# REPORTERS WITHOUT BORDERS

# WORLD DAY AGAINST CYBER CENSORSHIP

## 12 MARCH 2010

## [ Enemies of the Internet ]

## [ Countries under surveillance ]


**12 march 2010**
**New Media Desk**
Reporters Without Borders
47, rue Vivienne - 75002 Paris
Tel : (33) 1 44 83 84 84
Fax : (33) 1 45 23 11 51
E-mail : internet@rsf.org
Web : www.rsf.org


REPORTERS WITHOUT BORDERS FOR PRESS FREEDOM

# Web 2.0 versus Control 2.0

The fight for free access to information is being played out to an ever greater extent on the Internet. The emerging general trend is that a growing number of countries are attemptimg to tighten their control of the Net, but at the same time, increasingly inventive netizens demonstrate mutual solidarity by mobilizing when necessary.

## THE INTERNET: A SPACE FOR INFORMATION-SHARING AND MOBILIZING

In authoritarian countries in which the traditional media are state-controlled, the Internet offers a unique space for discussion and information-sharing, and has become an ever more important engine for protest and mobilization. The Internet is the crucible in which repressed civil societies can revive and develop.

The new media, and particularly social networks, have given populations' collaborative tools with which they can change the social order. Young people have taken them by storm. Facebook has become the rallying point for activists prevented from demonstrating in the streets. One simple video on YouTube – Neda in Iran or the Saffron march of the monks in Burma – can help to expose government abuses to the entire world. One simple USB flashdrive can be all it takes to disseminate news – as in Cuba, where they have become the local "samizdats."

Here, economic interest are intertwined with the need to defend free circulation of information. In some countries, it is companies that have obtained better access to the Internet and to the new media, sometimes with positive consequences for the rest of the population. As a barrier to trade, Web censorship should be included on the agenda of the World Trade Organization. Several of latter's members, including China and Vietnam, should to be required to open their Internet networks before being invited to join the global village of international commerce..

## TAKEOVER

Yet times have changed since the Internet and the new media were the exclusive province of dissidents and opponents. The leaders of certain countries have been taken aback by a proliferation of new technologies and even more by the emergence of a new form of public debate. They had to suddenly cope with the fact that "Colored Revolutions" had become "Twitter Revolutions." The vast potential of cyberspace can no longer be reserved for dissenting voices. Censoring political and social content with the latest technological tools by arresting and harassing netizens, using omnipresent surveillance and ID registration which compromise surfer anonymity – repressive governments are acting on their threats. In 2009, some sixty countries experienced a form of Web censorship, which is twice as many as in 2008. The World Wide Web is being progressively devoured by the implementation of national Intranets whose content is "approved" by the authorities. UzNet, Chinternet, TurkmenNet… It does not matter to those governments if more and more Internet users are going to become victims of a digital segregation. Web 2.0 is colliding with Control 2.0.

A few rare countries such as North Korea, Burma and Turkmenistan can afford to completely cut themselves off from the World Wide Web. They are not acting on their lack of infrastructure development because it serves their purpose, and it persists. Nonetheless, the telecom black market is prospering in Cuba and on the border between China and North Korea.

Netizens are being targeted at a growing rate. For the first time since the creation of the Internet, a record number of close to 120 bloggers, Internet users and cyberdissidents are behind bars for having expressed themselves freely online. The world's largest netizen prison is in China, which is far out ahead of

# Web 2.0 versus Control 2.0

other countries with 72 detainees, followed by Vietnam and then by Iran, which have all launched waves of brutal attacks on websites in recent months.

Some countries have been arresting netizens in the last few months, even though they have not yet pursued an elaborate Net control or repression strategy. In Morocco, a blogger and a cybercafé owner were jailed by local authorities trying to cover up a crackdown on a demonstration that turned awry. In Azerbaidjan, the regime is holding Adnan Hadjizade and Emin Milli – two bloggers who had exposed the corruption of certain officials and had ridiculed them in a video circulated on YouTube. Four online journalists are also behind bars in Yemen. It is too soon to tell if these arrests may herald a new media takeover.

More and more states are enacting or considering repressive laws pertaining to the Web, or are applying those that already exist, which is the case with Jordan, Kazakhstan, and Iraq. Western democracies are not immune from the Net regulation trend. In the name of the fight against child pornography or the theft of intellectual property, laws and decrees have been adopted, or are being deliberated, notably in Australia, France, Italy and Great Britain. On a global scale, the Anti-Counterfeiting Trade Agreement (ACTA), whose aim is to fight counterfeiting, is being negotiated behind closed doors, without consulting NGOs and civil society. It could possibly introduce potentially liberticidal measures such as the option to implement a filtering system without a court decision.

Some Scandinavian countries are taking a different direction. In Finland, Order no. 732/2009, states that Internet access is a fundamental right for all citizens. By virtue of this text, every Finnish household will have at least a 1 MB/s connection by July 31, 2010. By 2015, it will be at least 100 MB/s. Iceland's Parliament is currently examining a bill, the "Icelandic Modern Media Initiative" (IMMI), which is aimed at strictly protecting freedoms on the Internet by guaranteeing the transparency and independence of information. If it is adopted, Iceland will become a cyber-paradise for bloggers and citizen journalists.

## The Internet users' response

The outcome of the cyber-war between netizens and repressive authorities will also depend upon the effectiveness of the weapons each camp has available: powerful filtering and surveillance systems for decrypting e-mails, and ever more sophisticated proxies and censorship circumvention tools such as Tor, VPNs, Psiphon, and UltraReach. The latter are developed mainly thanks to the solidarity of netizens around the globe. For example, thousands of Iranians use proxies originally intended for Chinese surfers.

Global pressure makes a difference, too. The major world powers' geo-strategic interests are finding a communications platform on the Web. In January 2010, the United States made freedom of expression on the Internet the number one goal of its foreign policy. It remains to be seen how the country will apply this strategy to its foreign relations, and what the reaction of the countries concerned will be.

In their apparent isolation, Web users, dissidents and bloggers are vulnerable. They are therefore starting to organize, collectively or individually, depending upon what causes they wish to defend. This type of momentum can produce a Russian blogger association, or one comprised of Moroccans, or Belarus Web users groups launching campaigns to protest against government decisions, or an Egyptian blogger group mobilizing against torture or the cost of living, or even Chinese Internet users organizing cyber-movements on behalf of Iranian demonstrators on Twitter. Whether their causes are national or global, the messages they communicate are the ones that will decide the landscape of tomorrow's Internet. Resistance is getting organized.

# Web 2.0 versus Control 2.0

## THE ENEMIES OF THE INTERNET 2010

The "Enemies of the Internet" list drawn up again this year by Reporters Without Borders presents the worst violators of freedom of expression on the Net: Saudi Arabia, Burma, China, North Korea, Cuba, Egypt, Iran, Uzbekistan, Syria, Tunisia, Turkmenistan, and Vietnam.

Some of these countries are determined to use any means necessary to prevent their citizens from having access to the Internet: Burma, North Korea, Cuba, and Turkmenistan – countries in which technical and financial obstacles are coupled with harsh crackdowns and the existence of a very limited Intranet. Internet shutdowns or major slowdowns are commonplace in periods of unrest. The Internet's potential as a portal open to the world directly contradicts the propensity of these regimes to isolate themselves from other countries. Saudi Arabia and Uzbekistan have opted for such massive filtering that their Internet users have chosen to practice self-censorship. For economic purposes, China, Egypt, Tunisia and Vietnam have wagered on a infrastructure development strategy while keeping a tight control over the Web's political and social content (Chinese and Tunisian filtering systems are becoming increasingly sophisticated), and they are demonstrating a deep intolerance for critical opinions. The serious domestic crisis that Iran has been experiencing for months now has caught netizens and the new media in its net; they have become enemies of the regime.

Among the countries "under surveillance" are several democracies: Australia, because of the upcoming implementation of a highly developed Internet filtering system, and South Korea, where draconian laws are creating too many specific restrictions on Web users by challenging their anonymity and promoting self-censorship.

Turkey and Russia have just been added to the "Under Surveillance" list. In Russia, aside from the control exercised by the Kremlin on most of its media outlets, the Internet has become the freest space for sharing information. Yet its independence is being jeopardized by blogger arrests and prosecutions, as well as by blockings of so-called "extremist" websites. The regime's propaganda is increasingly omnipresent on the Web. There is a real risk that the Internet will be transformed into a tool for political control.

In Turkey, taboo topics mainly deal with Ataturk, the army, issues concerning minorities (notably Kurds and Armenians) and the dignity of the Nation. They have served as justification for blocking several thousand sites, including YouTube, thereby triggering a great deal of protest. Bloggers and netizens who express themselves freely on such topics may well face judicial reprisals.

Other countries, such as the United Arab Emirates, Belarus and Thailand are also maintaining their "under surveillance" status, but will need to make more progress to avoid getting transferred into the next "Enemies of the Internet" list. Thailand, because of abuses related to the crime of "lèse-majesté"; the Emirates, because they have bolstered their filtering system; Belarus because its president has just signed a liberticidal order that will regulate the Net, and which will enter into force this summer – just a few months before the elections.

Lucie Morillon
Head of the New Media Desk

Jean-François Julliard
Secretary-General

# BURMA

## Repression: Internet faces a militarist censorship

*Domain name : .mm*
*Population : 48 137*
*Internet-users : 250 000*
*Average monthly salary : about 27,32 US$*

*Number of imprisoned netizens : 2*
*Average charge for one hour's connection at a cybercafé : about 0,55 US$*

Two high-ranking government officials sentenced to death for having e-mailed documents abroad: Net censorship is a serious matter in Burma. Massive filtering of websites and extensive slowdowns during times of unrest are daily occurrences for the country's Internet users. The Military Junta considers netizens to be enemies of the State. The legislation governing Internet use – the Electronic Act – is one of the most liberticidal laws in the world.

### A RIGID FIREWALL

The Burmese firewall applies strict censorship, which limits users to an Intranet purged of any criticisms of the regime. Only the use of proxies or other censorship circumvention tools permits access to the World Wide Web. Blocked sites include those of exiled Burmese media groups and certain global media outlets, proxies and other censorship circumvention tools, blogs and study-abroad scholarship sites. Government authorities block both websites and URLs. Censorship is not consistent: for example, the site www.peoplemediavoice.com is filtered, but its identical counterpart, www.peoplemediavoice.net is not.

Consultation of private electronic mail is also curtailed. Officially, Internet users are prohibited from using e-mail services other than those provided by the government. Webmail services such as Yahoo and Hotmail are blocked in the country, but can be consulted via proxies.

### CONNECTION SPEED: A BAROMETER OF BURMA'S INTERNAL SITUATION

The ordinary connection speed is 512kb per line, which is the equivalent of a basic ADSL individual connection, but one line is shared by several users, thus slowing down online activities. It takes about ten seconds to open an email or load one page. Using a proxy speeds up things. However, cybercafés – the main connection points in a country where individual Internet subscriptions are very expensive and subject to government authorization – must share this 512 kb line with 10 to 15 computers, thereby reducing the connection speed. Gtalk cannot function on a 256 kb line. A 512 kb line is needed to use Gtalk and Skype in real time.

When the country is in the throes of political tension, connection speed drops sharply, since the Junta deems it necessary to prevent "information leaks abroad." In May and June 2009, when opposition leader Aung San Suu Kyi was on trial for having violated the terms of her house arrest by allowing an uninvited American citizen to stay two days in her home, the regime did not hesitate to cut the telephone and Internet lines of the city in which she was detained. Moreover, Burmese Internet users noticed there was a drastic slowdown in nation-wide connection speeds that made it impossible to send videos. At the time, it took nearly an hour to send a simple email with no attachment. According to local sources, the government may be planning to once again cut off Internet access during the October 2010 elections, just as it did in 2007, so as to assert total control over the dissemination of news

### INDEPENDENT NEWS SOURCES: THE REGIME'S PET PEEVE

Journalists who collaborate with exiled media and bloggers are being closely watched by the authorities, particularly since the 2007 Safran Revolution and international sentencing that followed the widespread distribution of photos of the crackdown. They are brazenly taking advantage of a highly repressive piece of legislation, the Electronic Act of 1996, which pertains to the Internet, television and radio. This law

prohibits the importation, possession and use of a modem without official permission, subject to a fifteen-year jail penalty for "endangering the security of the state, national unity, culture, the national economy, and law and order." Nay Phone Latt (http://www.nayphonelatt.net/), arrested in 2008, got a 15-year prison sentence for possessing a "subversive" film. The blogger has developed eyesight problems while incarcerated.

