Internet in China in more depth do not support the picture of a state rendered powerless over an uncontrollable Internet, but tend to conclude that the authorities are able to exert their control over online users as much by simple intimidation as by sophisticated electronic surveillance or by blocking direct access to politically suspect foreign Websites.[84]

IS RESISTANCE FUTILE?

In light of the above evidence, it is safest to conclude that while the Internet in China cannot be protected from every form of subversive usage by insurmountable 'digital fences', state control and censorship have not simply evaporated either. Instead, the state is meeting the challenges of the digital age by combining the kinds of factors of control elaborated on by writers like Lessig and Boyle. This involves a complex interplay between the state and the key commercial actors in the sector, namely ISPs, ICPs and the official media, most of which are partly or wholly owned by the state anyway. By practising self-censorship and executing the duties of surveillance and supervision assigned to them by the state, such actors partially relieve it of the task of control and censorship. All this becomes possible through the technological embedding of control in the architecture of the Internet itself, which is nothing specific to China, but mainly the result of the commercialisation of the Internet worldwide. The introduction of regulations is only really necessary to complement this strategy by increasing the deterrence effect of feeling that one's actions just might be under observation and by making examples of high profile cases in the courts.

This does not mean that the Internet is politically irrelevant, just that it is not likely to be the cause of significant social change. Instead, the freedom of expression in China has expanded considerably since the end of the late 1970s due to the overall policy of 'reform and opening' initiated by Deng Xiaoping, despite intermittent phases of contraction.[85] Thus, what can be said of the Internet can be said of other media in China as well, namely that the limits of toleration are constantly being tested and re-negotiated. The common practice of conducting activities under the cloak of pseudonyms in Chinese cyberspace and the relative weakness of 'virtual' sanctions might still make the Internet more of a catalyst of social change than other media, but it is most likely to play a significant role if a social or political movement emerges in the non-virtual world. It is then that, along with fax machines, mobile phones, and mails via mobile phones, the Internet's ability to distribute news and facilitate organisation could play a decisive role. However, there is little reason to believe in the kind of technological determinism that postulates that the Internet could trigger a democratic or other mass movement in China by itself. The Internet might ignore territorial boundaries or surmount them without much effort (although even this has begun to change), but this does not mean that it exists in a social and political vacuum, detached and independent of its environment.[86]

---

[1] Clinton's statement is cited in W.J. Drake, S. Kalathil and T.C. Boas, 'Dictatorships in the Digital Age: Some Considerations on the Internet in China and Cuba', *iMP*, October 2000. Online. Available HTTP: <http://www.cisp.org/imp/october_2000/10_00drake.htm> (accessed 11 November 2000).

[2] See 'Jiang looks to information technology to drive economy', *China IT and Telecom Report*, 25 August 2000, vol.1, no.45, pp. 4-5; A. Lin Neumann, 'The Great Firewall', *CPJ Briefings: Press Freedom Reports.* Online. Available HTTP: <http://www.cpj.org/Briefings/2001/China_jan01/China_jan01.html> (accessed 23 February 2001). In March 2001, an article in *People's Daily* divided 'unhealthy' Internet contents into 'black' (false information from hostile forces, intended to 'destroy' and 'westernise' China), 'grey' (a flood of meaningless blabbing, negative sentiments and vulgar thoughts) and 'yellow pollution' (pornography). See 'Party Daily Calls for Action Against Internet Pollution', *Renmin Ribao* Web site, March 21, 2001, in *BBC Summary of World Broadcast – Far East* (*SWB FE*), 28 March 2001, no. 4106, p. G/7.

[3] See Xiudian Dai's contribution to this book for more details on this issue.

[4] Dali L Yang, 'The Great Net of China'. Online. Available HTTP: <http://www.mfcinsight.com/article/010209/oped4.html> (accessed 16 February 2001); Zhang Junhua: 'China's "Government Online" and Attempts to Gain Technical Legitimacy', *Asien*, July 2001, no. 80, pp. 93-115.

[5] '*Wang ju ren de liliang*', literally 'the Net concentrates the power of people'. See Chinese Web site of Netease. Online. Available HTTP: http://news.163.com/editor/010220/010220_109937.html (accessed 26 March 2001).

