NEW TECHNOLOGIES, INNOVATIVE REPRESSION:
Growing Threats to Internet Freedom

By Sanja Kelly and Sarah Cook

Over the past decade, and particularly in the last few years, the influence of the internet as a means to spread information and challenge government-imposed media controls has steadily expanded. This mounting influence directly corresponds to the growth in the number of users around the world: over two billion people now have access to the internet, and the figure has more than doubled in the past five years. However, as more people use the internet to communicate, obtain information, socialize, and conduct commerce, governments have stepped up efforts to regulate, and in some instances tightly control, the new medium. Reports of website blocking and filtering, content manipulation, attacks on and imprisonment of bloggers, and cyberattacks have all increased sharply in recent years.

To illuminate the nature of the emerging threats and identify areas of growing opportunity, Freedom House has conducted a comprehensive study of internet freedom in 37 countries around the globe. An earlier, pilot version was published in 2009, covering a sample of 15 countries. The new edition, Freedom on the Net 2011, assesses a wider range of political systems, while tracking improvements and declines in the countries examined two years ago. Over 40 researchers, most of whom are based in the countries they examined, contributed to the project by researching laws and practices relevant to the internet, testing accessibility of select websites, and interviewing a wide range of sources. Although the study’s findings indicate that the threats to internet freedom are growing and have become more diverse, they also highlight a pushback by citizens and activists who have found ways to sidestep some of the restrictions and use the power of new internet-based platforms to promote democracy and human rights.

When the internet first became commercially available in the 1990s, very few restrictions on online communications and content were in place. Recognizing the economic potential of the new medium, many governments started investing heavily in telecommunications infrastructure, and internet-service providers (ISPs) sought to attract subscribers by creating online chat rooms and building communities of users around various topics of interest. Even the authorities in China, which today has the most sophisticated regime of internet controls, exerted very little oversight in the early days. However, as various dissident groups in the late 1990s began using the
internet to share information with audiences inside and outside the country, the government devoted tremendous human and material resources to the construction of a multilayered surveillance and censorship apparatus. Although China represents one of the most severe cases, similar dynamics are now becoming evident in many other countries.

Indeed, the country reports and numerical scores in this study reveal that a growing number of governments are moving to regulate or restrict the free flow of information on the internet. In authoritarian states, such efforts are partly rooted in the existing legal frameworks, which already limit the freedom of the traditional media. These states are increasingly blocking and filtering websites associated with the political opposition, coercing website owners into taking down politically and socially controversial content, and arresting bloggers and ordinary users for posting information that is contrary to the government’s views. Even in more democratic countries—such as Brazil, India, Indonesia, South Korea, Turkey, and the United Kingdom—internet freedom is increasingly undermined by legal harassment, opaque censorship procedures, or expanding surveillance. The spread and intensification of internet controls in each country that showed decline generally conformed to one of the following three patterns:

**Initial signs of politically motivated internet controls:** In several countries that were previously free from most internet controls, the first signs of politicized censorship and user rights violations emerged, often in the period before or during elections. Many of these incidents represented the first time that a website in the country had been blocked, a user detained, or a restrictive law passed. This dynamic was particularly evident in Venezuela, Azerbaijan, Jordan, and Rwanda. In Venezuela, for example, users subscribing to internet services through the state-owned telecommunications firm CANTV reported that they were unable to access opposition-oriented blogs and a popular news site in the days surrounding parliamentary elections in September 2010. In Azerbaijan in 2009, the authorities temporarily blocked several websites that lampooned the president, and jailed two youth activists who posted a video that mocked the government.

**Acceleration and institutionalization of internet controls:** In countries where the authorities had already shown some tendency toward politically motivated controls over the internet, the negative trend accelerated dramatically, and new institutions were created specifically to carry out censorship. In Pakistan, for example, where temporary blocks have been common in recent years, a new Inter-Ministerial Committee for the Evaluation of Websites was established in mid-2010 to flag sites for blocking based on vaguely defined offenses against the state or religion. In Thailand, the government has long blocked internet content and taken legal action against users, particularly those posting information that is critical of the monarchy. However, the number of detained offenders and blocked sites sharply increased over the last two years, particularly while top officials had the authority to extrajudicially order blockings under a state of emergency that lasted from April to December 2010.

