"Authoritarian countries such as China and Saudi Arabia are employing both technological and institutional means to control use of the Internet while also encouraging its growth. In doing so, they stand as counterevidence to much of the optimistic thinking about the Internet's effect on democratization. . . ."

Weaving the Authoritarian Web

TAYLOR C. BOAS

In preparatory meetings leading up to the December 2003 World Summit on the Information Society in Geneva, the delegations of several authoritarian regimes reacted negatively to the hands-off approach to Internet regulation promoted by the United States and other advanced democracies. Saudi Arabia proposed that the development of the information society "shall be done without any prejudice whatsoever to the moral, social, and religious values of all societies"—values to which the Saudi government has appealed when justifying its censorship of the Internet. The Chinese delegation campaigned vigorously against a statement of support for the principles of free speech enshrined in the Universal Declaration of Human Rights. Ultimately, the summit's final declaration disregarded the objections that these and other authoritarian regimes had voiced during the negotiations, but their positions stand as a vivid reminder that not all countries accept a laissez-faire vision for the future of the Internet.

TECHNOLOGY

The World, 2005

At first glance, the negotiating positions adopted by China and Saudi Arabia might seem to constitute evidence for the common belief that the Internet presents authoritarian leaders with a stark choice: either promote the development of an Internet that remains free from extensive government control, or exert control over the technology by restricting its diffusion within their borders. Whether because of inherent technological characteristics that complicate efforts to censor the Internet, or because countries are under pressure to align their policies with those preferred by the international community, many scholars have assumed that the only effective way to control the Internet is to limit its growth or even keep it out entirely.

They are wrong. Contrary to the assumption underlying many of the studies of Internet policies among autocratic regimes, governments can in fact establish effective control over the Internet while simultaneously promoting its development. Indeed, China and Saudi Arabia are two of the most prominent examples of this phenomenon. Far from trying to regulate the Internet by merely restricting its diffusion, authoritarian countries such as China and Saudi Arabia are employing both technological and institutional means to control use of the Internet while also encouraging its growth. In doing so, they stand as counterevidence to much of the optimistic thinking about the Internet's effect on democratization that pundits and politicians voiced during the net's early days and the technology boom of the late 1990s.

CONTROLLING THE INTERNET

The Internet was initially designed as a technology that would not lend itself to centralized control. The original engineering decisions that gave rise to this characteristic were a product of the specific economic, political, and social environment in which the Internet was created. In part, the technological characteristics of the early Internet derived from the norms of its designers and initial user community—a small group of engineers and academics who were wary of bureaucracy, trusted each other, and worked well through consensus rather than a centralized hierarchy. In light of this culture, they made specific choices about the design of the technology that rendered the network resistant to efforts at centralized control. An even more important influence on the technological configuration of the early Internet were the military imperatives for its development.

TAYLOR C. BOAS *is a doctoral candidate in political science at the University of California, Berkeley, and coauthor, with Shanthi Kalathil, of* Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule *(Carnegie Endowment for International Peace, 2003).*

The US Department of Defense was the sponsor and progenitor of the Internet's precursor network, the ARPANET, and the packet-switching technology on which it was based was designed to frustrate attempts at centralized control so that communications capacity could not be disabled by an enemy attack on a key portion of the network.

The particular characteristics of the Internet that served to frustrate attempts at centralized control involve what is called the "end-to-end arguments" in network design. As guidelines for the design of computer networks, the end-to-end arguments state that complexity and control should be implemented at the ends of the network (the multiple computers and individual users that are interconnected); the core of the network performs simple data transfer functions that do not require knowledge of how the ends are operating. Because the Internet was built around an end-to-end design, one cannot control the entire network through control of a small number of centralized nodes. Control can be exerted at the ends of the network, but as these ends multiply, controlling the entire network by controlling the ends becomes less and less feasible.