[6] For a summary of the arguments of 'digital libertarianism', see J. Boyle, 'Foucault in Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors', 1997. Online. Available HTTP: <http://www.wcl.american.edu/pub/faculty/boyle/foucault.htm> (accessed 6 November 2000). A definition of 'digital libertarianism' can be found under http://www.feedmag.com/html/feedline/97.09marshall/97.09marshall1.2.html (accessed 19 April 2001): The proponents of this approach argue, on the one hand, in

favour of the non-interference of the state in cyberspace, while on the other they claim that the Internet is characterised by certain features which are beyond the control of the state. Three main groups can be identified: computer enthusiasts, (hackers who want to keep 'their' Internet for themselves); traditional liberals who want to limit state interference; and economically oriented conservatives, who consider the global reach of the Internet as desirable since it weakens the regulatory powers of governments.

[7] See, for example, N. Robinson, 'New laws seek to balance privacy and surveillance', *Jane's Intelligence Review*, January 2002, vol. 14, no. 1, pp. 52-53; C.S. Kaplan, 'Concern Over Proposed Changes in Internet Surveillance', 21 September 2002. Online. Available HTTP: <http://www.nytimes.com/2001/09/21/technology/21CYBERLAW.html> (accessed 21 September 2001).

[8] See, for example, 'Putting it in its place' and 'The Internet's new borders', *The Economist*, 11 August 2001, pp. 18-20 and pp. 9-10; A.E. Cha, 'Bye-Bye Borderless Web: Countries Are Raising Electronic Fences', *International Herald Tribune*, 5 January 2002, pp. 1, 4.

[9] 'Putting it in its place', p. 18.

[10] L. Lessig, *Code and OtherLaws of Cyberspace*, New York: Basic Books, 1999.

[11] Ibid., Lessig, p. 89.

[12] Ibid., p. 57.

[13] Ibid., p. 60.

[14] Ibid., p. 97.

[15] For the following observations see Boyle, 'Foucault in Cyberspace'.

[16] M. Foucault, *Discipline and Punish. The Birth of the Prison*, London: Penguin, 1991. Especially Part 3, Chapter 3: 'Panopticism', pp. 195-228.

[17] Boyle, 'Foucault in Cyberspace'.

[18] For United States initiatives, such as the Clipper Chip, see Lessig, *Code and Other Laws of Cyberspace*, pp.47 ff.; A.L. Shapiro, 'The Internet', *Foreign Policy*, Summer 1999, no. 115, pp. 18-9. On a controversial draft in England in 2000 see C. Grande, 'Uunet and Nokia attack e-mail legislation', *Financial Times*, 12 July 2000, p. 12. Providing the state with access to encryption has been compared to forcing all citizens to deposit a key to their house at the police station, so that security forces could enter it if they suspect a burglary has taken place.

[19] J. Linchuan Qiu, 'Virtual Censorship in China: Keeping the Gate between the Cyberspaces', *International Journal of Communications Law and Policy*, Winter 1999/2000, issue 4. Online. Available HTTP: <http://111.ijclp.org/4_2000/ijclp_Webdoc_1_4_2000.html> (accessed 10 November 2000), p. 22.

[20] Ministry of Information Industry, 'Zhonghua Renmin Gongheguo dianxin tiaoli' (Telecommunication Regulations of the People's Republic of China), 25 September 2000, *Guowuyuan gongbao* (*GWYGB*), 2000, no. 33, pp. 11-21. Also Online. Available HTTP: <http://www.mii.gov.cn/news2000/1013_1.htm> (accessed 2 December 2000); State Council, 'Hulianwang xinxi fuwu guanli banfa' ('Methods for the Administration of Internet-Based Information Services'), 20 September 2000, *GWYGB*, 2000, no. 34, pp. 7-9. Also in *People's Daily*, 7 November 2000. Online. Available HTTP: <http://www.peopledaily.com.cn/GB/channel5/28/200010017/2557566.html> (accessed 24 October 2000)]; State Council Information Office, Ministry of

Information Industry, ‘Hulianwangzhan congshi dengzai xinwen yewu guanli zhanxing guiding’ (‘Interim Provisions for the Administration of Release of News by Websites’), 6 November 2000, *GWYGB*, 2001, no. 2, pp. 46-8; Ministry of Information Industry, ‘Hulianwang dianzi gonggao fuwu guanli guiding’ (‘Provisions for the Administration of Electronic Information Services on the Internet’), 8 October 2000, *GWYGB*, 2001, no. 2, pp. 45-6; Standing Committee of the National People’s Congress, ‘Guanyu weihu hulianwang anquan de jueding’ (‘Resolution of the Standing Committee of the National People’s Congress on Maintaining Security of Computer Networks’), 28 December 2000, *GWYGB*, 2001, no. 5, pp. 21-3. An excellent summary and evaluation of the main contents can be found in K. Giese, ‘Das gesetzliche Korsett für das Internet ist eng geschnürt’, *China aktuell*, October 2000, pp. 1173-81.