**Strengthening of existing internet-control apparatus:** Even in countries with some of the most robust censorship and internet surveillance systems in the world, measures were taken to eliminate loopholes and further strengthen the apparatus. In China, blogs on political and social issues were shut down, the space for anonymous communication has dwindled, and the
government has stepped up efforts to counter circumvention tools. In Bahrain, Iran, Ethiopia, and Tunisia, intensified censorship or user arrests came in the context of popular protests or contentious elections. Following the June 2009 elections in Iran, the country’s centralized filtering system evolved to the point of being able to block a website nationwide within a few hours, and over 50 bloggers have been detained. In Vietnam, in addition to blocking websites, restricting some social-networking tools, and instigating cyberattacks, the authorities displayed their muscle by sentencing four activists to a total of 33 years in prison for using the internet to report human rights violations and express prodemocracy views.

The new internet restrictions around the globe are partly a response to the explosion in the popularity of advanced applications like Facebook, YouTube, and Twitter, through which ordinary users can easily post their own content, share information, and connect with large audiences. While mostly serving as a form of entertainment, over the last two years these tools have also played a significant role in political and social activism. In Egypt and Tunisia, for example, democracy advocates have relied heavily on Facebook to mobilize supporters and organize mass rallies. Similarly, Bahraini activists have used Twitter and YouTube to inform the outside world about the government’s violent response to their protests. Even in Cuba, one of the most closed societies in the world, several bloggers have been able to report on daily life and human rights violations.

Many governments have started specifically targeting these new applications in their censorship campaigns. In 12 of the 37 countries examined, the authorities consistently or temporarily imposed total bans on YouTube, Facebook, Twitter, or equivalent services. Moreover, the increased user participation facilitated by the new platforms has exposed ordinary people to some of the same punishments faced by well-known bloggers, online journalists, and human rights activists. Among other recent cases, a Chinese woman was sent to a labor camp over a satirical Twitter message, and an Indonesian housewife faced high fines for an e-mail she sent to friends complaining about a local hospital. Because new technologies typically attract the young, some of those arrested have been teenagers, including an 18-year old Iranian blogger writing about women’s rights and a 19-year old Tibetan detained after looking at online photographs of the Dalai Lama.

KEY FINDINGS

The 2011 edition of Freedom on the Net identifies a growing set of obstacles that pose a common threat to internet freedom in many of the countries examined. Of the 15 countries covered in the pilot, a total of 9 registered score declines over the past two years. The newly added countries lack earlier scores for comparison, but conditions in at least half of them suggest a negative trajectory, with increased government blocking, filtering, legal action, and intimidation to prevent users from accessing unfavorable content. In cases where these tactics are deemed ineffective or inappropriate, authorities have turned to cyberattacks, misinformation, and other indirect methods to alter the information landscape.
Political Content Increasingly Blocked, Transparency Lacking

Governments around the world have responded to soaring internet penetration rates and the rise of user-generated content by establishing mechanisms to block what they deem to be undesirable information. In many cases, the censorship targets content involving illegal gambling, child pornography, copyright infringement, or the incitement of hatred or violence. However, a large number of governments are also engaging in deliberate efforts to block access to information related to politics, social issues, and human rights.

Of the 37 countries examined, the governments of 15 were found to engage in substantial blocking of politically relevant content. In these countries, instances of websites being blocked are not sporadic or limited in scope. Rather, they are the result of an apparent national policy to restrict users’ access to dozens, hundreds, or most often thousands of websites, including those of independent and opposition news outlets, international and local human rights groups, and individual blogs, online videos, or social-networking groups.

Website blocking is typically implemented by ISPs acting on instructions from a government agent, judge, or other appointed entity, whose orders may apply to a particular domain name, an internet-protocol (IP) address, or a specific URL. ISPs keep track of and periodically receive updates on the resulting blacklists of banned sites. In a small number of countries, the filtering technology employed is more sophisticated, and can scan users’ browsing requests for certain banned keywords. Keyword filtering is much more nuanced, enabling access to a given website but not to a particular article containing a sensitive keyword in its URL path. Among the countries studied, China, Iran, and Tunisia are known to have such systems in place. In China, which boasts the world’s most comprehensive censorship apparatus, keyword filtering is evident in instant-messaging services as well, having been built into the software of popular messaging programs like TOM Skype and QQ.