The well-known comedian, Zarganar, was sentenced to 35 years in prison for disseminating on the Web articles critical of the way the government handled humanitarian aid in the wake of Cyclone Nargis. His blog (link) was one of the most visited Burmese websites inside the country. On December 31, 2009, Hla Hla Win, a video journalist working with the Norway-based Democratic Voice of Burma (DVB) TV network, was given a 20-year jail sentence. In January 2010, journalist Ngwe Soe Lin also got a 13-year term for having worked for the DVB. He had been arrested in a cybercafé in the Rangoon's Kyaukmyaung district on June 26, 2009.

By arresting these Internet users and journalists, the Junta is trying to intimidate potential critics and impose self-censorship on its citizens. Like the state-owned media, online publications are subject to advance censorship, which ruthlessly eliminates any topic that is even slightly controversial.

Exiled Burmese media such as Mizzima and Irrawaddy were once again the target of cyberattacks in 2009.

## UNDER SURVEILLANCE

Cyber-café owners are under increasing pressure from Burmese authorities. They were already required to take screenshots every five minutes on every computer station and be prepared to provide every user's ID card number, telephone number, and address if the police requested them. They are now strictly forbidden to help a customer create an email account, particularly on Gmail, or to use a proxy, under penalty of being closed down. Many cyber-cafés have been shut down in the last few months, partly for economic reasons, but also because of more practical problems such as power outages, high maintenance fees, slow connection speeds, and lack of customers.

Despite these actions, blogs are multiplying. A survey conducted by the Burma Media Association in August 2009 showed that there were over 800 active blogs, most of them hosted by Blogspot and Wordpress. Eighty percent are in Burmese, 8% in English and 10% are bilingual. Three-fourths of the bloggers are between the ages of 21 and 35 and have a college education. Over half of them are living in Burma and began blogging less than one year ago. The majority of them focus on entertainment-related topics. Only 8% of them discuss news-related subjects.

## IS A CHINESE-LIKE ECONOMIC OPENING LIKELY?

Although Burma has one of the world's lowest Internet penetration rates, the regime is about to build its own "Silicon Valley" dubbed "Yadanabon Cyber City." Its objective is not to facilitate free Internet access for its citizens but to centralize control prior to the autumn 2010 elections, within the framework of "Road Map to Democracy," a political reform plan launched by the Junta in early 2003. According to the State media, this "business complex" may be called upon to become the national communications' clearing house. For now, priority is being given to setting up land and mobile telephone lines for businesses that will be opening offices in this center. Internet will be next. Some Junta generals' reservations about communications will not easily be laid to rest.

# Burma

## Repression: Internet faces a militarist censorship

For the moment, the Junta is using a Thai satellite station for Burma's Internet connection, but plans to launch its own communications satellite via a Chinese or Indian rocket. With its "Silicon Valley" and its own satellite, the military regime seems to be making a commitment to develop Internet infrastructure for economic reasons. At the same time, however, it stands ready to cut off all connections and totally isolate the country once again at the least suspicion of "domestic unrest."

# China

## "Control 2.0" offensive held in check by inventive netizens

*Domain name: .cn*
*Population : 1 338 612 968*
*Internet-users : 384 000 000*
*Average monthly salary : between 219 and 274 US$*
*Number of imprisoned netizens : 72*
*Average charge for one hour's connection at a cybercafé : About 2 US$*

As its polemic with Google and the United States on the Internet's future unfolds, China continues to intensify Web censorship, faced with an increasingly forceful online community. The much-vaunted promises made by organizers at the open ceremonies of the Beijing 2008 Olympic Games have proven to be mere illusions for the world's biggest netizen prison. Expanded dissemination of propaganda, generalized surveillance and crackdowns on Charter 08 signatories are commonplace on what has become the Chinese Intranet – with significant consequences for trade.

### THE GOOGLE POLEMIC

Internet giant Google spotlighted Internet censorship in China when it announced on January 12, 2010, that it would stop censoring the Chinese version of its search engine, www.google.cn, even if it meant having to withdraw from that market. This decision was made following some highly sophisticated cyber-attacks aimed at dozens of human rights activists and journalists. Since then, there has been some growing tension between Chinese authorities – who assured the world that China has a "completely open" Internet – and the American company, which has become the standard bearer for freedom-of-expression defenders on the Net. U.S. Secretary of State Hillary Clinton lent Google her support in a historic speech on January 21. She portrayed the United States as defenders of a free Internet, accessible to all, and named freedom of expression on the Internet as a U.S. foreign policy priority.

### THE "ELECTRONIC GREAT WALL": THE WORLD'S MOST CONSUMMATE CENSORSHIP SYSTEM

According to the authorities, China has the world's largest Internet user population: 380 million. Its censorship system is one of the most technologically advanced in existence. It was implemented when the Chinese Internet was first created to facilitate the latter's economic growth, while also strictly controlling its content to prevent the dissemination of "subversive" information. In the hands of a regime obsessed with maintaining stability – censorship has developed into a tool for political control.

Censors manage to block tens of thousands of websites by combining URL filtering with the censoring of keywords ranging from "Tiananmen" and "Dalai Lama" to "democracy" and "human rights."

Ever since Chinese characters were introduced on the Net and China took over domain names ending in ".cn," the regime has been developing a genuine Intranet. Ideogram-based domain names are used to access websites based in China. By typing ".com.cn," surfers are redirected to the Chinese version of the website concerned. Any Chinese Internet user using ideograms is thus restricted to this Intranet, disconnected from the World Wide Web, and directly controlled by the regime.

Censorship is institutionalized: it is managed by several ministries and administrations. In addition to the generalized filtering system, the largest blog platforms are also monitored. Assistance from foreign companies – mainly Yahoo!, Microsoft and, for now, Google – search engines is making their job that much easier.

The primary news sites, like the state-owned media, receive daily oral and written directives from the Department of Publicity specifying what topics can, or cannot, be covered and under what conditions. For example, the Department sent the following instructions to prevent coverage of a graft case implicating Hu Jintao's son, Hu Haifeng, in Namibia: "Hu Haifeng, Namibia, corruption probe Namibia, corruption

probe Yang Fan, corruption probe TsingHua TongFang, corruption probe South Africa – ensure that searches for these keywords yield no results." The search engines implemented a draconian censorship with regard to this case.

## PROSPECT OF TOUGHER CENSORSHIP AND MORE CRACKDOWNS

The year 2009 was punctuated by a series of controversial anniversaries: the Tibet rebellion (in March), the 10th year since the Falun Gong spiritual movement was banned, and the 20th anniversary (in June) of the bloody quashing of student protests in Tiananmen Square (June). Another political highlight of that year was the 60th anniversary (on October 1) of the People's Republic of China. On each occasion, the authorities' reaction was to impose an even more drastic censorship on the traditional and new media outlets.

On the eve of the commemoration of the 20th anniversary of the Tiananmen Square events, a dozen websites such as Twitter, YouTube, Bing, Flickr, Opera, Live, WordPress and Blogger were blocked. The information blackout has been so well-enforced for the last 20 years that the vast majority of young Chinese citizens are not even aware that the events of June 1989 ever happened. "The search does not comply with laws, regulations and policies." That is the response received when Internet users type "June 4" on the "Photos" pages of Baidu –the country's most popular search engine. Search results mention only official Chinese comments on the "events of June 4."

Prior to the anniversary of the People's Republic of China, censors redoubled their efforts to prevent Web users from using anti-censorship software such as FreeGate, by blocking thousands of foreign IP addresses suspected of participating in this network.

The government tightened its control at the end of 2009/early 2010. In December 2009, the authorities announced that they would soon require all websites to register on a "white list" under penalty of being placed on a "black list.". Millions of websites in China, as well as abroad, run the risk of being blocked if this rule is applied to them.

The rule prohibiting individuals from obtaining domain names ending in ".cn" was lifted in February 2010, but replaced by the implementation of a draconian system of censorship: now an individual who wants to create an Internet website must register for it by bringing ID papers to regulators in person.

The anti-pornography campaign launched in January 2009 – according to the authorities – resulted in 15,000 sites being shut down one year later, and in the arrest of over 5,000 people. It also led to the shutdown of websites totally unrelated to the subject. The New York Times was briefly blocked in January 2009. The blog platform www.Bullog.cn, very much in vogue among activist bloggers and intellectuals, was closed that same month for "publishing a lot of negative information in the public domain," according to the Chinese Ministry of Information. It had notably published Charter 08, an online petition calling for more freedoms in the country, and particularly on the Internet, which to date has been signed by thousands of Chinese people.

Within the scope of this campaign, the government has also ordered Chinese and foreign computer manufacturers to install on their products filtering software called "Green Dam Youth Escort," designed to protect young Web users from "harmful" content, but whose filtering options would include the blocking of political and religious content. Due to widespread opposition, authorities have postponed making installation of the software mandatory.

# China

## "Control 2.0" offensive held in check by inventive netizens

All Internet censorship is not done for anti-pornographic purposes. What makes it all the more dangerous is that it is constantly being revised to take into account current events. For example, the keyword list is updated regularly. Among recently censored sites are ImdB – a news website about motion pictures – and YouTube, Blogger, Twitter, Facebook, the BBC in Chinese, Friendfeed, Dailymotion, Flickr, etc. Censors are particularly interested in blocking participative and photo-exchange websites. On March 30, the State Administration of Radio, Film and Television (SARFT) issued a Memorandum of Understanding calling for stricter control of audiovisual material posted on the Internet, which lists some thirty content links that should be banned or modified.

Human rights activist websites, Chinese Human Rights Defenders (CHRC) and Independent Chinese PEN Center (ICPC), as well as the news site Boxun, were hacked in January 2010 and rendered inaccessible for days. Their foreign Internet service provider was the target of the most intense DDoS attack that it had ever experienced. These attacks were preceded by the installation of malware on the sites of the organizations concerned.

Finally, censorship and crackdowns are becoming decentralized and are now also more often enforced by local officials in an increasingly random and unexpected way, and, to a growing extent, eluding central government control.

### DISCRIMINATORY TREATMENT WITH REGARD TO XINJIANG AND TIBET INTERNET ACCESS

Chinese "at-risk" regions like Tibet and Xinjiang bear the full brunt of censorship. Repression is a permanent threat for anyone who tries to disseminate accounts of violence committed by security forces. Dozens of Tibetans and Uighurs are detained, and some of them received life sentences for having sent news abroad or tried to share information incompatible with the Party line.

Two Tibetan websites hosted in China, Tibet (http://www.tibettl.com/), known for hosting the blog of popular writer Jamyang Kyi and ChodMe (http://www.cmbpd.cn/index.html), are now inaccessible in most of the country, especially Tibet. In August 2009, Web surfer Pasang Norbu was arrested by Chinese authorities in Lhassa for having consulted the Radio Free Asia's website (http://www.rfa.org/english/). In November 2009, Tibetan writer and photographer Kunga Tseyang was given a five-year prison sentence for offenses that included publishing articles on the Internet. Two days earlier, the founder of a literary Internet website, Kunchok Tsephel, got fifteen years in prison for "dissemination of state secrets."

Xinjiang, cut off from the world following the July 2009 uprisings, is still waiting to be reconnected to the Internet. Although the authorities reestablished access in early 2010 – solely for the official media websites Xinhua and People's Daily – they continue to censor all websites in the Uighur language, and those dealing with Xinjiang. Internet users based in this region are not allowed to leave comments or to view the forum sections of the few accessible sites, nor can they send or receive emails. Censorship may be followed by arrests. Ilham Tohti, an economics professor at Beijing's Central Minorities University and editor of uighurbiz.net, was illegally detained for several weeks during the summer of 2009, which is also when cyber-dissidents and founders of Uighur websites Dilshat Parhat, Nureli, Obulkasim and Muhemmet were arrested. They are still in prison.

### THE WORLD'S BIGGEST PRISON FOR NETIZENS

Thirty journalists and seventy-two netizens are now behind bars for freely expressing their views. The charges brought against them are "subversion" and "dissemination of state secrets."

# China

## "Control 2.0" offensive held in check by inventive netizens

Netizens and dissidents have recently received very harsh prison terms. In December 2009, intellectual Liu Xiaobo was sentenced to a long jail term of eleven years for having written his opinions on the Internet and participated in the launching of Charter 08. Over one hundred other signatories have been questioned, threatened, or summoned by the secret police throughout the country.

Cyber-dissident Huang Qi's three-year jail sentence was upheld on appeal, and blogger Tan Zuoren got five years for having dared to contradict the official account of how the government dealt with victims in the aftermath of the May 2008 earthquake in Szechwan.

Finally, there has been no further news about human rights defense lawyer Gao Zhisheng, arrested on February 4, 2009, raising the fear that he may have died from ill-treatment at the hands of his torturers.

### TIGHTER SURVEILLANCE AND UNRESTRAINED PROPAGANDA

Surveillance is becoming more and more sophisticated. The over 40,000 members of the cyber-police are constantly scanning the Web, keeping a sharp eye out for "subversive elements."