[21] On the administrative structure see Xiudian Dai’s chapter in this volume. In addition, a whole number of ministries, government institutions and administrative units – such as the Ministry of Public Security, the ministries of Culture and of Health, the State Administration for Industry and Commerce and many more – have a say in drafting Internet regulations relevant for their respective domains.

[22] This list can be found as § 15 in ‘Hulianwang xinxi fuwu guanli banfa’, § 9 in ‘Hulianwang dianzi gonggao fuwu guanli guiding’ and § 13 in ‘Hulianwangzhan congshi dengzai xinwenyewu guanli zhanxing guiding’.

[23] State Council, ‘Chuban guanli tiaoli’ (‘Regulations Governing the Administration of the Publishing Industry’), 1 January 1997, *GWYGB*, 1997, no. 2, pp. 38-46. In fact, in these regulations electronic publications were already explicitly mentioned as falling under their jurisdiction (§ 2). The banned contents, which also include ‘superstition’, can be found in § 25. New regulations for the publishing industry were

issued in December 2001. They contain the complete list of forbidden contents cited above; State Council, 'Chuban guanli tiaoli' ('Regulations Governing the Administration of the Publishing Industry'), 25 December 2001, *GWYGB*, 2002, no. 4, pp. 14-20.

[24] G. Chen and D.A. Britton, 'China To Allow ICPs To Report Their Own News', 24 April 2000. Online. Available HTTP: <http://www.chinaonline.com/topstories/000424/1/C00042420.asp> (accessed 25 April 2000); 'China: Eastsay.com may not write, collect news', 5 June 2000. Online. Available HTTP: <http://www.chinaonline.com/topstories/000605/1/c00060203.asp> (accessed 6 June 2000).

[25] 'China's Print Media Concerned Over New Internet Portals', 22 September 1999. Online. Available HTTP: <http://www.chinaonline.com/issues/legal/currentnews/open/C9092180e-SS.asp> (accessed 24 October 1999); G. Chen, 'China's Booming Internet Sector: Open or Closed To Foreign Investment?', 8 October 1999. Online. Available HTTP: <http://www.chinaonline.com/industry/infotech/NewsArchive/Secure/1999/october/C9100519REV-SS.asp> (accessed 9 January 2000). In Shanghai, the most important traditional media (*Jiefang Ribao*, *Wenhui bao*, *Xinmin Wanbao*, Shanghai TV Station and others) united to form their own Internet portal. See 'China Web Site Has Got It Covered – Newswise', 24 May 2000. Online. Available HTTP: <http://www.chinaonline.com/issues/internet_policy/NewsArchive/Secure/2000/may/b100052237.asp> (accessed 19 April 2001).

[26] T. Fravel, 'The Bureaucrats' Battle over the Internet in China', 17 February 2000, Online. Available HTTP: <http://www.virtualchina.com/news/feb00/021800-ministries-tf.html> (accessed 19 February 2000). This is especially noteworthy if seen

against the background that the Party has drastically reduced the subsidies for newspaper publishing companies during the last years and that the publishing companies are strongly encouraged to finance themselves. See in detail D. Fischer, 'Rückzug des Staates aus dem chinesischen Mediensektor? Neue institutionelle Arrangements am Beispiel des Zeitungsmarktes', paper presented at the first meeting of ASC (=Arbeitskreis sozialwissenschaftliche Chinaforschung) 'Funktionswandel des Staates' 17-18 November 2000 in Witten.

[27] A portrait of this institution can be found under: 'Internet Information Management Bureau (IIMB)', 30 May 2000 Online. Available HTTP: <http://www.chinaonline.com/refer/ministry_profiles/IIMB.asp> (accessed 2 November 2000).

[28] Regulations for electronic information services can be found in §§ 14 and 15 of 'Hulianwang dianzi gonggao fuwu guanli guiding', p.46.