Two of the countries categorized by Freedom House as electoral democracies—Turkey and South Korea—were also found to engage in substantial political censorship. In Turkey, a range of advanced web applications were blocked, including the video-sharing website YouTube, which was not accessible in Turkey from May 2008 to October 2010. South Korean authorities blocked access to an estimated 65 North Korea–related sites, including the official North Korean Twitter account, launched in August 2010. Meanwhile, the governments of Australia, Indonesia, and Italy introduced proposals that would enable automated filtering by ISPs, create a state-led multimedia content screening entity, and extend prescreening requirements from television broadcasting to video-hosting websites, respectively. By the end of 2010, these proposals had been set aside or amended to remove the most egregious requirements.

One aspect of censorship was evident across the full spectrum of countries studied: the arbitrariness and opacity surrounding decisions to restrict particular content. In most nondemocratic settings, there is little government effort to inform the public about which content is censored and why. In many cases, authorities avoid confirming that a website has been
deliberately blocked and instead remain silent or cite “technical problems.” Saudi Arabia does inform users when they try to access a blocked site, and the rules governing internet usage are clearly articulated on government portals, but as in many countries, the Saudi authorities often disregard their own guidelines and block sites at will. Even in more transparent, democratic environments, censorship decisions are often made by private entities and without public discussion, and appeals processes may be onerous, little known, or nonexistent.

The widespread use of circumvention tools has eased the impact of content censorship and at times undermined it significantly. Such tools are particularly effective in countries with a high degree of computer literacy or relatively unsophisticated blocking techniques. For example, YouTube remained the eighth most popular website among Turkish users despite being officially blocked in that country for over two years, and the number of Vietnamese Facebook users doubled from one to two million within a year after November 2009, when the site became inaccessible by ordinary means. Users need special skills and knowledge to overcome blockages in countries such as China and Iran, where filtering methods are more sophisticated and the authorities devote considerable resources to limiting the effectiveness of circumvention tools. Still, activists with the requisite abilities managed to communicate with one another, discuss national events in an uncensored space, and transmit news and reports of human rights abuses abroad.

Cyberattacks Against Regime Critics Intensify

Some governments and their sympathizers are increasingly using technical attacks to disrupt activists’ online networks, eavesdrop on their communications, and cripple their websites. Such attacks were reported in at least 12 of the countries covered in this study. However, attacks perpetrated by nonstate actors for ordinary criminal purposes are also a growing problem, particularly as internet penetration deepens and more users turn to the medium for shopping, banking, and other activities.

China has emerged as a major global source of cyberattacks. Although not all attacks originating in the country have been explicitly traced back to the government, their scale, organization, and chosen targets have led many experts to conclude that they are either sponsored or condoned by Chinese military and intelligence agencies. The assaults have included denial-of-service (DoS) attacks on domestic and overseas human rights groups, e-mail messages to foreign journalists that carry malicious software capable of spying on the recipient’s computer, and large-scale hacking raids on the information systems of over 30 financial, defense, and technology companies, most of them based in the United States. In addition, independent analysts have detected cyberespionage networks that extend to 103 countries as part of an effort to spy on the Tibetan government-in-exile and its foreign government contacts.

As with offline forms of violence and intimidation, governments seem most likely to resort to cyberattacks when their power is threatened by disputed elections or some other political crisis. In Iran, for example, during the mass protests that followed the June 2009 presidential election, many opposition news sites were disabled by intense DoS attacks, and there is technical evidence confirming that government-owned IP addresses were used to launch the assaults. A group calling itself the Iranian Cyber Army, which operates under the command of the Islamic Revolutionary
Guard Corps, managed to hack a number of other sites with a mix of technical methods and forgery.

Similarly, in the wake of fraudulent elections in Belarus in December 2010, the government initiated DoS attacks against opposition websites, dramatically slowing down their connections and in some instances rendering them completely inaccessible. Belarusian authorities also engaged in a type of web forgery designed to confuse users and provide false information. For example, the country’s largest ISP, the state-owned Belpak, redirected users from independent media sites to nearly identical clones that provided misleading information, such as the incorrect location of a planned opposition rally.