Early this year, following revelations about the pirating of Gmail accounts, some human rights activists and journalists realized that their accounts had been hacked and their emails rerouted to another, unknown, email address.

Cybercafés have also been placed under close surveillance. Their customers are required to produce an ID and have their photo taken. A log of their connections is maintained and made available to the authorities. Their activities are privately monitored in real time by pressured café managers. The connection between police stations and "hotspots" such as cybercafés or financial centers has been expanded and improved within the scope of the "Safe City" project.

The government's position is to prevent access to any "harmful" piece of information by offering an "alternative" official view of events with the regime present "in the field," feeding cyber-space its propaganda, and ready to systematically respond online to criticisms of the regime. Discussion forums are infiltrated by Internet users known as the "Fifty Cent Party," paid to leave positive comments. Welcome to "Control 2.0."

### AN ACTIVE AND INVENTIVE ONLINE COMMUNITY

Nonetheless, a great deal of information is circulating on the Chinese Intranet and heated discussions are going on in online forums. Bloggers and Internet users alike are using more and more proxies and VPNs to circumvent censorship. They keep speaking out against the failings of Chinese society and government abuses, increasingly compelling the official media to cover embarrassing scandals. The new media is thus helping the traditional media to test the limits of censorship. The announcement of the fire that damaged one of the towers of state-owned TV network CCTV was first made via the Internet and Twitter – even though the state-owned media (including CCTV) had received the order not to mention it. Caught in the act, the latter ultimately had to reverse course and provide some form of coverage.

Bloggers like Zola became known for their coverage of social subjects, such as forced evictions. Cyber-dissident Huanq Qi helped to reveal the authorities' role in the collapsing of Szechwan schools after the earthquake. Some of the negligent local officials have been investigated.

# China

## "Control 2.0" offensive held in check by inventive netizens

Internet users can have some degree of influence when they get organized. Charter 08 was posted online and widely disseminated before it became the target of censorship, which explains the witch hunt for its writers. One young woman, Deng Yuqiao, who killed a man who tried to assault her, received support from a campaign conducted in the blogosphere and on Twitter. Netizens launched a genuine hunt to track down corrupt officials. When Twitter was blocked, angry surfers invaded a Twitter "copycat" website, www.t.people.com.cn, launched by the state-owned People's Daily, forcing the site to shut down.

The authorities have grasped the influence that netizens can have and sometimes call on them for help. Web users were invited to participate in an investigation into the death of a young detainee in a Yunnan province prison, although they unfortunately were not given access to all case file documents.

Internet users sometimes use humor, puns, and plays on word pronunciation to ridicule censors. For example, they have given a new twist to the slogan, "The Party's Central Committee policy is yakexi ("good"), which Uighurs chant during the final official Chinese New Year ceremonies using a yakexi homonym meaning "lizard." The term "lizard" began to be used throughout the Chinese Web as a symbol of the fight against censorship. Just like the story of the "Caonima" mudgrass horse, whose name – when pronounced somewhat differently – is an insult, and who is attacked by crabs from the river symbolizing the censors. This story surfaced at the same time that the authorities launched an anti-obscenity campaign. The lizard and the lama achieved unprecedented popularity and served as models for stuffed toys, clips, songs, cartoons, and even parodies of the state-owned CCTV network's "Animal World" program.

### TRADE BARRIERS AND PIRATING

Internet censorship concerns far more than human rights. It also affects trade and business, which are negatively impacted by the lack of access to reliable information. The importing of cell phones and laptop computers equipped with Wifi was prohibited in China because the latter come with filtering technologies that make surveillance more difficult. The iPhone was launched in China only in November 2009, two years after the rest of the world, and without WiFi. Online censorship has also become a way to discriminate against foreign companies and grant preferential treatment to Chinese companies. Visitors to www.Google.com occasionally find themselves rerouted to Baidu. According to the Inside Facebook website, Facebook's Chinese visitors plummeted from one million in July 2009 to 14,000 by the end of 2009. The site is now blocked. Its Chinese counterparts, notably www.Renren.com and www.51.com, now dominate the market. A local equivalent to Twitter was launched once the microblogging site was blocked. YouTube also has its share of Chinese clones, such as www.Tudou.com and www.Youkube.com.

The Wall Street Journal subsequently labeled Chinese Internet censorship as "disguised protectionism." China had promised in 2001, when it became a member of the World Trade Organization (WTO), that it would allow foreign companies to have unlimited access to many services, including online services. It was just critized in December 2009 for its regime's restrictions on the importation and distribution of movies, foreign books and music, which the U.S. has ruled as discriminatory. The WTO recommended that China "bring its measures into compliance." The WTO also needs to examine the issue of online censorship as a barrier to trade.

# CUBA

## Promoting collective access"…. to better prevent individual access

*Domain name : .cu*
*Population : 11 451 652*
*Internet-users : non-available data*
*Average monthly salary : around 20,48 US$*

*Number of imprisoned netizens : 0*
*Average charge for one hour's connection at a cybercafé : 1,63 US$ for the national network – 5,4 to 6,8 US$ for the international.*

Despite a few improvements, Internet access actually remains beyond the reach of most of the population because of its high cost and low connection speeds. The regime, which maintains two parallel network, is now taking aim at a small blogger community that is becoming increasingly active.

### MODEST IMPROVEMENTS

In January 2010, the government announced that Cuba had increased its Internet connection capacity by 10% in the previous month, thanks to an improved satellite link. Although it claims that there will be a qualitative improvement in the island's telecommunications services, it has no intention of expanding them. The government's strategy is to "promote collective access," but in reality, access is still reserved for a privileged few.

Raul Castro raised hopes for broader access in 2008, when he announced that he would lift the ban prohibiting Cubans from owning a personal computer and from visiting tourist hotels in order to access the Internet. However, these new rules did not translate into a more widespread Internet access. The government's priority is still total control of information. Boris Moreno, the Vice Minister of Information Technology and Communications, stated in 2008 that "the use of the Internet [must serve] to defend the Revolution and the principles in which [Cuba] has believed for years."

### THE CUBAN INTRANET AND ITS ABUSES

Two parallel networks co-exist on the island: the international network and a tightly controlled Cuban Intranet consisting solely of an encyclopedia, a few email addresses ending in ".cu" and some government news websites such as Granma. Outside of the hotels, only a few privileged people have special clearance to connect to the international network. The latter is also subject to censorship, which primarily targets dissident publications on foreign websites.

The regime lacks the means to set up a Chinese-style automatic filtering system. But they are counting on several factors to limit Internet access: the exorbitant connection cost – about USD 1.50 dollars per hour from point-of-access to the state-controlled Intranet, and USD 7 per hour in a hotel to access the international network, even though the average monthly salary is USD 20 – and infrastructural problems, notably slow connections. Such obstacles restrict the number of Internet users capable of surfing, as well as the time spent online. Most Internet users are content to read their emails and answer them – they don't have time to browse and "linger" online.

A genuine black market has emerged willing to buy or "rent" passwords and codes of the few individuals and companies that have clearance from the incumbent party to access the Internet. Navigating the Net costs USD 50 per month and receiving/sending one email message USD 1. Illegal users take the precaution of connecting only at night.

### USB FLASH DRIVES: THE LOCAL "SAMIZDAT"

Of the 150+ existing Cuban blogs, some twenty focus on news and commentary about local life. Even the Catholic Church has joined the Web by creating a blog. The majority of bloggers are apolitical and sign their postings using their real name. They avoid discussing the government and dissident movements on the is-

land or abroad. Instead, they focus on Cuban people's daily concerns, thereby filling a void in the regime-muffled state media, which limit themselves to singing the praises of the "Consulante." Bloggers avoid foreign embassies and their Internet access points so as not to be accused of being foreign agents. All of these reasons partially explain why the regime initially left them alone.

These bloggers do not have direct access to their websites, which are not hosted on the island. They have to publish their writings and posts via friends in foreign countries. They do that by following a well-tested procedure: they prepare their content in advance, copy it onto a USB flash drive, and send it via email from a hotel. The USB flash drives, which are being passed from one blogger to another, have become the new vectors of freedom of expression in Cuba – the local "samizdat."

## REGIME REPRISALS

In the last few months, the authorities have begun to unfavorably view this dissemination of news that has been outside of their control and to be offended by the increasing popularity of some of these bloggers, such as Yoani Sanchez and her blog, Generacion Y. Voted by Time magazine in 2008 as one of the year's 100 most influential people, she has been hounded by a genuine defamation campaign on the island. Accused of being a mercenary serving a foreign power, her name has been dragged through the mud by the state media. On November 6 of last year, state security policemen assaulted Yoani Sanchez and blogger Orlando Luis Pardo on the eve of a demonstration. A third blogger, Luis Felipe Rojas, was arrested twice in December 2009 and is being kept under house arrest.

A student named Darío Alejandro Paulino Escobar was expelled from the University of Havana in January 2010 for having created a "polemic" group on the social network Facebook. The group in question contained the minutes of a meeting held by the Union of Young Communists (UYC) (http://www.facebook.com/group.php?v=wall&gid=93444203329).
The authorities are now determined to occupy an area that they had previously overlooked: an official association of Cuban bloggers has been created. And possible links between the Cuban government and hackers who are attacking Cuban websites and blogs hosted abroad are under heavy scrutiny.

The judicial arsenal against online criticism remains particularly repressive. Cuban Internet users face up to 20 years in prison if they post what is deemed to be a "counter-revolutionary" article on a foreign-hosted Internet website, and 5 years if they connect illegally to the international network.

The Cuban regime has been blaming the American embargo for depriving the country of a good Web connection by preventing it from accessing international networks. This problem should be partially resolved in 2011, when the underwater optical fiber cable linking Cuba to Venezuela should come into service, thereby increasing the island's capacity to connect to the rest of the globe. The Cuban government will then need to come up with new excuses to continue justifying censorship, unless it should decide – for economic development reasons – to rethink its Internet strategy. Apparently Yoani Sanchez's predictions that "the real island is starting to convert into a virtual island" will take a little longer than expected to be realized.

# Egypt

## Power struggle between Egypt's government and bloggers

*Domain name: .eg*
*Population: 83 082 869*
*Internet-users: 16 636 000*
*Average monthly salary: around 49,11 US$*

*Number of imprisoned netizens : 2*
*Average charge for one hour's connection at a cybercafé: around 0,20 US$*

More than a mere virtual communications tool, the Egyptian Internet has become a mobilization and dissension platform. Although website blocking remains limited, authorities are striving to regain control over bloggers who are more and more organized, despite all the harassment and arrests.

### THE INTERNET: POPULAR AND POWERFUL

The blogosphere has experienced spectacular growth in the last few years, as a result of the IT development program initiated by the regime. Egypt enjoys one of the highest penetration rates in Africa, even though it is trailing far behind certain Middle East countries. Telecom Egypt, the Egyptian telecommunications company, still has a monopoly on land lines. Connections are often shared between several individuals. Telecom Egypt owns the Internet service provider TE Data, which controls more than half of the market.

Bloggers and netizens use the Internet's huge potential to denounce human rights abuses. It was on the Internet that one of the biggest scandals of the decade was exposed: following blogger Wael Abbas' posting of torture videos filmed in police stations, the implicated police officials were arrested and indicted.

### INTERNET: AN EFFECTIVE PROTEST ENGINE

Demonstrations that cannot take place in the streets because of state of emergency regulations are being transformed into online mobilization campaigns relayed by social networks. Calls for change in the society have been particularly frequent on Facebook. A strike broke out on 6 April 2008 in Mahalla, north of Cairo, site of the country's largest textile factory. The same day, members of a group on the social networking site Facebook were arrested for having passed on information about the strike. When activists declared April 6 the "Day of Anger" in 2009, the call spread via SMS to thousands of people in just a few days. Young people who had not been politically active until then started denouncing the abuses committed by the regime, and social problems that affected them, such as the decline in purchasing power. Some began blogging to imitate bloggers widely known for their activism, like Wael Abbas. April 6 became a symbolic date – a critical annual meeting date for dissenters. The emergence of these new dissidents is frightening the authorities. The regime feels obliged to retaliate and stop the movement by invoking the need to maintain order.

### BLOGGERS: MOBILIZED BUT ALSO HARASSED

In 2008, over 500 of them were arrested for "endangering state security," mainly by virtue of the State of Emergency Law. The crackdown continued in 2009 and prisoners were often ill-treated. Most have been released since then, yet two bloggers are still behind bars. Since January 2009, an average of one complaint per day is lodged against a journalist or a blogger. Legal proceedings are brought at the initiative of the authorities, but sometimes also that of the army or private companies.