[29] See, for example, V. Pik-Kwan Chan, 'Beijing in hard drive to patrol Net users', 18 January 2002, online, available HTTP: <http://china.scmp.com/ZZZTHW3M5WC.html> (accessed 18 January 2002).

[30] 'Hulianwang dianzi gonggao fuwu guanli guiding', p.46 (§ 10).

[31] 'Hulianwang dianzi gonggao fuwu guanli guiding', p.46 (§ 10).

[32] This difference is stressed by Qiu, 'Virtual Censorship in China'. On Singapore's Internet policy in detail G. Rodan, 'The Internet and Political Control in Singapore', *Political Science Quarterly*, 2998, vol. 113, no. 1, pp. 63-89.

[33] References to §§ 21 and 22 in 'Hulianwang xinxi fuwu guanli banfa'.

[34] §§ 22 and 23 of 'Hulianwang xinxi fuwu guanli banfa'.

[35] According to the penal law of the PRC, sentences for several years are possible. See Giese, 'Das gesetzliche Korsett für das Internet ist eng geschnürt', p. 1176.

[36] See also Giese, 'Das gesetzliche Korsett für das Internet ist eng geschnürt', pp. 1176ff.

[37] The number of cases varies depending on the source used. J. Linchuan Qiu, 'Internet Censorship in China (1999-2000)', *Communications Law in Transition Newsletter*, 18 February 2001, vol. 2, no. 3. Online. Available HTTP: <http://pcmlp.socleg.ox.ac.uk/transition/issue2_3/qiu.htm> (accessed 25 February 2002). Qiu states that due to the increase in specialised police units and the deployment of new technologies, 13 people were arrested between summer 1999 and the end of 2000, while only one person was arrested in the years prior to that date. According to Neumann, 'The Great Firewall', seven people were arrested for Internet 'crimes' between 1998 and 2000. A *Human Rights Watch Backgrounder* published in July 2001 lists 15 individuals detained for posting material on the Internet. See 'Freedom of Expression and the Internet in China'. Online. Available HTTP: <http://www.hrw.org/backgrounder/asia/china-bck-0701.pdf> (accessed 24 August 2001).

[38] 'The Cracker War on China', 15 January 1999. Online. Available HTTP: <http://www.virtualchina.com/infotech/perspectives/perspective-011599.html> (accessed 2 January 2000); 'Whither the China Net?', 5 February 1999. Online. available HTTP: <http://www.virtualchina.com/infotech/perspectives/perspective-020599.html> (accessed 2 January 2000); 'Chinese engineer who helped dissident newsletter is freed', *Digital Freedom Network*, 6 March 2000. Online. Available HTTP: <http://www.dfn.org/focus/china/linhai.htm> (accessed 28 February 2001).

[39] 'Trial of Internet Entrepreneur Starts in Chengdu', RTHK Radio 3 audio Web site, Hong Kong, 13 February 2001, cf. *SWB FE*, 14 February 2001, no. 4070, p. G/4. See on this case also 'Chinese Webmaster to be tried February 13', 9 February 2001,

Digital Freedom Network, online, available HTTP: <http://www.dfn.org/focus/china/huangqi-trialdate.htm> (accessed 28 February 2001); '"6-4" Web Site Creator Put to Subversion Trial in Sichuan', 11 February 2001, *China News Digest*, no. GL01-019, availabe e-mail: LISTSERV@LISTSERV.ACSU.BUFFALO.EDU (12 February 2001).

[40] 'Chinese Internet café owner arrested', 24 August 2000, *Digital Freedom Network*. Online. Available HTTP: <http://www.dfn.org/focus/china/jiangshihua.htm> (accessed 28 February 2001).

[41] 'Banned Chinese Web site reappears', 11 August 2000, *Digital Freedom Network*. Online. Available HTTP: <http://www.dfn.org/focus/china/xinwenming-back.htm> (accessed 28 February 2001).

[42] C.S. Smith, 'Falun Dafa Defies Authority by Preaching in Cyberspace', *Asian Wall Street Journal*, 10-11 September 1999, pp. 1, 6; I. Buruma, 'China in Cyberspace', *The New York Review of Books*, 4 November 1999, vol. 46, no. 17, pp. 9-12; 'Falun Dafa and the Internet: A Marriage Made in Web Heaven', 30 July 1999. Online. Available HTTP: <http://www.virtualchina.com/infotech/perspectives/perspective-073099.html> (accessed 2 January 2000); 'Government, Falun Gong followers in Internet battle', *Sing Tao Jih Pao* (Hong Kong), 28 July 1999, p.A4, cf. *SWB FE*, 29 July 1999, no. 3599, p. G/5-6.

