Internet crackdown in China

James Conachy
2 March 1999

In the first week of February, the Chinese regime announced the formation of a new state authority. With the Orwellian title of the "State Information Security Appraisal and Identification Management Committee", the body will focus on strengthening the computer firewalls set up to regulate Internet activity within China, protecting government and commercial websites from hackers, and developing new techniques to identify and monitor Internet users and their activities.

Its establishment is part of a crackdown by the Beijing regime on information flows taking place through the Internet and the broader suppression of political dissent, particularly as the tenth anniversary of the Tianenmen Square massacre approaches.

On January 20, a sentence of two years imprisonment was handed down in the landmark trial of Lin Hai, the Shanghai Internet services provider arrested on March 25, 1998 and charged with the crime of "inciting the subversion of state authority". He had sold 30,000 e-mail addresses to a US-based Chinese dissident Internet publication, *VIP Reference*.

VIP Reference--the name is a parody of an official Communist Party journal--sends a regular update of dissident news to over 250,000 e-mail addresses in mainland China. Employing a simple system of changing its posting site each day, it has thus far evaded attempts by Chinese security to prevent its distribution.

Lin Hai was the first Chinese citizen charged with political crimes for Internet activities and is appealing his sentence. The prison term imposed on him reflects growing pressures on the providers of Internet services to assist the government in preventing Chinese Internet users from accessing political organisations or news services that provide analysis critical of the regime. Unable to stop the flood of messages, the state is now turning on the message deliverers.

On February 1, Richtalk, one of the most used Chinese language web bulletin boards (www.sina.com.cn/richtalk/news/forum) was shut down by government decree and has not been resumed.

The Information Center of Human Rights and Democratic Movement in China, a Hong Kong-based dissident group, claimed that the Richtalk forum had signed up 600,000 new members in two months and that "bold" discussions were taking place on the events of June 1989. Richtalk's crime was that it had not attempted to censor the debate.

The Internet, more so than any previous medium, has posed a fundamental challenge to the control and censorship the Stalinist dictatorship has traditionally exerted over the flows of information, political discourse and international contact.

The aggressive market policies pursued since the early 1970s have transformed China into a central component of world capitalist economy, with thousands of transnational firms locating production facilities on the mainland to take advantage of the vast low-cost labour market and the brutal suppression of the working class.

To facilitate the expansion of transnational production, the regime has been compelled to establish modern international telecommunication links and to encourage the adoption and use of the Internet by Chinese citizens. Internet usage in China is rising exponentially, increasing from around one million in 1996 to over four million today.

Yet with access to a computer and a modem a Chinese citizen can, theoretically, read what they like and communicate with whom they like, outside of the control of government censors. In a society riven by social tensions, this is a troubling reality for ruling circles. The government has sought to deal with this "problem" by implementing some of the world's most bureaucratic laws and regulations governing Internet use.

To purchase a modem or obtain an Internet account requires a police permit, which is issued by a body known as the Computer Security and Supervision Authority. The user must sign a "Net Access Responsibility Agreement" which bars the use of the Internet for a lengthy list of forbidden purposes, including reading, reproducing or transmitting material that "endangers the state".

Without a police permit a Chinese citizen cannot open an Internet account or even casually use the web at an Internet café, which for many, particularly students, is their only option. An Internet account can cost up to half the monthly salary of a professional worker.

All Internet service providers (ISP) must pass through government controlled servers to access the World Wide Web. The government top-tier providers implement firewalls that prevent ISP servers accessing websites that are prohibited by the central authorities--a policy referred to as the "Great Firewall of China".

The banned sites include those of dissident organisations, Amnesty International, Human Rights Watch, and at different times has included the major world press, from the BBC to CNN. Users attempting to reach the firewalled sites get a "server not found" error message.

According to a report in *Online US News* last September, the Chinese bureaucracy has established a new force of more than 200 "Internet security guards". Qin Guang, head of the Computer Department for the Shanghai Public Security Bureau, was quoted as saying: "Our goal is to have a security guard in every work unit."

However ominous on paper such measures appear, they have had only a minimal impact or, as in the case of the Richtalk forum, proven ineffectual at stopping exchanges of opinion on political and social issues.

Politically motivated users have sidestepped them by dialling into ISPs located in Hong Kong, Taiwan or the US or used simple hacking techniques to bypass the firewalls. Publishers seeking to disseminate controversial information on the mainland frequently change the location of sites, mirror them on accessible sites or, more commonly, employ the same mass e-mail techniques of *VIP Reference*.

Many users have relied on the fact it was unlikely the state would ever actually check what they do on the web, assuming that there was safety in numbers. While the ISP logs of e-mail use and web movements are available for the state to inspect, the activity of millions of Internet users creates an enormous haystack for security agencies to sift through and uncover "suspicious" needles. Widely available encryption tools such as Pretty Good Privacy (PGP) further complicate attempts at monitoring e-mail.

The effectiveness of the existing controls was called into question in December and January when the banned China Democratic Party used e-mail to coordinate the public establishment of branches around China, without the knowledge of the security agencies.

The activities of Internet hackers have also raised alarm in Beijing. A Chinese computer magazine has alleged that 95 percent of Chinese computer networks with Internet access have been hacked. An Internet security company that tested dozens of government networks in the major cities of Shanghai and Shenzhen found that in most cases they could reach restricted information within one minute. Security assessments have uncovered over 100 serious hacking episodes against security, corporate or financial institutions.

In October two US-based hackers penetrated the server hosting the official Chinese government human rights website the day it was launched and replaced it with a page of denunciations of China's human rights record, links to Amnesty International and insults about the servers' standard of security. In December, in protest at the trial of Lin Hai, the same pair hacked into one of main Chinese backbone providers and disabled the firewalls on five servers.

What effect the new state authority will have in strengthening the hand of the Stalinist bureaucracy over the use of the Internet in China remains to be seen. But there is little doubt that the web will remain a major tool for the expression and organisation of political discontent and opposition to the Beijing regime.