Blogger Abdel Kareem Nabil Suleiman, nicknamed "Kareem Amer," is still behind bars. After being made a scapegoat and arrested in November, he was sentenced to three years in prison for "insulting the President" and one year for "inciting hatred of Islam" because of a comment he posted – deemed overly critical of the government – on an Internet forum. He would regularly denounce on his blog the government's totalitarian abuses and criticize the countries most highly respected religious institutions.

Another blogger was imprisoned on very unusual grounds. Ahmed Abdel Fattah Mustafa was brought before a military court on March 1, 2010, where he was court-martialed – despite the fact that he is a civilian – for comments he had posted on his blog in early 2009 alleging a case of nepotism in an Egyptian military school. Detained in solitary confinement for several days, this student was charged with "publishing false news" about the army and "attempting to undermine people's confidence in the armed forces." He was finally released on March 7, after he posted apologies on his blog.

Blogger Tamer Mabrouk was sentenced in May 2009 to pay EGP 45,000 (about USD 8,000) on "defamation" and "insult" charges brought by the Trust Chemical Company, which, in one of his articles, he had accused of polluting.

Wael Abbas, considered to be one of the country's most high-profile bloggers, has been the victim of constant judicial harassment aimed at silencing him – a strategy that is obviously bound to fail. After repeated international protests, in February 2010, he was acquitted on appeal of the six-month prison sentence pronounced against him in November 2009. In a case trumped up by the authorities, he had been found guilty of damaging an Internet cable. Prosecuted again, this time by Telecom Egypt, the blogger was sentenced in February 2010 to another six-month prison term and a fine for "illegal use" of his Internet connection, which he is accused of having shared with several other users.

To demonstrate the kind of influence these bloggers and activists can have, when some twenty of them paid a visit to the city of Nag Hammadi (in Upper Egypt) in January 2010 to pay their condolences to the families of six Coptic Christians killed in a shooting, the police were resolutely waiting for them and sent them back to Cairo on the first train. Authorities were fearful that "they might inflame public opinion and call for demonstrations," in an atmosphere of religious tension that the regime would attempt to put down, according to Nag Hammadi inhabitants.

## NETIZENS UNDER SURVEILLANCE

Since early 2007, the government has been reinforcing Web surveillance in the name of the fight against terrorism, under the iron fist of a special department of Egypt's Ministry of Interior. Facebook has been placed under surveillance, rather than blocked, so that activists can be observed or arrested. Authorities are monitoring their people's emails and telephone calls without any court order, by virtue of the Telecommunications Law, which requires Internet service providers to supply them with the necessary surveillance services and equipment.

Since 2008, conditions for using the wireless Internet network (WiFi) have changed. The connection is not only fee-based now, but it also requires an email address to which the password and user name have to be sent. Cell phone companies are required to obtain their customers' personal data before selling them their services. Anonymity is under siege.

Surveillance is also commonplace in cybercafés, which are frequently visited by the population. The authorities often pressure café managers to gain access to the personal data of Internet users that interest them. A limited number of cafés are asking their customers to present their IDs in exchange for a PIN code that will enable them to access the Net.

Egypt has not yet implemented a Web-filtering policy. In 2007, an administrative tribunal rejected a judge's request to block some forty websites, on the grounds of the need to defend freedom of expression. A few

## Egypt

### Power struggle between Egypt's government and bloggers

"jihadists'" websites are sometimes temporarily blocked. Yet in May 2009, a Cairo court ordered the Egyptian government to block access to pornographic websites deemed incompatible with the country's religious and social values. The result of the appeal and the authorities' reaction will determine whether this ruling will lead to an Internet filtering system in Egypt. For now, however, the Minister of Communications and Information Technologies has publicly excluded this option.

Egyptian bloggers have prevailed in their latest differences with the authorities: according to the Arab Network for Human Rights Information (ANHRI), one Ministry of Communications project was being planned to limit individuals' monthly uploads and downloads to 2 GB at a speed of 264 kb/second. Its aim was to better control the dissemination of information – especially videos. On October 8, 2009, netizens called for boycotting the Web in the course of a campaign nicknamed "the Internet users' revolution." The Ministry chose to back down rather than have to cope with the general outcry raised by this initiative. It acknowledged that "illegal Internet connections are not the problem, rather it is the growing Internet usage." Such statements seem to imply that the power struggle between authorities and bloggers is far from over, with a new mobilization expected on April 6.

# IRAN

## The new media: Enemies of the regime

*Nom de domaine : .ir*
*Population : 66 429 284*
*Internautes : 32 200 000*
*Salaire mensuel moyen : environ 300 euros*

*Nombre de net-citoyens emprisonnés : 13*
*Prix moyen d'une heure de connexion dans un cybercafé : 70 centimes d'euro*

Iran, one of cyber-censorship's record-holding countries, has stepped up its crackdown and online surveillance since the protests over the disputed presidential reelection of Mahmoud Ahmadinejad on June 12, 2009. The regime is demonizing the new media, which it is accusing of serving foreign interest. While a dozen netizens are serving out their terms in Evin Prison, bold Internet users are continuing to mobilize.

### A SMOOTH-RUNNING FILTERING SYSTEM

Censorship is a core part of Iran's state apparatus. Internet surveillance has been centralized, thereby facilitating implementation of censorship. Internet service providers rent bandwidth to the Telecommunication Company of Iran (TCI), controlled by the Islamic Revolutionary Guard Corps (RGC). ICT is responsible for ordering the blocking of websites, which ensures a consistent censorship policy using filtering software developed in Iran. Blocking criteria are defined by the Committee in Charge of Determining Unauthorized Websites (CCDUW). The latter is comprised of members from several government branches and the judicial wing: the Ministry of Communications and Information Technology, the Ministry of Culture and Islamic Guidance, the Ministry of National Security and Teheran's Public Prosecutor.

Censorship is done by combining URL blocking with keyword filtering, as deemed necessary according to changing current events. Among the keywords that have been blocked are the words "woman" in Farsi, "torture," and "rape," since August 2009, when one of the opposition leaders, Mehdi Karoubi, condemned the harsh treatment inflicted on incarcerated demonstrators in Kahrizak Prison.

The connection speed for individuals in Iran is slow and limited to 128 kb/s. By order of the Ministry of Communications, households and cybercafés are prohibited from accessing broadband. This technical obstacle limits Internet users' ability to upload and download photos and videos. Speeds can be even slower in periods of social unrest.

The authorities rely on the Iran Press Law, Penal Code and the Cyber Crime Act of 2009 to prosecute Internet users. Article 18 of the latter provides for a prison term of up to two years and a fine for anyone found guilty of "disseminating false information likely to agitate public opinion."

### SITE BLOCKING

Iran applies one of the world's strictest filtering policies, which have been tightened even more since June 2009. To date, authorities claim to have blocked hundreds of thousands of sites. One thing is certain: thousands of websites and millions of associated pages are now inaccessible in Iran.

Iranian authorities had customarily filtered religious content and sites considered pornographic or obscene. But ever since Mahmoud Ahmadinedjad became President, the censorship has increasingly focused politically oriented websites, or those dealing with the women's rights movement or the defense of human rights. Blocked "feminist" websites include www.we-change.org, www.roozmaregiha2.blogfa.com, and www.parga1.blogfa.com. The reformers' website, www.baharestaniran.com, is also blocked, as is former president Khatami's website, www.yaarinews.ir.

# IRAN



Censorship has mainly affected news websites in the Farsi language, but the blocking of English sites is becoming more and more frequent. The BBC website broadcasts in Farsi have been jammed since January 2006, and the English version only since June 2009.

Just before the presidential elections in the spring of 2009, the authorities issued a list of instructions describing how the campaign should be covered and the responsibilities of Internet service providers. These instructions went into detail concerning some twenty banned topics, including: "endangering national unity" and "creating negative feelings toward the government." This is how news sites likely to contest Mahmoud Ahmadinejad's victory – notably a dozen pro-opposition websites – were censored on the eve of the election.

Since June 12, censorship has reached unprecedented proportions. Officials are tightening their grip on all news media and means of communication that could be used to dispute the "victory." Pro-opposition websites such as www.sahamnews.info, or new websites like www.mizanews.com, are being targeted. Censorship is even affecting such pro-conservative sites as www.ayandenews.com, which highlights the divisions within the regime. Parlemannews - the official website of the reformist deputies' minority fraction – has been intermittently inaccessible since December 26, after the Supreme Council for National Security issued a press release banning any ceremonies commemorating Ayatollah Montazeri, an Iranian religious leader who died last December 20th (http://www.rsf.org/Enterrement-de-l-Ayatollah.html). Some blog platforms such as www.blogfa.com are not totally blocked, but certain individual blogs have been.

## SOCIAL NETWORKS FEEL THE FULL BRUNT OF POST-ELECTORAL CENSORSHIP

Iran's regime considers social networks to be instruments of the opposition. Facebook and Twitter, which relayed the calls for demonstrations, have been continuously blocked since June 2009. MySpace.com and Orkut.com have received the same treatment.

Participative photo- or video-exchange websites were among the first hit: Flickr.com and YouTube.com are inaccessible. The authorities want to block the transmission via the Internet of photos taken with a cell phone. Dissemination of the photos of the young female demonstrator, Neda Agha-Soltan, was too harmful to the regime's reputation. The anonymous video received the prestigious American George Polk Award for Excellence in Journalism in February 2010, while Neda acquired martyr status. During the demonstrations of December 7, 2009, for example, some demonstrators' cell phones were therefore seized by security forces. An as yet undetermined number of people who were taking photos or filming the events with their telephones may have also been arrested.

## CONNECTION SPEED AND TENSION INDICATOR

Since the summer of 2009, as every new opposition event or potential demonstration approaches, Internet speed has been considerably slowed down in the country's major cities, to the point of falling to 56 kb, according to some Internet users contacted by Reporters Without Borders. The authorities' explanation is that it is caused by a technical glitch. They cannot allow themselves to cut off Internet access too long without jeopardizing the Revolutionary Guards' economic interests, but some temporary down times have been noted at critical moments, such as during the 31st-anniversary celebrations of the Islamic Revolution on February 12, 2010. Widespread connection slowdowns, as well as total or limited power outages in certain districts, were observed in several of Iran's largest cities, particularly in Tehran, Mashhad, Ispahan, Ahvaz, and Shiraz. Some cell phone companies would no longer allow users send SMS's after the night of February 6. Cell phone signal jamming had also intensified.

Enemies of the Internet

## SURVEILLANCE

Internet user surveillance is made easier by the fact that all traffic has to pass through a single point controlled by the Revolutionary Guards. A cyber police force permanently monitors the population's online activities.

This partially explains the decision made on February 10, 2010 to suspend Gmail messaging service, which is very popular with the dissidents and more difficult to censor, especially since the emails are encrypted. But users can still access the messaging service via proxy servers. The authorities have announced that a national messaging service will be launched in the near future.

The Nokia-Siemens Network company is suspected of having collaborated with the authorities and facilitated their surveillance of dissidents. Reporters Without Borders asked it to provide explanations in an email dated June 29, 2009. The company acknowledged that it sold traditional surveillance equipment capable of tapping phone conversations to the Iranian Telecommunications Company, but denies that it sold to the latter software capable of intercepting data or monitor Internet activities

## A WAVE OF ROUND-UPS TARGET NETIZENS

With some sixty journalists and bloggers behind bars and another fifty forced to seek asylum elsewhere, the Islamic Republic of Iran has become the largest prison in the Middle East – and one of the world's largest prisons – for journalists and netizens.

Some thirty netizens have been arrested since June 2009, and a dozen are still being detained. They include human rights blogger and activist Shiva Nazar Ahari (http://azadiezan.blogspot.com), who was arrested on December 20 last year, just before Ayatollah Montazeri's funeral. She had already been arrested on June 14, 2009 and held for five months. In Novembre 2008, cyber-dissident Mojtaba Lotfi had been sentenced to four years in prison and to five years of banishment for "disseminating opinions of the Grand Ayatollah Montazeri" and for promoting "anti-government publicity."

Several bloggers and journalistes have been charged with being "mohareb" (enemies of God). They may be facing the death penalty.

## A BLOGGER DIES IN DETENTION

Omidreza Mirsayafi died while being detained, on March 18, 2009. The circumstances of his death have yet to be clarified. He had been given a two-year prison sentence in December 2008 by the Tehran Revolutionary Court for "insulting leaders of the Islamic Republic," and six months for "anti-government publicity," after he posted the offending articles on his blog.

## THE AUTHORITIES RETALIATE VIA PROPAGANDA, INFILTRATIONS AND CYBER-ATTACKS

The opposition has permeated the new media, but the regime was quick to find a way to convey its own message – thus triggering a war of words. A spokesperson for the Islamic Revolutionary Guards announced a plan to launch 10,000 blogs under the supervision of the paramilitary Basij forces. Young IT experts were recruited to form the Revolutionary Guards' "electronic arm." This Iranian Cyber Army is taking credit for cyber-attacks against numerous dissident websites.