[43] 'Sentencing postponed in "cult" Web case', 19 Februry 2002. Online. Available HTTP: <http://uk.news.yahoo.com/020219/80/csj9z.html> (accessed 22 February 2002).

[44] J. Lee, 'U.S. May Help Chinese Evade Net Censorship', *New York Times*, 30 August 2001. Online. Available HTTP:

<http://www.nytimes.com/2001/08/30/technology/30VOIC.html> (accessed 31 August 2001).

[45] A. Lin Neumann, 'The Great Firewall'.

[46] 'China eases Net censorship during APEC talks', *South China Morning Post*, 17 October 2001. Online. Available HTTP: <http://technology.scmp.com/internet/ZZZMEIMFRSC.html> (accessed 17 October 2001).

[47] Slow speed of Internet access and data transfer is the most frequent complaint of Internet users in China. International bandwidth was expanded by 163 per cent between July 1998 and December 1999 (from 84.64 to 351 Mbps). Since the number of Internet users grew by 291 per cent during the same time, there was no improvement of the situation. However, during the year 2000, this trend was reversed: While international bandwidth grew again by 370 per cent, the number of users increased by 'only' 123 per cent. (Calculated on the basis of statistical data provided by CNNIC, the reliability of which is questioned by Giese in his chapter in this volume). See also Qiu, 'Virtual Censorship in China', p. 7.

[48] 'Should Internet Cafes Be Closed?', *Beijing Review*, 26 April 2001, pp. 30-1.

[49] 'China Issues New Regulations for Internet Cafes', 21 January 1999. Online. Available HTTP: <http://www.chinaonline.com/industry/infotech/NewsArchive/Secure/1998/August/it_b8081003e.asp> (accessed 27 January 2000); 'China's Beijing Cracks Down on Internet Cafes', 24 March 2000. Online. Available HTTP: <http://www.chinaonline.com/topstories/000324/2B200032207.asp> (accessed 29 March 2000).

[50] 'State Council tightens control over Internet cafes', 17 April 2001. Online. Available HTTP: <http://www.chinaonline.com/topstories/010417/1/C0104201.asp> (accessed 18 April 2001). On the crackdowns in 2001: 'Beijing Police pull plug on illegal Internet cafés', 23 February 2001. Online. Available HTTP: <http://www.chinaonline.com/topstories/010223/1/C01021611.asp> (accessed 26 February 2001). According to this report, in the year 2000, in Beijing's Chaoyang district alone, 41 illegal Internet cafés were closed and had to pay RMB350,000 fines, and 11 Internet cafés were reprimanded and temporarily closed. In the first two months of 2001, the police found five more illegal businesses. See also 'Hubei's Daye City closes cybercafés for pornography, Falun Gong information', Hubei Radio Webseite, 10 February 2001, cf. *BBC SWB FE*, 16 February 2001, no. 4072, pp. G/7-8.

[51] 'China shuts down nearly 2,000 Internet cafes', 19 July 2001. Online. Available HTTP: <http://asia.dailynews.yahoo.com/headlines/regional/china.html> (accessed 19 July 2001).

[52] Michael Ma, 'Beijing gets tough on Internet bar and BBS operators', *South China Morning Post*, 10 May 2001. Online. Available HTTP: <http://china.scmp.com/today/ZZZY0FMKYLC.html> (accessed 10 May 2001).

[53] 'Shanghai conducts random check of Web site operators', 20 March 2001. Online. Available HTTP: <http://www.chinaonline.com/topstories/010320/1/b101030934.asp> (accessed 21 March 2001).

[54] See Neumann, 'The Great Firewall'; 'Internet police ranks swell to 300,000', *Ming Pao* Web site, 8 December 2000. See also *BBC SWB FE*, 11 December 2000, no. 4020, pp. G/5-7.

[55] O. Winkel, 'Sicherheit in der digitalen Informationsgesellschaft', *Aus Politik und Zeitgeschichte*, 6 October 2000, no. B 41-42, p. 21.