While a control-frustrating technological architecture suited the needs and preferences of the Internet's designers and initial user community, the technology has since spread into a number of environments in which centralized control of information is a more desirable feature. One of the most important of these major shifts involves the global diffusion of the Internet. With Internet use in the developing world growing rapidly, the Internet is moving into a number of authoritarian countries where standards of information control are quite different from those in the United States. The leaders of these countries generally recognize the tangible benefits that the Internet has to offer, such as the promotion of economic development and the provision of online government services. Yet they worry that Internet use might pose political threats, challenge state control of economic resources, or offend local cultural sensitivities. To reap the benefits of the technology while avoiding what they see as negative ramifications, some leaders would prefer to exert greater centralized control over Internet use.

The idea of an inherently control-frustrating Internet rests on the assumption that the network's architecture is incapable of fundamental change. But many of the same characteristics that made the Internet hard to control make it a flexible technology as well. Unlike the telephone network, which was designed specifically for voice traffic, the core of the Internet was not optimized for any particular service. At the time of its creation, there was little sense of what services the Internet would need to support in the future, so the network's core was built as a set of simple, flexible tools. Any service that conforms to the published protocols for addressing and transmitting information can be implemented at the ends of the network without altering the center. The Internet's central mechanisms simply move information indiscriminately; the core of the network does not need to know if it is transmitting packets from an e-mail, a website, streaming audio, or some as-of-yet uninvented service. Thus, the characteristics of the Internet as a whole can be altered by adding new protocols that will help the technology meet the needs of operating in new environments.

Censors at the Gateways

The Internet is much less a single network of individual users than a network connecting separate computer networks. Networks are interconnected through a gateway; behind the gateway, each individual network can be configured in any number of ways. Conceptually, therefore, it may well make more sense to think of the Internet's component networks as its ends than to view individual users as the outer edge of a single, seamlessly interconnected Internet.

Controlling the *entire* Internet by controlling each of its component networks would remain a nearly impossible task. But no governing authority realistically seeks to control the whole Internet in this fashion. Rather, authorities attempt to control a relevant subset of Internet users. The administrators of corporate computer networks, for instance, often monitor employees' usage and block certain types of non–work-related traffic. Users who have a choice of networks will always be able to switch to a more liberal environment. For those with no realistic choice, however, the distinction between control of the entire Internet and control of a network attached to the Internet is largely irrelevant. For them, the choice is between access to a restricted Internet and access to nothing at all.

Such is the situation in many countries where the authoritarian regimes are developing national computer networks with connections to the Internet. While in most democracies a number of individual Internet service providers (ISPs) maintain separate links to the global Internet, under authoritarian regimes all Internet users may effectively be members of a single national network. Even where

there are multiple ISPs within a country, international connections to the global Internet are often channeled through a single government-controlled gateway. Indeed, the image of the Internet's global diffusion, in which a single transnational network makes inroads into countries around the world, is something of an inaccurate picture. What has occurred historically is the development of national computer networks (typically under the guidance of the state) that are then connected to the Internet.

Given the political, economic, and social conditions prevailing in many authoritarian-ruled countries, it is not surprising that their governments have sought to establish technological measures of control over the portions of the Internet within their borders. Authoritarian regimes are typically central players in the growth of their countries' information infrastructures, and the conditions under which this technological development takes place are far removed from those that prevailed in the early days of the Internet in the United States. Rather than an environment in which military imperatives and engineering culture demand a control-frustrating network, authoritarian countries are places in which political elites typically seek a fair degree of control over information flow. Given the flexibility of Internet technology at the macro-level, one would expect authoritarian regimes to build architectures of control into their "ends" of the Internet.

In Saudi Arabia, the government has found support for its censorship regime among conservative Islamist groups that are primarily concerned about pornography.

THE SAUDI CASE

Saudi Arabia's approach to the Internet has been strongly influenced by the pressures of a conservative society, with significant public concern over pornography and material offensive to Islam, and considerable societal support for censorship of this type of content on the Internet. In addition, Saudi Arabia is a monarchy in which the royal family is quite sensitive to criticism and dissent; it is particularly cognizant of the threat posed by overseas opposition groups. Because of these conditions, Saudi Arabia has moved very slowly in its approach to the Internet. The country's first connection was established in 1994, but public access was delayed until 1999 while authorities perfected their technological mechanism for Internet control. Saudi Arabia has chosen to permit multiple, privately owned ISPs, but all international connections to the global Internet pass through a gateway maintained by the Internet Services Unit (ISU) of the King Abdulaziz City for Science and Technology, the Internet's governing authority in the country. Effectively, all Internet use within Saudi Arabia can be thought of as taking place within a single national network.