The Tunisian regime of President Zine al-Abidine Ben Ali accelerated its hacking activity in the run-up to the January 2011 uprising that drove it from power. Security officials regularly broke into the e-mail, Facebook, and blogging accounts of opposition and human rights activists, either deleting specific material or simply collecting intelligence about their plans and contacts.

**Governments Increasingly Exploit Centralized Infrastructure and Built-In Internet Chokepoints**

Although it often goes largely unnoticed, centralized government control over a country’s connection to international internet traffic poses a significant threat to online free expression and privacy, particularly at times of political turmoil. In about a third of the states examined, the authorities have exploited their control over infrastructure to limit widespread access to politically and socially controversial content, or in extreme cases, to cut off access to the internet entirely.

This centralization can take several forms. In Ethiopia and Cuba, for example, state-run telecommunications companies hold a monopoly on internet service, giving them unchecked control over users’ ability to communicate with one another and the outside world. Elsewhere, the state-run company’s control of the market is not complete, but its dominance is sufficient to significantly influence people’s access to information. Thus when CANTV in Venezuela or Kazakhtelecom in Kazakhstan block a website, it becomes inaccessible to the vast majority of internet users.

As a growing number of governments liberalize the ISP market, such centralization may become less obvious. In countries including Egypt and Belarus, a state-controlled company owns the country’s network of copper wires or fiber-optic cables and sells bandwidth downstream to a variety of retail-level ISPs. In China, Vietnam, and Saudi Arabia, an array of three to eight international gateways are available to multiple, economically competitive ISPs, yet ultimate control over the country’s connectivity rests with the government.

Of the 37 countries assessed, 19 had at least a partially centralized and government-controlled international connection. Authorities in at least 12 of these were known to have used their leverage to restrict users’ access to politically relevant information or engage in widespread
surveillance. Egypt joined the list in January 2011, when officials shut down the internet nationwide for five days in an unsuccessful attempt to curb antigovernment protests. Technicians reportedly cut off almost all international traffic flowing through a tiny number of portals, while ISPs, particularly state-owned Telecom Egypt, removed the routes to Egypt’s networks from global routing tables—the mechanism that provides pathways for users’ computers to connect to requested websites. The operation was accomplished within the span of one hour.

The Egyptian case demonstrates that at times of political unrest, authoritarian leaders do not hesitate to exploit infrastructural controls to protect their rule, even if it causes massive disruptions to economic activity and personal communications. Several other instances of this “kill switch” phenomenon have occurred in recent years. In 2007, at the height of a wave of popular protests led by Buddhist monks in Burma, state-run ISPs cut off the country’s internet connection from September 27 to October 4. More recently, from July 2009 to May 2010, the Chinese authorities severed all connections to the northwestern region of Xinjiang while security forces carried out mass arrests in the wake of ethnic violence. Local government websites and other content hosted within Xinjiang remained accessible, but the region’s 20 million residents were cut off from outside information and a range of services used daily by individuals and businesses—including e-mail, instant messaging, and blog-hosting.

In addition to outright shutdowns, a centralized, state-controlled internet infrastructure facilitates two other types of restrictions: the deliberate slowing of connection speeds and the imposition of a nationwide system of filtering and surveillance. During opposition protests in Iran in the summer of 2009, authorities sharply reduced the speed of network traffic, making it difficult to conduct basic online activities like opening e-mail messages. Uploading a single image could take up to an hour. In early 2011, as protests began flaring up across the Middle East, the Bahraini government selectively slowed down internet connections at newspaper offices, hotels, and homes. The prime example of a centralized filtering system is China’s so-called Great Firewall, but other countries, including Iran and Saudi Arabia, also use such systems to enforce nationwide censorship and monitor dissident activity.

Offline Coercion, Online Manipulation Alter Available Information

Rather than relying exclusively on technological sophistication to control internet content, many governments employ cruder but nevertheless effective tactics to delete and manipulate politically or socially relevant information. These methods are often ingenious in their simplicity, in that their effects are more difficult to track and counteract than ordinary blocking.