Another method used is to reroute certain independent website home pages by linking them to pages on websites relaying government propaganda. The Balatarin website – one of the protest movement's online bastions – was victimized by this strategy.

The regime also created fake Internet websites supposedly run by political organizations or the foreign media, on which surfers are invited to send in emails, videos, and post notices about rallies. This method thus allows authorities to accuse Internet users of being spies acting on behalf of foreign organizations.

## CYBER-DISSIDENCE IS ALIVE AND WELL

The Iranian blogosphere is one of the most active on the planet. The country's young population is very enthusiastic about the Internet, not intimidated by censorship, and very familiar with such circumvention software as UltraReach and FreeGate, developed in the United States by the Global Internet Freedom Consortium, and which many Iranians use.

Another example of mobilization occurred when hundreds of Iranians dressed up as women wearing a "hijab" and posted a photo of themselves on their Facebook profiles in December 2009. That was their way of expressing support for Majid Tavakoli, an activist student arrested in Tehran and charged with disguising himself as a woman so that he could make a discreet getaway following a Tehran rally celebrating National Students Day, in which he made a speech. Surfers around the globe expressed their solidarity with the Iranian demonstrators, as did the Chinese netizens who launched the "#CN4Iran" (China for Iran) campaign on Twitter.

# North Korea

## Excluded from the digital era

*Domain name : .kp*
*Population : 22 665 345*
*Internet-users : non-available data*
*Average monthly salary : around 17,74 US$*

*Number of imprisoned netizens : 0*
*Average charge for one hour's connection at a cybercafé : around 8,19 US$*

In the world's most hermetic country, the large majority of the population is not even aware that the Internet exists. An extremely limited Intranet has been created, but few can access it. The network is used by Kim Jong-il and a few senior officials for their personal enjoyment and to help spread the regime's propaganda to foreign countries. The only glimmer of hope: the communications black market on the North Korean-Chinese border.

### INTERNET: NOTHING BUT A VAGUE RUMOR

North Korea is literally cut off from the rest of the world, and the Internet is no exception. The international network is accessible only by a small minority: a few high-ranking members of the regime and foreign diplomats, via a satellite link with servers based abroad. Kim Jong-il is known for his obsession with electronic gadgets, and for having asked former U.S. Secretary of State Madeleine Albright for her email address so that he could write to her. However, he is keeping the rest of the population totally secluded from the Web. In a country whose inhabitants' main concern is survival, the Internet's existence is little more than a rumor.

A very limited Intranet has developed, consisting of an email inbox, a few news sites relaying regime propaganda, and a browser providing access to the databank Web pages of the country's three biggest libraries: the Grand People's Study House and those of the Kim Il-Sung and Kim Chaek Universities. This Intranet is accessible only by academics, businessmen and high-ranking civil servants who have received special clearance.

The very rare cybercafés that have opened in the capital are under the strict control of the Korean Computer Center, the country's sole access provider. Although they make it possible to connect to the North Korean Internet, their customers consider them first and foremost as points of access to computers and games.

The Internet Corporation for Assigned Names and Numbers (ICANN) has finally assigned North Korea the ".kp" domain name and appointed the President of the Chosun Computer Center's European Section, a German, as Administrator. The country is said to have thirty IP addresses that it is not using at the moment. The official state website, www.korea-dpr.com, is supposedly hosted in the United States, and that of the Chosun Central News Agency in Japan.

### ONLINE PROPAGANDA

North Korea's very minimal presence on the Web is totally devoted to singing the praises of Kim Jong-il and of his father, Kim Il-sung, as well as the self-reliance ideology – "Juche Idea" – extolled by the regime. A few dozen websites relay these official positions...and are blocked in South Korea. The official Chosun News Agency website, for example, disseminates only "positive" news about the country, whether Kim Jong Il's visits to his compatriots or news about the extremely rare groups abroad that still support the country. Any negative news is intentionally omitted.

North Korea is also suspected of having mounted a DdoS-type cyberattack against some thirty American and South Korean business and government websites in the summer of 2009.

# North Korea

Excluded from the digital era



## VAGUE HINTS OF A CONCILIATORY ATTITUDE?

Since the beginning of 2008, a new cell phone service has been installed by the Egyptian company Orascom, but it is very limited, servicing mainly Pyongyang and a few large southern cities. It is too expensive for most of the population and does not allow international calls. The state security police track any people who might be tempted to use telecommunications to circumvent censorship. One man was executed in 2007 for making an unauthorized phone call to a foreign country. North Korea is probably the only country in the world in which the telephone book is classified as "top secret."

Accustomed to maintaining complex relations with the global community, the regime is vacillating between provocation and dialogue. When it makes a seemingly conciliatory gesture and allows foreigners to enter its territory, it grants them access to the World Wide Web. For example, when the New York Philharmonic Orchestra visited the country in 2008, the musicians and journalists who accompanied them had access, in their hotel, to a high-speed World Wide Web connection. Some tourist sites also reportedly benefit from Internet access at certain times.

The limited news that enters the country comes through its border with China, thanks to individuals who commute between the two countries, and the CDs and DVDs that are illegally brought in. The black market is thriving. Telephones from China allow users to make calls by picking up a signal at the border. The recent introduction of 3G telephones in China may also allow better access to the Internet in these border regions. Other alternative news sources include the DailyNK website, managed by North Korean refugees based in South Korea. Independent radio stations that transmit from South Korea to North Korea – Free North Korea Radio, Radio Free Chosun, Open Radio for North Korea and North Korea Reform Radio – gather their news by calling upon "stringers" based on the Chinese border.

## THE REGIME'S REVENGE

Nonetheless, in February 2010, North Korean authorities announced that they would intensify the crackdown on "defectors," and by the same token deploy stricter control on the means of communication at the border, notably targeting the Chinese cell phones used in North Korea. The regime boasted that it has the means to "crush reactionary forces" and that it has already provided an example by executing a worker accused of having used an "illegal" Chinese cell phone. According to Open Radio for North Korea, he allegedly divulged information about the price of rice and his lifestyle to a "defector" friend living in South Korea. Radio Free Asia has specified that the government has acquired equipment that can block cell phone signals and intensified the tracking and jamming of such signals. Allegedly, the equipment concerned will be installed at the country's Chinese border, in cities such as Shinuiju, Hyesan and Hweryong.

Although the "Beloved Leader" is sick, very little news has leaked about his potential successor – his youngest son – other than the fact that he studied in Switzerland. His views on information control are therefore completely unknown.

One thing is clear: the incumbent regime has no intention of allowing its population – steeped in an omnipresent propaganda – to learn more about the outside world. The information disseminated on the Internet, as well as news broadcast on international radio stations, could convince more North Koreans to flee the country.

# Saudi Arabia

## An emerging bloggers' community is up against harsh censorship

*Domain name : .sa*
*Population : 28.686.633*
*Internet-users : 7.700.000*
*Average monthly salary : around 21 836 US$*
*Number of imprisoned netizens : 0*
*Average charge for one hour's connection at a cybercafé : 2 to 4 US$*

These bloggers are confronting the traditional forces of Saudi society which are attempting to prevent the Internet from becoming a forum for free discussions. A legislative arsenal is bound to intimidate netizens and promote a tendency for self-censorship.

Saudi Arabia is one of the first countries to have been authorized to write Internet domain names in Arabic. The Internet penetration rate, currently estimated at about 38% of the population, is rising. However, it is still one of the most repressive countries with regard to the Internet.

### SEVERE FILTERING AND DENOUNCEMENTS

Very strict filtering targets any content of a pornographic and "morally reprehensible" nature. Websites that broach the subject of religion, human rights or positions taken by the opposition are also rendered inaccessible. Far from denying it, the authorities maintain that their censorship decisions are justified and claim to have blocked some 400,000 websites. Moreover, the Internet Services Unit explains the principle involved on its site www.isu.net.sa/saudi-internet/contenet-filtring/filtring.htm. It is making available special forms which citizens can use to request the blocking or unblocking of a website.

And citizens are taking full advantage of it. The Telecommunications and Information Technologies Agency recently stated that the number of such blocking requests concerns between 700 and 1,000 sites per day, or an average of 300,000 sites "denounced" by citizens per year. A representative of the same Agency estimates that 93% of the filtered sites are pornographic in nature. The others are said to concern sites which circulate information "contrary to Kingdom values." In a recent study, however, the Agency acknowledges that 55% of the users are worried about these site blockings and feel that the current filtering practice is excessive.

### CYBER CAFES UNDER SURVEILLANCE

Draconian restrictions were imposed on cyber cafes in April 2009. Since then, they have been required to install hidden cameras, supply a list of customers and websites consulted, not permit the use of prepaid cards or of unauthorized Internet links by satellite, close at midnight and not admit minors.
Their owners can face a prison sentence if their premises are used to distribute information contrary to "Kingdom values" by virtue of the new law on the use of technology which entered into force in January 2008.

This law also provides a ten-year prison term for owners of Internet websites which support terrorism and five years for those who distribute information of a pornographic nature or which is in violation of the country's religious and social values.

### RISKS INCURRED BY INCREASINGLY ACTIVE NETIZENS

The Arab Network for Human Rights Information estimates that there are about 10,000 active blogs in Arabic and in English in the country.

# Saudi Arabia

## An emerging bloggers' community is up against harsh censorship

Bloggers who permit discussion of sensitive subjects run the risk of censors' reprisals. In 2008, for the first time, Saudi authorities imprisoned a blogger, Fouad Al-Farhan, for having published on his blog (http://www.alfarhan.org) an article describing the "advantages" and "disadvantages" of being a Muslim. In July 2009, Syrian blogger Raafat Al-Ghanim, a resident of Saudi Arabia, was also arrested. He did not hesitate to criticize the social and political status of both countries. There has been no news of the blogger since his arrest.

Recently, participating websites have been particularly targeted by censors. The site newarabia.org, a political discussion forum, is inaccessible in the country. The blogger.com platform, which was at first totally blocked, is now the subject of a targeted censorship of its content – proof that the authorities cannot prevent bloggers from existing, either. Authorities cracked down for the first time on Saudi users of the Twitter micro-blogging website last August. The Twitter pages of two human rights activists, Khaled al-Nasser and Walid Abdelkhair, were then blocked.

The American journalist Courtney C. Radsch, who was working in Dubai for the Internet website of the Saudi information chain Al-Arabiya, was fired in October 2009 following the posting on the Internet site of an article about safety violations by the national air carrier, Emirates Airlines. Her work permit having been revoked, she was forced to leave the country.

The Al Watan newspaper's website was hacked into last November. The following statement was posted on the home page against a black background: "There is only one God and Mohammed is his prophet." The newspaper is said to have come under constant attack since an article was printed criticizing certain religious leaders for having denounced the "mixed regime" in the newly built King Abdullah University of Science and Technology (KAUST).

The tight control of the Internet in Saudi Arabia also reveals the government's determination to maintain the social order – for the Net has provided a previously non-existent space in which women, who represent over half of the bloggers and two-thirds of Saudi netizens, can express their views. Women can discuss subjects online that would be taboo for them to mention in public, such as health.

# SYRIA

## Zero tolerance for freedom of speech on the Internet

*Domain name : .sy*
*Population : 21 762 978*
*Internet-users : 3 565 000*

*Average monthly salary : around 1 079 US$*
*Number of imprisoned netizens : 4*
*Average hourly charge for one hour's connection at a cybercafé : 1,4 to 2 US$*

Syria is reinforcing its censorship of troublesome topics on the Web and tracking netizens who dare to express themselves freely on it. As a result, social networks have been particularly targeted by omnipresent surveillance. The promised technological improvements are slow to materialize. The authorities' distrust of the potential for dissident online mobilization may be playing a role in this delay.

### CONTROLLED INTERNET GROWTH

The number of Syrian surfers has soared in the last ten years. Over 16.5% of the population uses the Internet, and conditions for access have been facilitated. Today, anyone can buy a pre-paid Internet access card and get connected. There is no longer a requirement to provide personal data since these are already registered when Syrians acquire their land phone lines. The limited number of ADSL or 3G is probably due to their high cost. Satellite connections are prohibited without the authorities' express permission.
The officials have centralized Internet surveillance by entrusting it to two government bodies: the Syrian Telecommunications Establishment (STE) and the Syrian Information Organization (SIO), which controls bandwidth. Since 2005, several private Internet service providers have emerged, but they are far from being independent. The Arab Network for Human Rights Information claims that while Internet access has boomed, the infrastructure has not improved much since Internet service became available in the country, thus leading to problems with overload, connection speed slowdowns and frequent power outages. The Ministry of Communications and Technology announced a "global development and reform of the Internet" strategy which, in reality, has yet to be implemented. The quality of the cable connecting Syria via Cyprus needs to be improved, as does the bandwidth capacity. A new trans-ocean cable could be set up.

