Internet Censorship in China: Domestic Politics Important

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In the previous article in this pair of columns, I reviewed the indubitable evidence that the government of China is systematically trying to control its population’s access to information delivered through the Internet. The conventional view is that the Chinese government fears the effects of free access to Western knowledge and ideas and that their efforts to control their people’s access to the ‘Net are futile.

In contrast with the cut-and-dried, black-and-white vision of a suffering population suffering solely from repression of free access to the riches of Western information, scholar Lokman Tsui<http://www.lokman.org/> warns that the “Great Firewall of China”<http://www.greatfirewallofchina.org/> metaphor misleads foreign observers by simplifying a complex situation.

In his thoughtful analysis, “An Inadequate Metaphor: The Great Firewall and Chinese Internet Censorship,”<http://www.worlddialogue.org/content.php?id=400> he identifies the “Great Firewall Myth,” which he characterizes as follows:

First, the Great Firewall is a spatial metaphor. It depicts a situation in which China is protecting its own boundaries from foreign flows of data that might threaten the Communist Party’s monopoly on information. The metaphor represents China as closing itself up and censoring everything that comes in from the outside. One literally envisions a wall surrounding China.

However, he writes, of equal importance is the authoritarian control over dissemination of information within the country:

Just as important, though, if not more so, is the censorship of information that flows within China’s legal jurisdiction, and this censorship is of a vastly different nature. Here, Beijing does not have to rely solely on filtering technology, but rather uses a mix of socio-legal, political and economic methods in order to censor—something companies such as Yahoo!, Microsoft and Google have themselves experienced, being criticised in the worldwide press for complying with the regime’s demands. . . . The image of the Great Firewall protecting China from the West thus obscures the fact that “undesirable” information often comes not from the West but from within China itself.

For anyone interested in delving into the complexities of the Chinese stance with respect to the Internet, Lokman Tsui’s work is a treasure trove. His entire Master’s thesis<http://www.lokman.nu/thesis/> is available online: “Internet in China: Big Mama is Watching You – Internet Control and the Chinese Government”<http://www.lokman.nu/thesis/010717-thesis.pdf>. The crux of the problem is that, contrary to the widespread assumption in the West that the Internet inevitably leads to less governmental power, “The conclusions are that the Chinese government are quite capable of controlling the internet in China and that China has the perfect ingredients for deploying a digital Panopticon [a controlled representation of reality]. This digital Panopticon will continue to improve and develop, driven by the market. These
conclusions show that the internet, to contrary belief, can be controlled and even be used as a means for control.”

The point I take from Lokman Tsui’s analysis is that we are deluding ourselves if we think that merely sitting back and waiting for China to fail will solve the censorship problem in that vast country. On the contrary, the systematic shaping of information flows by a totalitarian regime is a grave threat to the entire world. People who have been brought up to see – and believe – what they are told without questioning authority are dangerous. I can easily imagine a billion-plus people following orders in the Internet-mediated belief that they are defending their homeland against external threats. In this case, the Internet may become, not a tool for freedom of expression and independent thought, but rather the instrument of a malevolent autocracy with little concern for law, human rights, or even the interest of its own people.

* * *

M. E. Kabay, PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc. and Associate Professor of Information Assurance in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.

Copyright © 2010 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.