
SUMMARY

In authoritarian societies from Saudi Arabia, to Cuba, to Myanmar, to the People's Republic of China (PRC), dissidents are using the Internet to organize and communicate with each other, to access banned information, and to draw support from a global network of activists and nongovernmental organizations (NGOs). At the same time, the governments of these countries are struggling to prevent activists from using the Internet to erode government controls over the flow of information and to promote political or social agendas that the regimes find threatening. This gives rise to a series of questions about the political impact of the Internet in authoritarian societies: Does the Internet provide dissidents with potent new tools that they can use to promote their causes, break through the barriers of censorship, and perhaps ultimately undermine the power and authority of nondemocratic regimes? Or, on the contrary, is it more likely that those authoritarian governments will use the Internet as another instrument to repress dissent, silence their critics, and strengthen their own power?

This report addresses the use of the Internet by Chinese dissidents, Falungong practitioners, Tibetan activists, and other groups and individuals in the PRC and abroad who are regarded as subversive by the authorities in China. It also examines the counterstrategies that Beijing has employed in its attempts to prevent or minimize the political impact of Chinese-dissident use of the Internet.

The arrival of the Internet has altered the dynamic between the Beijing regime and the dissident community. For the state, the political use of the Internet further degrades the Chinese Communist Party's

(CCP's) ability to control the flow of information it deems politically sensitive or subversive into China and within China. The party, however, still uses Leninist methods to crush potential organized opposition, and as a result, no organization with the capacity to challenge the CCP's monopoly on political power presently exists in China.

For dissidents, students, and members of groups such as Falungong, the Internet—especially through its two-way communication capabilities, e.g., e-mail and bulletin board sites (BBS)—permits the global dissemination of information for communication, coordination, and organization with greater ease and rapidity than ever before. Moreover, it allows these activities to take place in some instances without attracting the attention of the authorities, as exemplified by the unexpected appearance of an estimated 10,000 to 15,000 members of Falungong outside Zhongnanhai, the Chinese central leadership compound, in April 1999.

The capability of even one-way Internet communication—particularly e-mail “spamming”—enables the dissident community to transmit uncensored information to an unprecedented number of people within China and to provide recipients with plausible deniability in that they can claim that they did not request the information. In part because of dissident countermeasures (such as the use of different originating e-mail addresses for each message), the PRC is unable to stop these attempts to “break the information blockade.” There is a trend toward more groups and individuals becoming involved in activities of this type, which some have dubbed a form of “Internet guerilla warfare.”

Small groups of activists, and even individuals, can use the Internet as a force multiplier to exercise influence disproportionate to their limited manpower and financial resources. At the same time, however, enhanced communication does not always further the dissident cause. In some cases, it serves as a potent new forum for discord and rivalry among various dissident factions.

In its counterstrategies, the PRC regime has made some use of high-tech solutions, including blocking of web sites, e-mail monitoring and filtering, denial, deception, disinformation, and even the hacking of dissident and Falungong web sites. There is some evidence that Beijing's technical countermeasures are becoming increasingly

sophisticated. In addition, some nongovernmental groups have launched “vigilante hacks” against dissident web sites, which compounds the difficulty of determining the level of official government sponsorship for such activities. Beijing’s approach, however, is predominantly “low-tech Leninist,” employing traditional measures such as surveillance, informants, searches, confiscation of computer equipment, regulations, and physical shutdown of parts of the information infrastructure.

The regime understands implicitly that the center of gravity is not necessarily the information itself, but the organization of information and the use of information for political action. The strategy of the security apparatus is to create a climate that promotes self-censorship and self-deterrence. This is exemplified by the comments of a Public Security Bureau official: “People are used to being wary, and the general sense that you are under surveillance acts as a disincentive. The key to controlling the net in China is in managing people, and this is a process that begins the moment you purchase a modem.”

The government’s strategy is also aided by the current economic environment in China, which encourages the commercialization of the Internet, not its politicization. As one Internet executive put it, for Chinese and foreign companies, “the point is to make profits, not political statements.”

On the whole, Beijing’s countermeasures have been relatively successful to date. The current lack of credible challenges to the regime despite the introduction of massive amounts of modern telecommunications infrastructure, however, does not inexorably lead to the conclusion that the regime will continue to be immune from the forces unleashed by the increasingly unfettered flow of information within and across its borders. While Beijing has done a remarkable job thus far of finding effective counterstrategies to what it perceives as the potential negative effects of the information revolution, the scale of China’s information-technology modernization would suggest that time is eventually on the side of the regime’s opponents.