This concentrated network structure has facilitated the technological control of Internet content, a goal about which Saudi authorities have been quite open. Since the debut of public access in Saudi Arabia, all traffic to the global Internet has been filtered through a set of proxy servers managed by the ISU, aiming to block information that authorities consider socially or politically inappropriate. Market conditions have facilitated this imposition of censorship, with Saudi Arabia outsourcing the provision of censorship software to foreign firms that specialize in this area. Saudi authorities rely on a pre-set list of sexually explicit sites contained in a computer program that has been customized with the addition of impermissible political and religious sites. In addition, the ISU's website includes forms with which the public can request that sites be blocked or unblocked; officials report an average of 500 block requests and 100 unblock requests per day.

CHINA'S INTERNETS

China in its approach to the Internet has sought a strategy that will allow it to promote widespread market-based diffusion of the technology while still retaining government control. In contrast to Saudi Arabia, in which all blocking takes place at a single international gateway, Internet control in China is more diffuse. It is difficult to ascertain the specific technological details of this case because China has been much less open about the configuration and extent of its censorship regime. All evidence suggests, however, that China employs multiple, overlapping layers of Internet control that have been effective at limiting the access of the majority of users. Blocking specific web pages on the basis of IP address has been the most common; a similar procedure can block e-mails sent to or received from a host computer. Beginning in September 2002, authorities implemented a more sophisticated system capable of blocking pages dynamically, based on either keywords in the web address

(URL)—prohibiting Google searches on specific terms, for instance—or keywords in the actual web page requested. These methods of blocking are a step beyond previous strategies and mechanisms employed elsewhere, since they do not rely on a preexisting blacklist of prohibited websites.

At the level of the international gateway, the cornerstone of China's Internet control has been its system of interconnecting networks. While promoting rapid proliferation of the ISPs that offer Internet access to end-users, actual connectivity to the global Internet has long been channeled through a small number of interconnecting networks with ties to government ministries or important state companies. Four interconnecting networks were initially established in 1996; the number has since grown to nine. As the Ministry of Information Industries has licensed additional networks, it has made certain they are under effective state control. Moreover, the structure of this market is more concentrated than the number of interconnecting networks implies; the top two networks, ChinaNET and China Netcom, jointly control 81 percent of international bandwidth. Most national-level Internet filtering is implemented by the International Connection Bureau, based on a set of computers belonging to ChinaNET owner China Telecom. And the major networks routinely exchange information about specific websites that they seek to block.

In the Cafés and Chat Rooms

In addition to blocking mechanisms implemented at the level of the interconnecting network, China has extended its management of Internet architecture by establishing control at the level of ISPs, Internet cafés, and chat rooms. These points of access to the Internet number into the thousands, and most are thoroughly private entities without the same ties to the regime as the interconnecting networks, so direct government imposition of technological control is less of an option here. At this more diffuse level, authorities implement an architecture of control indirectly, through their legal influence over these intermediaries and their creation of a market environment in which cooperation with authorities is good business practice. Technological measures of censorship at a centralized level are thus augmented by additional filtering at a level much closer to the individual user.

China's Internet regulations make ISPs, Internet cafés, and chat rooms responsible for online content, and the threat of sanctions (and occasional large-scale crackdowns) has encouraged these entities to implement their own technological measures of control. It is likely that at least some filtering methods are implemented by ISPs instead of (or in addition to) the interconnecting networks. For their part, many Internet cafés have chosen to install blocking software to limit what their patrons can view, and chat rooms use a technology that scans for potentially sensitive postings and sends them to a webmaster for review. In addition to these filtering measures, ISPs and Internet cafés have been required to implement technological architectures that facilitate government surveillance. Regulations introduced in October 2000 require ISPs to keep logs of Internet traffic for 60 days and deliver the information to authorities on request. Many Internet cafés have installed software that allows public security bureaus to track user records and monitor Internet traffic remotely.