[56] The idea of a 'firewall' within one own's head was explicitly advocated in an article on the Web site of *Renmin Ribao*. 'Party daily calls for action against Internet pollution', 21 March 2001, in *BBC SWB FE*, 28 March 2001, no. 4106, p. G/7.

[57] 'Bureau for the Protection of State Secrets (State Secrets Bureau)', 28 January 2000. Online. Available HTTP: <http://www.chinaonline.com/refer/ministry_profiles/Secrets-3-S.asp> (accessed 31 January 2000). The State Secrets Law came into force in 1988. 'Provisions governing the Implementation of the State Secrets Law of the People's Republic of China' was issued in 1990. State Secrets Bureau, 'Zhonghua Renmin Gongheguo baoshou guojia mimi fa shishi banfa', *GWYGB*, 1990, no.14, pp. 538-43. The regulations define, under what circumstances an information is considered to be a state secret. One of the points listed here refers to information which '[...] undermines consolidation and defence of the State's political power and which influences the unity of the State, ethnic unity and social stability' (p. 538).

[58] Qiu, 'Internet Censorship in China (1999-2000)'. Commercialisation changed the nature of the Internet in ways that mean that earlier claims can no longer be unconditionally sustained. Cyberspace now allows practically everyone to become both a recipient *and* a provider of information, since no costly means of production are needed (in contrast to traditional media) and market entry costs are extremely low.

[59] Commentary by representative of an Internet portal, cited in Neumann, 'The Great Firewall'. See also D. Cowhig, 'New Net rules not a nuisance?', 5 December 2000. Online. Available HTTP:

<http://www.chinaonline.com/commentary_analysis/internet/NewsArchive/secure/2000/December/c00120160.asp> (accessed 6 December 2000).

[60] Cited in D.C. McGill, 'Sina.com's Delicate Balancing Act', 23 May 2000. Online. Available HTTP: <http://www.virtualchina.com/finance/stirfry/052300-stirfry-dcm-alo2.html> (accessed 25 May 2000).

[61] On the 'Golden Shield' project see G. Walton, 'China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China', Rights & Democracy Web site. Online. Available HTTP: <http://www.ichrdd.ca/111/english/contentsEnglish.html> (accessed 21 October 2001). Western companies also compete to help Saudi Arabia in blocking the Internet. See J. Lee, 'Companies Compete to Provide Saudi Internet Veil', *New York Times*, 19 November 2001. Online. Available HTTP: <http://www.nytimes.com/2001/11/19/technology/19SAUD.html> (accessed 19 November 2001). The first 'golden' projects were launched in 1994 in order to 'informatize' China – such as the 'Golden Card', 'Golden Customs', 'Golden Tax' and 'Golden Sea'. See N. Hachigian, 'China and the Net: A love-hate relationship, Part II'. Online. Available HTTP: <http://www.chinaonline.com/commentary/archive/secure/2011/March/c01030260.asp> (accessed 8 March 2001); M. Mueller and Zixiang Tan, *China in the Information Age: Telecommunications and the Dilemmas of Reform*, Westport, Connecticut, London: Praeger Publishers, 1997, pp. 45-64.

[62] On the implications for national security arising from Chinese dependency of foreign software and hardware see the chapter by Christopher Hughes in this volume.

[63] 'Spy Systems on Show in China', *Far Eastern Economic Review*, 2 November 2000, p. 10; '"Purifying" the Net, China-style'. Online. Available HTTP: <http://www.dfn.org/focus/china/filteringsw.htm> (accessed 28 February 2001); D. Gebler, 'Chinese Web Filter May Block Western Sites'. Online. Available HTTP: <http://www.newsfactor.com/perl/printer/7805/> (accessed 28 February 2001); M. Fackler, 'The Great Fire Wall of China?', 8 November 2000. Online. Available HTTP: <http://www.abcnews.go.com/sections/tech/DailyNews/chinanet001108.html> (accessed 28 February 2001); A. C. LoBaido, 'Life with Beijing's bruisers'. Online. Available HTTP: <http://www.worldnetdaily.com/news/printer-friendly.asp?ARTICLE_ID=21446> (accessed 28 February 2001). On the question of importing Western hardware and software for surveillance see also F. Sieren, 'Von Netzen und Mauern. Über die Substanz chinesischer Internetphantasien', K. Leggewie und C. Maar (eds), *Internet & Politik. Von der Zuschauer- zur Beteiligungsdemokratie*, Cologne: Bollmann, 1998, pp. 229-235.