The Syrian government, which for had long been minimizing its Web presence, has completely reversed course: propaganda sites and those promoting the official position are proliferating, such as the Syrian News Agency (SANA), or the Syria News, Al-Gamal, Sada Suria and Sham Press websites.

The ThunderCache software program is used by the STE and the SIO to ensure centralized censorship of the Web. Its distributor, Platinum Inc., defines it as being used "to protect Web communications against risks from spyware, viruses, inappropriate Web surfing, instant messaging (IM), video streaming and peer-to-peer (P2P) file sharing, while actually improving Web performance." It conducts website surveillance and filtering by searching for keywords "banned" by the authorities.

### FILTERING OF SPECIFIC CONTENT

Censorship in Syria has intensified since 2009. Over 200 sites are currently blocked. The content affected concerns political criticism, religious matters, websites deemed "obscene," those dealing with the Kurd minority and Israel-based websites. Also targeted are opposition party sites, those of certain Lebanese media and independent news websites. The Syrian government justifies such censorship by emphasizing the need to prevent religious discord and Israeli infiltration.

Censorship is particularly targeting social networks and blog platforms in an effort to prevent dissidents from getting organized and recruiting new members using the new media. Blogspot and Maktoob are blocked. YouTube has been blocked since August 2007 after videos were circulated denouncing the crackdown on the Kurd minority. Wikipedia's Arabic version was blocked from May 2008 to February 2009. Amazon and Skype are also inaccessible.

# SYRIA

## Zero tolerance for freedom of speech on the Internet



### PRISON SENTENCES IN EXCHANGE FOR FREE EXPRESSION OF VIEWS ON THE INTERNET

At least four netizens are currently behind bars. They are meant to serve as examples to other Internet users, who prefer self-censorship to loss of their freedom over a few online comments. The authorities have several legislative weapons at their disposal: the Penal Code, the 1962 State of Emergency Law, and the repressive 2001 Press Code amended in 2005 to cover online publications.

In May 2008, blogger Tariq Biassi (http://alzohaly.ektob.com/) was sentenced to three years in prison for having posted an article on an Internet forum criticizing Syrian security agencies. He was found guilty of "spreading false information" and "weakening national sentiment" by virtue of Articles 285 and 286 of the Syrian Penal Code. He had denied all of the charges and assured authorities that the published comments were not his, because he shared his telephone line with six other subscribers, including a cybercafé. In September 2009, Blogger Kareem Arbaji, who is also the Akhawiya forum webmaster, received a three-year prison term for "publishing mendacious information liable to weaken the nation's morale." He had been arrested in 2007, and is said to have been tortured while being detained. On April 9, 2008, writer and poet Firas Saad was sentenced to four years in prison based on the same charges as Tariq Biassi. On May 6, 2008, Syrian government security agents arrested Habib Saleh, a writer and a cyber-dissident.

### CLOSELY WATCHED SURFERS

The authorities never relax their surveillance efforts: They eventually identified Tariq Biassi by retracing the origin of his Internet connection. Since July 25, 2007, owners of Internet websites are required to maintain the personal data of anyone who posts online articles and comments.

Police raids of cybercafés are common. Security agents who catch Web users in the act of "excessive surfing" suggest that they "take a coffee break" with them – their expression for taking them in "for an interrogation." The café managers have to keep a record of their customers' personal data and a list of the websites they consult, and must alert authorities if they observe any illegal activities. Users even have to provide their fathers' and mothers' names. In 2009, a Menassat website contributor was arrested in a cybercafé and briefly questioned.

### EMERGENCE OF ONLINE PRESSURE GROUPS

Many Internet users are mastering the use of censorship circumvention tools. Some use Lebanese or Saudi Arabian servers to access the Internet. When the authorities start to block the most often-used proxy servers, others are created.

Facebook was blocked when Syrians began to make friends with Israelis. However, the surfers are now using proxies to gain access to it. The social network, which is very popular in the country, hosts hundreds of groups with hundreds – or even thousands – of members, devoted to tourism, business, sports, technology and entertainment. Facing pressure from the general population, authorities are examining the possibility of unblocking Facebook.

# Syria

## Zero tolerance for freedom of speech on the Internet

Online pressure groups have formed to express their economic or social demands. One online campaign that opposes a bill on amending the existing personal statute law seems to have played a crucial role in the government's decision to abandon it. Bloggers launched a plea for a boycott of cell phone service providers because of their high cost and declining service quality. Mobilization efforts were also made on behalf of imprisoned bloggers. Despite the crackdown, courageous netizens are capable of organizing themselves. They are counting on the upcoming technological improvements – essential to the country's economic future – to provide them with more options for circumventing censorship and ensuring its failure.

# TUNISIA

## Shameless censors

*Domain name : .tn*
*Population : 10 486 339*
*Internet-users : 3 000 000*
*Average monthly salary : about 424 US$*

*Number of imprisoned netizens : 0*
*Average charge for one hour's connection at a cybercafé : between 0,68 and 1,37 US$*

Deemed a potential threat to the country's stability and image, the Internet is the target of pernicious censorship. Very strict filtering, opponent harassment and Big Brother-like surveillance enable the authorities to keep tight control over the news media.

Unsurprisingly, the presidential and legislative elections of October 25, 2009 led to the victory of outgoing President Zine El Abidine Ben Ali, ushering in a period of repression against opponents and dissidents. The Internet was not spared. Any criticism of the regime, whether online or offline, exposes offenders to reprisals.

### STRICTLY CONTROLLED GROWTH

Pursuing an active infrastructures and communications development plan to attract foreign investors, Tunisia has acquired the status of IT leader in the region. Yet this plan does not at all encompass letting the Internet become a free expression Space.

In the last few years, Tunisia's lower-cost Internet access policy has been pursued in tandem with strict content control. Bandwidth is owned by the Tunisian Internet Agency (TIA), under the control of the government, which imposes strict filtering. Both URL addresses and keywords are blocked. All of the country's 12 state-owned or private Internet access providers are controlled directly or indirectly by the regime. Filtering is performed via SmartFilter and Websense software programs at the network entry level.

### PERNICIOUS CENSORSHIP

Authorities claim to target only pornographic or terrorist websites. However, censorship applies above all to political opposition, independent news, and human rights websites. Websites now inaccessible include those of Tunisnews, Nawaat, the Progressive Democratic Party (PDPinfo.org), the "Al-Nahda" (Renaissance") movement, Tunisonline, Assabilonline, Reporters Without Borders, and Al-Jazeera in Arabic. Al-Jazeera in English, however, is still available.

Social networks and other participating websites whose mobilization /whose potential as a mobilization tool terrifies the regime are targeted when their users behave too boldly. Facebook was blocked in August 2008, raising a wave of general protests within Tunisian society. As a result, President Ben Ali ordered it to be unblocked. Interestingly, rich and fashionable young people as well as people close to the government use it regularly. The President's own page has over 120,000 fans. However, frequent pirating of dissidents' Facebook pages has been observed, as well as blockings of specific groups such as one created to call for the release of independent journalist Taoufik Ben Brik.

When an Internet user attempts to access a prohibited website, the following automatic error message appears: "Error 404: page not found," without displaying the familiar "Error 403" more typical of a blocked site. Users thus do not know if the site has been blacklisted, or if it is simply a technical glitch. This strategy equates to a disguised form of censorship.

# TUNISIA





## GENERALIZED SURVEILLANCE

No one escapes such surveillance – certainly not dissidents, not top presidential advisors, nor even Tunisians based abroad.

The National Information Security Agency, whose official mandate is to protect clients from viruses, has turned into a cyber-police force for the surveillance of email boxes and Internet user websites – particularly those of dissidents. A ministerial order requires service providers to convey a list of their subscribers to the TIA. The filtering software can be used to monitor and intercept emails, as authorized by the 1998 Postal Code law prohibiting email deemed to "threaten the public order."

Censorship does not create a pro-business environment. Businesses and embassies which cannot solely rely on the Tunisian network, and which need to maintain the confidentiality of their communications, are turning to secure connections via satellite.

However, private Internet connections via satellite are prohibited for individuals via land-line telephones. In order to more closely monitor dissidents, users keep the same IP address regardless of whether they are connecting from their homes or from their workplaces. Email boxes are also under surveillance.

Cybercafés have not escaped this oppressive surveillance: instructions about which websites should not be visited are posted on the walls. Managers are responsible for the content viewed by their customers, who usually need to show their IDs. All cybercafés were ordered to use the Publisoft software in 2009, several months before the elections, so that the authorities could spy on users and their online behavior.

## NETIZENS IMPRISONED IN THE LAST FEW MONTHS

The authorities used the legislative arsenal at their disposal to silence dissidents online and put them behind bars, just like they were already doing with journalists. Zouhaïer Makhlouf, an online journalist for the news website Assabilonline, was released on February 12, 2010 after having spent nearly four months in prison. He had received a four-month jail term and been fined TND 6,000 (about USD 4,200) for his report on environmental conditions in the industrial zone of Nabeul. Well-known blogger Fatma Arabbica was detained for several days in November 2009 and is still being investigated.

## HACKED WEBSITES AND OTHER HARASSMENTS NOT DETERRING ACTIVIST BLOGGERS

Two blogs hosted on the RSFBlog platform were hacked in September 2009: http://tunisiawatch.rsfblog.org – the blog of former judge and human rights activist Mokhtar Yahiaoui – and http://www.moncefmarzouki.com, the blog of a Tunisian dissident, Dr Moncef Marzouki. Tunisian opposition news websites Tunisnews and Kalima, hosted abroad, are frequently hacked, most often by way of Ddos attacks, and deletion of content.

Other methods used against dissidents include: Internet connection cut-offs, port /no hyphen/blocking, virus and malware infections, infiltration of discussion forums. E-mails originating from "hostile" destinations cannot be viewed properly or at all. E-mails sent by Reporters Without Borders have been rendered illegible or have disappeared from inboxes.

# TUNISIA

## Shameless censors

The escalation of abuses and sanctions imposed might discourage netizens. But the Tunisian blogosphere is turning out to be energetic and ready to mobilize for certain causes. One example was in February 2010, when users rallied around a campaign to demand the release of Tunisian students arrested for having defended the right of female/important distinction/ students to obtain lodging. The censorship of the "Free Tunisian Students" blog – like that of Fatma Arabicca's blog – triggered waves of protest in the blogosphere that, according to Global Voices, denounced the censorship of "Ammar Scissorhands" – the nickname given to Tunisia's censorship machine.

# TURKMENISTAN

## Internet overlooked in the energetic opening

*Domain name: .tm*
*Population: 5 342 342*
*Internet-users: 127 000*
*Average monthly salary: around 205 US$*

*Number of imprisoned netizens : 0*
*Average charge for one hour's connection at a cybercafé: 0,8 to 1,4 US$*

President Berdymukhamedov has partially broken the diplomatic isolation maintained by his predecessor, the tyrant Niyazov. But the relative economic openness has not translated into more Internet or social freedoms. Scarcely 1% of the population has access to the Web. Information is still oppressively controlled in this post-Stalinian dictatorship.

### TENTATIVE IMPROVEMENTS

Individual Web connections have only been authorized since 2008. Permission for Internet access was first granted to businesses, then gradually extended to their employees, and finally to the country's citizens. Pyramid Research, a telecommunications research organization, estimates the number of individual subscriptions as of the end of 2009 at 13,200 and the number of users at 127,000. The American Information Center, French Cultural Center, and International Turkmen Turk University, as well as some Turkmen private schools, are proposing access to the international network.

Connection speed is not as slow as it used to be: it now takes only a few minutes to open an e-mail, as opposed to at least a half-hour in 2008. Sending or receiving a photo takes longer, and a video takes 30 minutes.

Given this situation, very few Turkmen have acquired an Internet connection in their homes. The cost is prohibitive: a monthly subscription costs USD 5, and an additional USD 0.50 per hour. The average salary is less than USD 200 per month.

The incumbent president has kept his promise to allow cyber cafes to open. However, users are required to show an ID and to pay the considerable sum of USD 1 to 2 per hour. Some 15 of them are currently operating in the capital Ashgabat, as well as in other large cities such as Dashoguz. Uniformed policemen are no longer being posted at cyber café entrances to intimidate customers, but the secret service still raids them on occasion. In one raid in 2008, an Internet user accused of consulting prohibited websites was arrested.

### THE "TURKMENET"

Apart from a few businesses and foreign embassies that can access the Worldwide Web, the few other Internet users can only access an ultra-censored version of the Internet nicknamed "the Turkmenet," unless they know how to use censorship circumvention tools.