One common method is for a government official to contact a content producer or host, for example by telephone, and request that particular information be deleted from the internet. In some cases, individual bloggers or webmasters are threatened with various reprisals should they refuse the request. Increasingly, governments and their supporters are also taking advantage of

Countries with at least partially centralized and government-controlled internet connections:
Azerbaijan, Bahrain, Belarus, Burma, China, Cuba, Egypt, Ethiopia, Iran, Jordan, Kazakhstan, Malaysia, Saudi Arabia, Thailand, Tunisia, Turkey, Venezuela, Vietnam, Zimbabwe
international hosting platforms’ complaint mechanisms to have user-generated content removed. Over the past two years, activists from China, Egypt, Ethiopia, Mexico, and Tunisia found that their YouTube videos or Facebook accounts had been removed or disabled after complaints were filed, apparently by regime supporters. In several of these instances, the content was restored once the problem was brought to the hosting company’s attention, but the threat of a blanket ban is sometimes enough to induce large websites to meet governments’ specific deletion demands.

A certain set of countries have laws in place to hold content providers and hosts legally responsible for what others post on their sites. Such provisions effectively force the site owner to screen all user-generated content and delete what might be deemed offensive by the authorities. Long-standing laws in China have led internet companies there to employ hundreds of thousands of people responsible for monitoring and censoring online videos, bulletin-board discussions, blog posts, and microblog messages. Nevertheless, in 2009 and 2010, the Chinese authorities adopted various measures to increase pressure on private websites, obliging them to be more vigilant and prevent content from slipping through the cracks. In Thailand, Kazakhstan, Vietnam, and Venezuela, new laws or directives promulgated since 2007 have led to an increase in this type of censorship. In Thailand, for instance, online news outlets are legally responsible for comments posted by readers, and at least one editor is facing criminal charges over reader comments that were critical of the monarchy. In Vietnam and Venezuela, some webmasters and bloggers have disabled the comment feature on their sites to avoid potential liability.

In addition, a range of governments have deployed manpower and resources to proactively manipulate online discussion and bolster progovernment views. Thailand has military units assigned to countering online criticism of the monarchy, and Burma has established a blogging committee in each ministry. Elsewhere, those recruited and paid for such tasks may be ordinary citizens, often youth. Thus China has cadres, known as the “50 Cent Party” for their supposed per-comment fees, who are employed to post progovernment remarks on various online forums, and recruiting advertisements for similar commentators have reportedly begun to appear on Russian job sites. Government-sponsored posts aim not only to defend the leadership and its policies, but also to discredit opposition voices or human rights activists, and to deceive everyday users. During postelection protests in Iran, for example, government supporters posted fake user-generated content to Twitter and YouTube to mislead protesters and journalists.

In a somewhat different manipulation technique, search-engine providers in some countries, most notably China, are required to adjust search results to match government-imposed criteria, for instance by only offering government-affiliated sources on particular topics. In addition to displeasure over a series of cyberattacks, this obligation was at the center of Google’s decision to withdraw from China in early 2010.
COUNTRIES AT RISK

After reviewing the findings for the 37 countries covered in this edition of *Freedom on the Net*, Freedom House has identified five that are at particular risk of suffering setbacks related to internet freedom in 2011 and 2012. A number of other countries showed deterioration over the past two years and may continue to decline, but the internet controls in these states—which include Bahrain, China, and Iran—are already well developed. By contrast, in most of the five countries listed below, the internet remains a relatively unconstrained space for free expression, even if there has been some obstruction of internet freedom to date. These countries also typically feature a repressive environment for traditional media, as well as an internet penetration rate of at least 25 percent, meaning the internet is both vitally important and in significant danger of repression.

**Thailand**

Internet users in Thailand have played a significant role in challenging the political establishment and the role of the monarchy in Thai politics since the military coup of 2006. This has provoked efforts by the government and military to control the free flow of information and commentary online. Although the government has been blocking some internet content since 2003, over the past two years online censorship has increased in both scale and scope, affecting tens of thousands of websites by the end of 2010, including independent news outlets and human rights groups. Restrictions intensified between April and December 2010, when a state of emergency allowed the authorities to extrajudicially block any website. Dozens of people have been charged under various laws for expressing their views online, particularly those that are critical of the monarchy. As of the end of 2010, many of these cases had yet to be decided. The country’s political turmoil has continued, and parliamentary elections are tentatively scheduled for December 2011, raising the likelihood of additional backsliding on freedom of expression issues. In a worrying sign, a Thai judge in March 2011 sentenced a web developer to 13 years in prison for comments he posted and for refusing to remove the remarks of others.