[64] A representative of Sohu.com described the approach as follows: 'We go with our intuition [...] If something makes us uncomfortable, we nix it.' Cited inT. Marshall and A. Kuhn, 'China Goes One-on-One With the Net', *LA Times*, 27 January 27 2001. Online. Available HTTP: <http://www.latimes.com/business/cutting/lat_chitek010127.htm> (accessed 29 January 2001).

[65] For a detailed description of this method see Wenzhao Tao, 'Censorship and Protest: The Regulation of BBS in China People Daily', *first monday*. Online. Available HTTP: <http://www.firstmonday.dk/issues/issue6_1/tao/index.html> (accessed 23 February 2001); Qiu, 'Virtual Censorship in China'.

[66] To be found on the *People's Daily* homepage, http://www.peopledaily.com.cn. The rules governing postings to *Qiang guo* are published on this site as well. No postings are permitted, for example, that 'contradict reform and opening as well as the four basic principles'. The same is true for unconfirmed news. Accounts of personal experiences are to be marked as such. No names of leading members of Party and government or other prominent personalities are to be used as pen names (*biming*). See <http://www.qglt.com/wsrmlt/rule.html> (accessed 7 March 2001).

[67] 'Top Website shuts chatroom over school blast anger', 9 March 2001. Online. Available HTTP: <http://www.ptdprolog.net/Webnews/wed/bo/Qchina-blast-internet.Rp0__BM9.html> (accessed 19 April 2001). It remained unclear, however, whether this closure was ordered by the authorities or was based on an in-house decision.

[68] 'China Fetes Falun Gong Day With Slow Bandwidth', 15 May 2000. Online. Available HTTP: <http://www.chinaonline.com/topstories/000515/x/C0051520.asp> (accessed 16 May 2000).

[69] Wenzhao Tao, 'Censorship and Protest'.

[70] On the question of Chinese nationalism on the Internet see C.R. Hughes, 'Nationalism in Chinese Cyberspace', *Cambridge Review of International Affairs*, Spring/Summer 2000, vol. 13, no. 2, pp. 195-209; A. R. Kluver, 'New media and the end of nationalism: China and the US in a war of words', *Mots Pluriels*, August 2001, no.18. Online. Available HTTP: <http://www.arts.uwa.edu.au/MotsPluriels/MP1801ak.html> (accessed 29 August 2001).

[71] English translation of the Chinese posting: 'PRC Chatroom Censorship Criticized – Chatroom discussion', H-ASIA, available as e-mail: H-ASIA@H-NET.MSU.EDU

(11 April 2001). The author makes the criticism that contributions which criticised the reaction of the Chinese government to the incident for being too lenient were removed from the Net. This critical message itself was able to survive on the Net for a while, however.

[72] See J. Linchuan Qiu, 'Chinese Opinions Collide Online', *Online Journalism Review*. Online. Available HTTP: <http://ojr.usc.edu/content/story.cfm?request=561> (accessed 17 April 2001).

[73] G. Wacker, 'Chinesische Reaktionen auf die Terroranschläge in den USA'. Online. Available HTTP: <http://www.swp-berlin.org/produkte/brennpunkte/wnd11sep6C.htm> (accessed 21 November 2001); N. D. Kristof, 'The Chip on China's Shoulder', *New York Times*, 18 January 2002. Online. Available HTTP: <http://www.nytimes.com/2002/01/18/opinion/18KRIS.html> (accessed 18 January 2002).

[74] This involves the user maintaining anonymity by accessing the site in question by using a proxy-server to make a connection.

[75] I. Johnson, 'Falun Gong Faces Added Pressure As Crackdown Grows', *The Asian Wall Street Journal*, 28 March 2001, pp. 1, 6; C.S. Smith, 'Sect Clings to the Web in the Face of Beijing's Ban', *New York Times*, 5 July 2001. Online. Available HTTP: <http://www.nytimes.com/2001/07/05/world/05FALU.html> (accessed 7 July 2001).