Evidence from the cases of Saudi Arabia and China confirms the view that the architecture of the Internet is not inherently control-frustrating, even if this characteristic was a feature of the early Internet in the United States. Rather, the logic of end-to-end network design allows authoritarian governments to construct national computer networks attached to the Internet in ways that facilitate technological control. In Saudi Arabia, a single gateway to the global Internet effectively creates a single national network within the country. Even in the case of China, where infrastructure is more developed and international connections to the Internet are more diffuse, influence over intermediaries through legal or market channels allows for the creation of control-facilitating technological architectures.

Perfect vs. Effective Control

Those skeptical of arguments about Internet control routinely point to the myriad ways in which determined users can circumvent technological measures of control. Indeed, evidence from Saudi Arabia, China, and many other authoritarian countries confirms that some individuals are finding ways to elude government censors. Saudi authorities have acknowledged that many users are finding ways to access forbidden websites, often through the use of overseas proxy servers. Wealthy Internet users who find this avenue blocked can always dial into unrestricted accounts in neighboring Bahrain—a common practice in the days before public access was permitted in Saudi Arabia. Chinese Internet users can attempt to circumvent controls in a variety of ways, from the use of peer-to-peer file-sharing systems to entering the URLs of blocked pages in ways that may fool censorship mechanisms. In the Chi-

nese case, ongoing arrests of online dissidents confirm that people are successfully engaging in types of Internet use that the government seeks to block. And in each of these countries, it is more difficult to exert technological control over the use of e-mail than it is to filter access to international websites.

In addressing the implications of these inevitable cracks in national firewall systems, it is important to distinguish between perfect control and effective control of the Internet. Ultimately, libertarian perspectives on Internet control are concerned with the individual: will the government be able to prevent *me* from doing what I want to do online? For the most determined and technology-savvy users, only perfect architectural constraints will be able to control their online activity. But the perspective of authoritarian governments, or of any authority seeking to exert control over the Internet, is different. For them, the goal is almost never perfect control, attempting to thwart the evasive maneuvers of every enterprising individual. Rather, authoritarian leaders seek to exert control with an external criterion of success—control that is in effect "good enough" to serve any number of objectives, including regime stability and protection of local culture. Effective control of this sort may not be capable of changing the behavior of the last tenth of a percent of Internet users, but this small number is rarely enough to seriously challenge the goals that most authoritarian regimes are trying to pursue.

China employs multiple, overlapping layers of Internet control that have been effective at limiting the access of the majority of users.

THE COST OF CIRCUMVENTION

It is in establishing and enforcing effective rather than perfect control over the Internet that institutional constraints on Internet use come most clearly into play. In contrast to the architectural characteristics that render certain types of Internet use easier, more difficult, or impossible, institutional constraints consist of the legal regulations, market conditions, and social norms that exert an influence on what individual users do with the technology. To understand the interplay of these two categories of constraints, an economic interpretation is useful, with unrestricted Internet access thought of as a good demanded by different numbers of users depending on the price.

In this economic model, most consumers are quite happy using the Internet for entertainment, online games, communication with friends, and access to officially sanctioned news sources; they place a low value on circumventing controls, especially with regard to political information. Similarly, some percentage of users will always demand unrestricted access to the Internet even at extremely high prices; they will spend money for technology to circumvent censorship, engage in illegal political communication at the risk of punishment, and ignore disapproval from members of society who frown on lawless activity. As these costs are raised, however, demand for unrestricted Internet access shrinks. The government's goal is not to set the cost so high that demand is completely eliminated; rather, authorities seek to reduce this demand to the point of political insignificance.

Law, social norms, and market forces that raise the cost of unrestricted Internet use allow for a much more effective implementation of control than architectural constraints alone. Arguably, the establishment of perfect technological control is impossible short of cutting off access to the global Internet. For this reason, countries such as Cuba and Burma have chosen control of access rather than extensive content censorship as their strategy for Internet regulation. For countries that promote widespread access to the Internet, however, filtering alone is insufficient. In the absence of perfect architectures of control, technological constraints are most effective when they interact with alternative, institutional constraints. If firewalls can be circumvented with sophisticated technology or international phone calls, the high price of these activities helps to render this architectural constraint effective. If tech-savvy patrons of Internet cafés can configure their browsers to access pornographic or dissident websites, they will be stopped only by the ingrained knowledge that such behavior is socially unacceptable, or that café managers may be observing their Internet use and could report their transgressions to authorities.