**Russia**

Given the elimination of independent television channels and the tightening of press restrictions since 2000, the internet has become Russia’s last relatively uncensored platform for public debate and the expression of political opinions. However, even as access conditions have improved, internet freedom has eroded. In the last two years, the country’s first high-profile cases of technical blocking were reported, while tactics for proactively manipulating discussion in the online sphere were refined. Russian bloggers faced increasing intimidation: at least 25 cases of harassment of bloggers by the authorities occurred in 2009 and 2010, including 11 arrests. Greater efforts to increase government influence over the internet are anticipated as the country prepares for parliamentary elections in December 2011 and a presidential election in early 2012. In March 2011, bloggers reportedly uncovered evidence that Russian officials were hiring users to post
comments that would shape a “positive image” of the ruling United Russia party and “form a negative attitude” toward the author of a targeted blog.

**Venezuela**

While restrictions on broadcast media outlets have grown in recent years, the internet has remained relatively free, with blogs, Facebook, and Twitter becoming important spaces for the free diffusion of information. Opposition groups have used these platforms to mobilize support, and the authorities have responded with some attempts to restrict online content, though to date they have not engaged in large-scale filtering or blogger arrests. There have been periodic interruptions of access to opposition or independent websites, efforts to intimidate websites into censoring the comments of their users, and several prosecutions for information posted on Twitter. Perhaps the most worrying recent development is the passage in December 2010 of laws that increased state control over telecommunications networks and laid the foundation for website managers and service providers to be required to censor the comments of users. President Hugo Chávez had declared in March 2010 that the internet could not be “a free thing where you do and say whatever you want,” and progovernment lawmakers were spurred to act in December following opposition gains in September parliamentary elections. The country is now preparing for a presidential election in 2012, and the state-run telecommunications firm CANTV has a record of apparently restricting access to websites and blogs at sensitive times, suggesting that there is a strong possibility of increased censorship and harassment of internet users in the coming months.

**Zimbabwe**

Internet access remains limited in Zimbabwe, but the number of mobile-phone users has increased rapidly since early 2009, from less than 10 percent of the population to nearly 50 percent by the end of 2010. While the regime of President Robert Mugabe has committed rampant human rights abuses and exercised strict control over the traditional media, the internet is nominally free from government interference. Nevertheless, there are indications that the government has a strong desire to control new information and communication technologies (ICTs), particularly mobile phones. The 2007 Interception of Communications Act allows the authorities to monitor telephone and internet traffic, and requires service providers to intercept communications on the state’s behalf. In addition, some content restrictions and registration requirements related to mobile phones have been imposed in recent years. Parliamentary elections are likely to take place in late 2011, internet access via mobile phones is increasing, and there are a number of influential Zimbabwean news sites based in foreign countries, all of which may tempt Mugabe and his ZANU-PF party to increase ICT controls. Given the prevalence of mobile-phone use, this could take the form of censorship of text-messaging or even a “kill switch” action to disable the entire network.
Jordan

Jordan prides itself on offering broader freedom to use the internet than many other Middle Eastern countries. Nonetheless, internet users are aware that their browsing history, comments, and posted materials may be monitored by the authorities. Until recently, the government’s interest in maintaining this direct access to public opinion seemed to have outweighed its impulses to control content. In August 2010, despite objections from civil society, the government adopted a new law on cybercrimes that could be used to limit free expression on the internet. For example, it prohibits the posting of any previously nonpublic information relevant to foreign affairs, national security, the national economy, or public safety. Many bloggers and web users have expressed concern that the government could exploit the ambiguous definitions for each of these categories and use the law selectively to silence its critics. Currently, outright blocking of websites by the authorities remains rare, but website owners often remove material after receiving informal complaints via telephone from government officials, and several popular news websites have been subjected to hacking attacks after posting sensitive material. In February 2011, Ammonnews.net was hacked and temporarily disabled after its editors refused to comply with security agents’ demands to remove a statement in which Jordanian tribesmen called for democratic and economic reforms.