[76] State Council, 'Shangyong mima guanli tiaoli' ('Regulations for the Administration of Commercial Encryption'), Directive No.273, December 1999, *GWYGB*, 1999, no.36, pp. 1663-7. The regulations, which came into force on 31 January 2000, stipulate that all companies must register encryption products and any equipment that uses such products. As a result of the protests, the regulations, which had been rather

unclear to begin with, were revised in the sense that they would not apply to mobile phones, Windows software and Internet browsers. See K. Marlow, 'China Softens Encryption Rules', 14 March 2000. Online. Available HTTP: <http://www.chinaonline.com/topstories/000314/1/C00031430.asp> (accessed 15 March 2000). On the question of encryption in general see Lessig, *Code and Other Laws of Cyberspace*, pp. 35ff.

[77] This is mentioned in Qiu, 'Internet Censorship in China (1999-2000)'; J. M. Chen, 'Willing partners to repression?', 27 November 2000, *Digital Freedom Network*. Online. Available HTTP: <http://www.dfn.org/focus/china/multinationals.htm> (accessed 28 February 2001).

[78] J. Lee, 'U.S. May Help Chinese Evade Net Censorship', *New York Times*, 30 August 2001. Online. Available HTTP: <http://www.nytimes.com/2001/08/30/technology/30VOIC.html> (accessed 30 August 2001).

[79] E. Mills Abreu, 'SafeWeb shuts free Web service catering to users in China', Chinese Internet Research, 20 November 2001. Online. E-mail posting. Available at: chineseinternetresearch@egroups.com (21 November 2001).

[80] On the details of Internet distribution in China see Giese's contribution to this volume.

[81] The Web site 'FM365.com', which is sponsored by the biggest computer company in China, Legend Computers, offered an online game just in time for the National People's Congress in March 2001. The player could choose one of four officials accused of corruption (Yang Xianqian, Cheng Kejie, Wang Baosen, and Hu Changqing) and shoot at them by mouse-click. Moreover, the site offered background information on the four cases and even the option to give a vote on questions like

'How do you judge the government's efforts to fight top-level corruption?' Possible answers were 'not enough by far', 'so-so' (*mama-huhu*), 'quite ok' and 'cannot say'. Online. Available HTTP: <http://www.fm356.com/shequ/> (accessed March 28 2001). In real life, three of the officials were sentenced to death and the fourth (Wang Baosen) committed suicide. The question whether this game could have gone online without official approval was briefly discussed in March 2001 in the mailing list 'Chinese Internet Research'. From a Western perspective, such a game might seem macabre, especially because it featured real individuals. It is remarkable, however, how the game 'Corrupt Officials' combined entertainment, information and popular feed-back.

[82] Guo Liang and Bu Wei, '2000 nian Beijing, Shanghai, Guangzhou, Chengdu, Changsha Qingshao nian hulianwang shiyong zhuangkuang ji yingxiang de tiaocha baogao' (Survey report on Internet usage and influence in Beijing, Shanghai, Guangzhou, Chengdu and Changsha in the year 2000), April 2001. Online. Available HTTP: <http://www.chinace.org/ce/itre/index_.htm> (accessed 9 August 2001); J.J.H. Zhu and Zhou He, 'Information Accessibility, User Sophistication, and Source Credibility: The Impact of the Internet on Value Orientations in Mainland China', *Journal of Computer-Mediated Communication*, January 2002, vol. 7, no. 2. Online. Available HTTP: <http://www.ascusc.org/jcmc/vol7/issue2/china.html> (accessed 21 February 2002).

[83] Neumann, 'The Great Firewall'.

[84] Marshall and Kuhn, 'China Goes One-on-One With the Net'; Drake, Kalathil and Boas, 'Dictatorships in the Digital Age'; K. Hartford, 'Cyberspace With Chinese Characteristics', *Current History*, September 2000, vol. 99, no. 638, pp. 255-62.

[85] The kind of public discussion that takes place in electronic forums today over issues like homosexuality or AIDS would have been unthinkable some years ago. Although the number of taboos has decreased, however, subjects like the events surrounding the Tiananmen Massacre of 3-4 June 1989 remain out of bounds.

[86] Shapiro points out that when we consider the way a technology is used and the social environment in which it is deployed, taking into account the factors of design, use, and environment, it becomes clear that the Internet might just as well suppress democracy as promote it. 'The Internet', p. 15. However, while the sheer amount of information and multitude of opinions carried in cyberspace will not necessarily lead to more openness or tolerance of dissident views on its own. The multitude of Internet users with widely diverging interests and opinions may instead make it possible to create one's own 'global village', populated only by like-minded people and well secluded from the rest of the virtual world. 'The Internet', p. 25.