"BIG MAMA" IS WATCHING

The cases of Saudi Arabia and China illustrate how governments can leverage institutional constraints in combination with technological filters to establish effective control over Internet use. In Saudi Arabia, the government has found support for its censorship regime among conservative Islamist groups that are primarily concerned about pornog-

raphy. Social norms against viewing material deemed offensive to Islam encourage self-censorship among users, as do legal prohibitions on accessing forbidden content and the possibility that surveillance mechanisms can identify violators. Attempts to view blocked sites are greeted with a message that all access attempts are logged; ISPs are required to keep records on the identity of users and provide such information to authorities if requested. In addition to these legal and normative sanctions, market conditions (such as the high price of dialing into an ISP outside of the country) have also discouraged those who would seek to obtain unrestricted Internet access in Saudi Arabia.

In China, the use of institutional constraints on Internet access has been even more extensive, probably a result of the greater challenge of exerting purely technological control over a broader and more diffuse Internet. One major way that China promotes self-censorship involves regulation of users. Authorities have engaged in high-profile crackdowns on various dissidents and individuals who run afoul of the regulations by engaging in politically sensitive communication. Examples include Huang Qi, who operated a website with news about the Tiananmen massacre, and members of the Falun Gong, who disseminate their materials online. Sentences of several years in prison are common for such offenses, undoubtedly deterring others who might have the inclination to engage in similar activity.

Periodic crackdowns on the Internet cafés and chat rooms that allow patrons to engage in prohibited activities have encouraged these intermediaries to police their own users. In addition to implementing the technological measures of censorship and surveillance, China's Internet cafés have added elements of human control to comply with regulations. Managers tend to observe closely their users' surfing habits, especially after a series of crackdowns and closures of Internet cafés in 2001. Similarly, most chat rooms employ censors known as "big mamas" who screen postings and delete those that touch on prohibited topics. The operators of major Internet portals, who are forbidden to post information that "undermines social stability," have steered clear of anything potentially sensitive, offering primarily entertainment, sports information, and news from official sources.

Even where regulations do not specifically require it, market conditions have encouraged the private sector to comply with the state's broad goals for the Internet. Doing business in China means maintaining good relations with the government; for Internet-related businesses, this means complying with the state's overall designs for the technology, both written and unwritten. In early 2000, for example, more than 100 of China's major Internet entrepreneurs signed a pledge to promote self-discipline and encourage the "elimination of deleterious information [on] the Internet."

JUST A TOOL

Ultimately, the Internet is a tool, a medium of communication much like any other. It has no inherent political logic. As a tool, its political impacts will depend largely on who controls the medium and in what manner they seek to use it. In countries such as Mexico and Indonesia, where authorities have taken a more hands-off approach to Internet regulation, protesters and civil society groups were able to use the Internet for organization and pressure politics in ways that may have contributed to regime change. There are few such opportunities in Saudi Arabia and China with their extensive government control of the Internet by both technological and institutional means.

In speculating about the longer-term prospects for the Internet under authoritarian regimes, one should recall that accurately predicting the impact of a flexible technology is an inherently difficult enterprise. However, given the flexible nature of Internet technology, its specific design will reflect the social, political, and economic environment in which it is developed. Where these conditions do not favor a liberal technology, it is unlikely that one will emerge.

Of course, the institutional constraints that influence Internet use—law, the market, and social norms—are similarly capable of change over time even when they exhibit a certain degree of stickiness. To say that China's laws and market environment or the social norms prevailing in Saudi Arabia currently support government control of Internet use does not mean that they will continue to do so 50 years hence. While it is not an automatically control-frustrating technology, a more liberal future for the Internet is certainly possible. But that future will depend largely on the institutional variables shaping the evolution of Internet technology and the manner in which it is used—not on any inherent characteristic of the Internet itself. ■