A very strict filtering is now focused on critical publications likely to initially target local users and potential dissidents, mainly for linguistic reasons. Opposition websites such as XpoHo.tm and Gundogar, and regional news sites covering Central Asia, such as ferghana.ru or eurasianet, are blocked. YouTube and LiveJournal were rendered inaccessible at the end of 2009 to prevent Turkmen from blogging or sending videos abroad. Facebook, which is not used very extensively in the country, is not blocked – at least not for the moment. However, Turkmen can visit most generalist NGO Websites. The same scenario applies to Russian and Turkmen media sites that contain no articles critical of the country, notably because of the significant commercial ties between Turkmenistan on one hand, and Russia and Turkey on the other.

# TURKMENISTAN

## Internet overlooked in the energetic opening

The government is keeping a close watch on its netizens' activities. Officials prefer to monitor the surfers' e-mail accounts (mail.ru, hotmail, etc.), rather than block them, so that they can identify potential dissidents.

### WESTERN BUSINESSES: VECTORS OF CHANGE?

The Russian telecommunications company MTS holds an 80% share of the mobile telephone market, which is an increasingly lucrative sector. MTS is now also offering Internet access via GPRS, which may facilitate access for the general population. The terms of use specify that the Internet is filtered.

Improving telecommunications infrastructures is not an absolute priority for authorities at the moment, when close to 25% of the population are still living below the poverty level. The international community cannot be counted upon to further the cause of freedom of expression in a country which seems to be an Eldorado for Western businesses enticed by Turkmen gas fields. However, the country's economic openness could have a positive impact on the Internet penetration rate within the population, as long as the latter does not try to explore subjects deemed too sensitive, or develop any form of civil society. Foreign companies could become vectors of change by calling for a generalization of modern means of communication suitable for commercial and entrepreneurial activities.

# UZBEKISTAN

## Draconian censorship amidst widespread indifference

*Domain name : .uz*
*Population : 26 606 007*
*Internet users : 7 740 000*
*Average monthly salary : around 68 US$*

*Number of imprisoned netizens : 0*
*Average price of an hour's connection in a cybercafé : around 0,19 US$*

In this country deprived of independent media outlets, the authorities impose a very strict Internet censorship, while refusing to admit it publicly. Website filtering, sanctions and intimidations are used against potential critics of the regime. Netizens have learned to practice self-censorship..

### MASSIVE CENSORSHIP OF POLITICALLY ORIENTED CONTENT

The government intensified its crackdown on the Internet, particularly after the 2005 Andijan massacre, in order to impose only its version of the facts on the Uzbekistan population. At that time, access to nearly all Internet websites had been blocked. Authorities are now attempting to prevent the opposition based both inside and outside of Uzbekistan from connecting with the Uzbek society via the Internet and the new media, which are becoming increasingly popular in the country. The number of Internet users rose from 2.4 to 7.74 million from 2008 to 2009, according to the authorities.

The lengthy list of "sensitive" subjects includes corruption of government officials, criticism of the regime, and the deplorable status of human rights. Among the blocked sites are those of the online news agency www.Ferghana.ru, and Nezavisimaya Gazeta (www.ng.ru). The regional news website www.CentrAsia.ru is partially blocked, but most of its pages can be viewed. If surfers attempt to gain access to prohibited articles, they are redirected to the home page. The website of the Central Asian News Service, www.ca-news.org, is also partially blocked. The BBC's Uzbek-language broadcasts are constantly blocked, while the Russian version is only periodically blocked. Social networks such as Livejournal, MySpace, Facebook, Twitter, Blogger, Flickr and Uzbekistan's most popular blog platform, www.Kloop.kg, are sporadically inaccessible. The websites of Russian TV networks Russia 1 and Vesti 24 were blocked after they broadcast news that Uzbek photographer Oumida Akhmedova, accused of "insulting" and "slandering" the Uzbek people, had been granted an amnesty. The artist's works had addressed poverty and women's rights.

Most Internet service providers gain World Wide Web access through the National Information Transmission Network (UzPAK) operator. Filtering is enforced at this level. But one of the state-owned service providers, Tashkent City Telephone Network (www.tshtt.uz) independently blocks websites not rendered inaccessible by UzPAK. Every service provider must obtain a license from the Ministry of Communications and Information.

The Internet version that the population can access once the "harmful" websites are made unavailable is called "UzNet."

According to the online news agency www.Ferghana.ru, the regime launched a campaign through the state-controlled media to justify Internet censorship to the general public. The deputy editor-in-chief of Halk Suzi, one of the country's three biggest dailies, allegedly supported the muzzling of websites relaying "unacceptable criticism," and suggested setting up a system equivalent to an "Electronic Great Wall of China."

### A LIBERTICIDAL LEGISLATIVE APPARATUS THAT SCOFFS AT THE CONSTITUTION

While the Constitution guarantees free access to information, this principle is ridiculed on a daily basis, mainly because it is rendered ineffective by the adoption of many other pieces of legislation.

# UZBEKISTAN

Draconian censorship amidst widespread indifference

The 2002 Law on the Principles and Guarantees of Freedom of Information authorizes the government to use restrictions when it deems it necessary to protect anyone against "the psychological impact of negative information." Decree no. 216 of 2004 prohibits ISPs and operators from disseminating certain types of information. The national operator UzbekTelecom broadly interprets targeted content. The 2007 Media Law, which also applies to online media, renders editors and journalists liable for the "objectivity" of their publications.

The Uzbek National Security Service (NSS) is responsible for Internet surveillance and for ensuring that these rules are being enforced by ISPs and cybercafés

## NETIZENS UNDER SURVEILLANCE

The one thousand cybercafés that operate in the country are unevenly monitored. The use of spyware is widespread. Tests carried out by Reporters Without Borders have shown that certain café managers resisted installing anti-spyware software on one of their computers, while in other cybercafés, this tampering went almost unnoticed. Various censorship circumvention tools may have been used in certain cafés, but not in others. Several OpenNet Initiative researchers were therefore questioned in 2007, while they were testing website filtering systems.

Emails are also under surveillance, as are chat rooms, particularly those of ICQ and Mail.ru Agent. Several people are thought to have been arrested in January 2010 for their alleged membership in extremist religious organizations, after being spotted from their conversations on Mail.ru Agent.

## HARASSMENTS AND INTIMIDATIONS

Netizens wishing to express themselves freely online are risking a great deal. One high-profile case is that of online journalist Djamshid Karimov, the President's nephew, widely known for having denounced corruption among the Jizzak region's authorities, and who was forcibly confined in a psychiatric hospital in 2006. The rare independent journalists who have remained in the country are constantly harassed by authorities and summoned to the police station. Ten of them are behind bars. Among them is Solijon Abdurakhmanov, who was sentenced in 2008 to serve a ten-year prison sentence for "drug possession with the intent to sell," in a totally fabricated case.

## HYPOCRITICAL AUTHORITIES ENCOURAGED BY A NON-REACTIVE INTERNATIONAL COMMUNITY

Despite this incriminating record, Uzbek authorities deny the scope of the censorship, which they justify by claiming it is necessary to protect national security, and they are even trying to make it seem reasonable to the international community. The government is displaying boundless hypocrisy in attempting to make people believe that the country is opening up to some degree. In a February 2010 speech, President Islam Karimov blamed the media for not being aggressive enough. He stated: "It is necessary to create additional conditions for better coverage of both foreign and domestic policy by [the] mass media". His sole aim is to please investors. Karimov has no intention of stopping the censorship.

At any rate, the country's strategy seems to be working. Attracted by Uzbekistan's energy resources, the European Union has agreed to take a reconciliatory approach with Uzbekistan and voted in 2008, and again in 2009, to lift the sanctions that had been imposed following the Andijan massacre.

# VIETNAM

## A wave of brutal crackdowns

*Domain name : .vn*
*Population : 88 578 758*
*Internet-users : 21 963 117*
*Average monthly salary : about 68 US$*

*Number of imprisoned netizens : 17*
*Average charge for one hour's connection at a cyber-café : about 2,7 US$ for tourists. But cheaper for nationals.*

The progress made by Vietnam in the domain of human rights, which allowed the country to become a member of the World Trade Organization in 2007, is nothing but a distant memory. As the 2011 Communist Party Congress draws nearer, the regime is muffling dissident views on the Internet, and its first target is critics of the country's policy toward China.

### TOO POPULAR FOR ITS OWN GOOD

In the last ten years, the Internet's growth has soared, as has the country's economic integration. The Web has been a great success with Vietnam's young population. In November 2009, the social network Facebook boasted a million users, as compared to only 50,000 early in that year.

Cybercafés are still the main means of Internet access. Managers rarely ask their customers to present their IDs, but they are required to record in detail what connections they make. Some arrests involving customers who consult prohibited websites have been noted in the past.

A citizen journalism network has developed. Websites such as Vietnam Net and Vietnam News discuss subjects like corruption, social issues, and the country's political situation. Blogger conduct actual on-site investigations that could not be reported by the traditional state-owned media. Thanks to the Internet and the discussion and information-sharing forums that it offers, a virtual civil society has emerged in which pro-democracy activists can find refuge – a fact that unnerves the authorities.

After having paved the way for it in 2008, in 2009 the regime initiated a takeover of the Internet. In October 2008, the government set up a new administrative entity, the Department of Radio, Television and Electronic Information under the Ministry of Information and Communications. This Ministry passed an order in December 2008 that reinforces government control of the Internet. Web users who disseminate information "hostile" toward the government may be subject to sanctions. Since January 2009, new measures have been implemented to regulate Vietnamese blogs. In a document intitled "Circular no. 7," the authorities required that blogs only provide strictly personal information (Art. 1). For example, Internet users are not permitted to disseminate press articles, literary works, or other publications prohibited under the Press Law (Art. 2). Further, every six months, or at the authorities' request, the host companies must produce a report on their customers' activities that mentions the number of blogs they manage and their statistics, as well as any data relating to blogs that have violated the host company's regulations (Art. 6). The Ministry of Public Security is also implicated in Web surveillance.

### EXCESSIVE CENSORSHIP

Even though the country claims to filter only content that is obscene or endangers national security, censorship also affects opposition websites or those that are in any way critical of the regime. One subject that is growing more and more taboo is territorial disputes between Vietnam and China in the China Sea. Censorship primarily involves blocking website addresses, and particularly concerns sites in Vietnamese. The various Internet service providers enforce these rules unevenly.

The number of cyber-attacks is growing. Hackers – especially in January 2010 – have zeroed in on sites that "push the envelope" of freedom of expression on the Internet: www.bauxitevietnam.info and www.bl-

ogosin.org. Although they take a moderate tone, these sites have proven to be critical of the authorities' policies with regard to Beijing. The "Bauxite VietNam" website was created by three intellectuals in 2008 to relay a campaign objecting to the operating plan of a Chinese company's bauxite mining project in Vietnam's Central Highland region, approved by the Vietnam government despite the unfavorable opinion of scientists and environmental activists. This website has been turned into a sort of forum for the free exchange of ideas on controversial subjects such as corruption, democracy, and particularly Sino-Vietnamese relations. Its editor, Nguyen Hue Chi, has been summoned several times by the police.

Pressure is being placed on editors of unauthorized online newspaper websites like To Quoc (the Homeland) in an attempt to force them to shut down. Teacher Nguyen Thuong Long, To Quoc's associate editor was summoned by police in February 2010. As for Nguyen Thanh Giang, one of this newspaper's cofounders, on one occasion police surrounded his house.

There has been limited access to Facebook since November 2009. Blocking has occurred on occasion, but is not yet permanent. According to the Associated Press, a technician from Vietnam Data Corp. had confirmed in November 2009 that the government had ordered Internet service providers to block the social network. Some enforced the order, while others were less zealous. This measure was implemented when Facebook was being used by pro-democracy groups to denounce arrests of activists like Nguyen Tien Trung. But Web surfers are still using Facebook – they have simply decided to use proxy servers more often.

In 2008, the regime had announced its desire to require foreign companies to collaborate, mainly on blog platforms. Some Web users who were worried about their personal data migrated from Yahoo! 360plus to platforms like WordPress, Blogspot and Multiply, after the U.S. company decided to transfer its servers from Singapore to Vietnam.

## MASSIVE ARRESTS AND CONVICTIONS

Vietnam is the world's second biggest prison for netizens: it now has seventeen of them behind bars. The government shows zero tolerance toward websites and netizens thought to be jeopardizing the government's stability. Most of them are prosecuted – and convicted – for "subversion" or "attempting to overthrow the people's government." They invoke Articles 79 and 88 of the Penal Code.

The latest wave of crackdowns began in September 2009, with the arrest of nine dissidents in Hanoi and Hai Phong. They are paying the price for the "internal cleanup" now underway in anticipation of the next Communist Party Congress. Some very harsh prison sentences have been meted out to pro-democracy activists who appealed for multipartism on the Internet. The authorities are promoting the theory of a foreign-based plot and point out the destabilizing effect of proliferating Western values.

The well-known lawyer Le Cong Dinh was sentenced on January 20, 2010 to a five-year prison term without parole, and pro-democracy activists Nguyen Tien Trung, Le Thang Long and Tran Huynh Duy Thuc received prison sentences of seven years, five years, and sixteen years, respectively, by virtue of Article 79 of the Vietnamese Penal Code. To these sentences were added three years of house arrest (to be served after their release from prison) for all of them except Tran Huynh Duy Thuc, who was sentenced to five years behind bars. The four activists were found guilty of "endangering national security," by "organizing campaigns in collusion with reactionary organizations based abroad," designed to "overthrow the people's government (…) with the help of the Internet." Eight bloggers were also given prison sentences in October 2009.

# VIETNAM

## A wave of brutal crackdowns

At the end of a completely trumped-up trial, writer and human rights activist Tran Khai Thanh Thuy was sentenced to three and one-half years in prison for "assault" even though she was the one assaulted. Her writings on the Internet were very popular in both Viet Nam and abroad.

Journalist and blogger Nguyen Van Dai, better known as Dieu Cay, is still behind bars. Arrested in 2008 a few days before the Olympic torch was due to pass through Ho Chi Minh City, he was sentenced in December 2008 to serve two and one-half years in prison for "tax fraud" – a totally fabricated charge. According to his own son's testimony, Dieu Cay had been closely watched since participating, in early 2008, in demonstrations in Ho Chi Minh City protesting against China's policy in the Paracels and Spratley archipelagos.

Those arrests and convictions are compelling arguments for self-censorship. Blogger Nguyen Ngoc Nhu Quynh, a.k.a. Me Nam, was released in September 2009, but ultimately yielding to police pressure, she decided to close down her blog.

### INTERNATIONAL PRESSURES?

In December 2009, Western donor countries had warned Hanoï against imposing restrictions on the Internet, a step which would be liable to slow down the country's economic development. The Ambassador of the United States – Vietnam's biggest export market – asserted in February 2010 that these convictions of dissidents "were affecting bilateral relations."

Reporters Without Borders called upon the European Union to suspend any dialog with Vietnam on the subject of human rights as long as its netizens and jailed journalists remain in custody.

# AUSTRALIA

## Unpopular censorship

Under the guise of fighting child pornography, the government wants to set up a filtering system never before seen in a democracy. The State of South Australia has passed a law prohibiting online anonymity in an electoral context.

### A DRACONIAN FILTERING SYSTEM

After a year of testing conducted by the government in joint cooperation with Australian Internet service providers, Telecommunications Minister Stephen Conroy reaffirmed, on December 15, 2009, that the government plans to call for a vote on a bill that would impose mandatory filtering of what it considers "inappropriate" websites. The decision to block access to a website would not be made by a judge, but by a government agency, the Australian Communications and Media Authority (ACMA). Such a procedure, without a court decision, does not satisfy the requirements of the rule of law: the ACMA classifies content secretly, compiling a website blacklist by means of unilateral and arbitrary administrative decision-making. The filtering would target websites featuring "refused classification" (RC) content, a category already applied to the traditional media, and would therefore apply to content completely unrelated to government efforts to combat child pornography, defamation or copyright, thus creating an obvious potential for overblocking. Subjects such as aborigines, abortion, anorexia, or laws governing the sale of marijuana would all risk being filtered, as would media reports or medically related information on these subjects. Moreover, although the government has announced that filtering would be 100% effective – a claim highly disputed by experts – the Wikileaks website has revealed the blacklist of filtered sites that had nothing reprehensible in their content, such as YouTube links, poker games, gay networks, Wikipedia pages, Christian sites, etc.

### AN UNPOPULAR BILL

Even though a true national debate on the subject is needed, Stephen Conroy has made such a discussion very problematic by branding his critics as child pornography advocates. A poll of 20,000 Australians conducted by Fairfax Media in December 2009 showed that 96% of them are strongly opposed to this bill. The U.S. company Google has also voiced strong reservations, explaining that this filtering system is "heavy handed and can raise genuine questions about restrictions on access to information." On January 28 and 29, hundreds of Australian Internet websites participated in a national "Internet Blackout" day to oppose this measure.

The announcement of this bill's approaching introduction came soon after the current administration terminated the program launched by the previous government, which procured free filtering systems for Australian families.

In fact, child pornography content is already banned by the Broadcasting Services Act of 2000. The Australian Broadcasting Authority is empowered to require that access providers of the sites concerned to block access to them.

Anti-terrorist legislation is already leading to serious breaches of private e-mail confidentiality. Since 2001, the ACMA is lawfully entitled to intercept any suspicious e-mail message and conduct investigations without prior judicial authorization.

# AUSTRALIA

Unpopular censorship

## ONLINE ANONYMITY IS THREATENED IN THE STATE OF SOUTHERN AUSTRALIA

At the federal level, Australian law guarantees Internet users the right to post anonymous comments, but this is not necessarily the case at the local level. By virtue of new amendments to the State of Southern Australia's electoral law, any comments posted on news sites discussing the local elections to be held on March 20, 2010 must be signed by their author's real name, or the latter may have to pay a fine ranging from AUD 1,250 to 5,000 (USD 1,114 to 4,456). These websites are required to retain, for a period of six months, all information that would permit an Internet user who has written any statement on the site to be identified.

# Bahrain

## Internet filtering: full speed ahead

Bahrain is experiencing one of the region's highest Internet penetration rates. The democratization process has been losing momentum, which has had a negative impact on freedom of expression on the Web. The authorities have adopted the course of a massive filtering campaign, but the country's netizens are proving to be inventive when it comes to circumventing censorship and are mobilizing to defend their rights.

### REINFORCED FILTERING SYSTEMS

The authorities' technological innovation efforts go hand-in-hand with a need to tighten their control of the Web. A rigorous filtering policy is being enforced on the Internet that targets political and religious content considered to be obscene or which casts doubt on the dignity of the royal family. The blocked websites include opposition sites, sites deemed anti-Islamic, discussion forums on taboo subjects, and news sites.

Since 2009, the new Minister of Culture and Information, Sheikha Mai Bint Mohammed Al-Khalifa, a member of the royal family, launched a "anti-pornography campaign" that led to the closing of 1,040 websites. Some of them, however, had nothing whatsoever to do with the subject. The blocking of the Arab Network for Human Rights Information (ANHRI) website, and that of the Bahrain Center for Human Rights, reveals the government's intention to attack websites critical of its policies, the royal family, or even the Parliament. In fact, Google Earth has been rendered inaccessible so that the Bahrainis could not learn the places in which the royal family resides. Certain pages of YouTube, Wikipedia and Facebook have also been banned as a result of this campaign. A precedent: the Twitter account of a foreign national critical of the regime was blocked in early January.

### HIGHLY RESOURCEFUL NETIZENS REMAIN UNDER SURVEILLANCE

The use of proxy servers is very common. Close to 200 Bahraini bloggers frequently voice their opinions on the Web, but they usually prefer to remain anonymous. The authorities regularly monitor Internet websites and the use of censorship circumvention tools. They do not hesitate to pursue or harass "irritating" journalists and bloggers.

The country's cyber cafés are subject to increasing surveillance. Their control is coordinated by a commission consisting of members from four ministries, which ensures strict compliance with the rules concerning non-admittance of minors and computer station visibility.

### PROHIBITIVE LAWS AND DECREES

Internet laws are particularly harsh. The Internet is regulated by the Telecommunications Regulatory Authority, which was established by the Telecommunications Law No. 47 of 2002. Its scope of application was extended to online media. A 2008 amendment eliminated advance censorship and prison terms for reporters, but journalists and Internet users can still be prosecuted by virtue of the anti-terrorist law or the penal code.

Two decrees specifically addressing the Internet were adopted in 2009. The first allows websites to be shut down without a court ruling, merely upon a decision of the Minister of Culture. The second requires the growing number of Internet service providers – of which there are now about 20 – to block websites featuring pornographic material or likely to incite users to violence or racial hatred.

# Bahrain

## Internet filtering: full speed ahead

In 2007, the Ministry of Information's Printing and Publications Department ordered the registration of all Internet websites hosted in the country or abroad featuring information about the kingdom's business, arts, religion, politics, etc. This decision met with significant opposition from a large number of Internet website owners. The latter tacitly decided not to register their sites, thereby commiting an act of civil disobedience via the Web. They regarded the government's requirement as an assault on freedom of expression under the pretext of protecting state security. The regime then rescinded that reversed its position, and registration became optional.

# Belarus

## Takeover of the Internet – the last bastion of freedom – on the eve of elections

The government is planning to arm itself with every possible weapon to ensure tight control of the Internet through the latest legal provisions. After locking down the traditional media, the regime is ramping up its Internet offensive to intimidate members of the civil society who have found refuge within its portals.

### A NEW LIBERTICIDAL DECREE

On February 1, 2010, President Lukashenko signed a Presidential Decree on "Measures to Improve the Use of the National Segment of the Internet Network," which provides for a strong censorship overseen by the presidency. The decree requires that Internet service providers (ISPs) identify and register all Internet access media (computers, telephones, etc.). Cyber café customers will need to identify themselves, and each connection will be recorded and maintained for one year. The same rule applies to shared connection users (i.e., co-owners). Finally, the Decree provides for the creation of an "Analysis Center" that will report to the presidency and be responsible for content surveillance prior to any dissemination over the Internet. This Center will assign domain names and be empowered to order ISPs to close a website. The latter will then have 24 hours to comply. Sites can also be shut down at an ordinary citizen's request, thereby introducing a form of online denunciation. The thirty-odd existing ISPs must use the bandwidth provided by Belpak, an affiliate of Beltelekom that occupies a monopoly position, thus facilitating control and surveillance.

### MORE-THAN-DUBIOUS INTENTIONS DENOUNCED BY THE INTERNATIONAL COMMUNITY

The President of Belarus tries to appear reassuring: every individual will be free to do whatever he wants on the Internet: The purpose of the Decree is to "protect the rights of Belarussian citizens, the society and the state in the field of information," to defend morality and intellectual property, and to encourage further growth of the Internet for economic purposes. Only it is difficult to believe someone who, several months ago, had announced his intention to "eliminate anarchy on the Internet" while referring to the Chinese model. No one has been duped: his real aim is to prevent the opposition from expressing their views on the Internet just before the 2011 presidential elections. The Decree is slated to enter into force in July 2010.

The European Union has chosen to take a tougher stand toward the "last European dictatorship" by qualifying this Decree as "a step in the wrong direction." The EU and the OSCE are currently reviewing the text to determine whether or not it is compatible with the commitments that Belarus has made with those two bodies.

### A VIBRANT ONLINE CIVIL SOCIETY, DESPITE THE CRACKDOWN

Nearly three million Belarussians actively surf the Web. Dissidents, independent journalists and the civil society as a whole have found the Internet to be a space for discussion and exchanges of opinion that no longer exists in the traditional media. Dozens of cyber cafés in the capital, Minsk, as well as in the rest of the country, are their main access points. Since a decree issued in 2007, they have been subject to a form of surveillance by the authorities.

Belarussian netizens have already paid the price of repression. Andrei Klimau, the first opposition activist to be prosecuted after posting an article on the Internet, was given a two-year prison term in August 2007 for "inciting the overthrow of the regime." He was released in February 2008. Cyber attacks against independent sites like Charter 97 – the country's most frequently visited opposition website – or the

# Belarus

## Takeover of the Internet – the last bastion of freedom – on the eve of elections

Radio Free Europe / Radio Liberty website, are common, as are threats against their journalists, or blockings during major political events and demonstrations. The anew Press Law of August 2008 established control over online publications.

The Belarus online community mobilizes quickly, and its activism is echoed within the society. In protest against the elimination of free public transport for the elderly, indignant Internet users and bloggers asked their fellow countrymen to hand out bus tokens to senior citizens. Several hundred people pitched in, and the initiative was filmed and posted on the Internet – an unmistakable way of defying the authorities, similar to what happened on "Democracy Day," when citizens blackened one side of the token to affirm their allegiance to democracy.

# ERITREA

## Cut off from the world

A brutal dictatorship cut off from the external world and digital universe, trying to keep its population away from the Web by resorting to a variety of tactics such as technical barriers or attempts to intimidate users. In instances of social unrest, it does not hesitate to block Internet access.

### STRICTLY CONTROLLED INTERNET GROWTH

This country, which is governed with an iron fist by an uncompromising dictator, President Issaias Afeworki, is politically and virtually cut off from the rest of the world. Its independent press was wiped off the map in 2001. The state-controlled media do little more than relay the regime's ultra-nationalist ideology. The Internet is no exception: the two official websites, www.Shabait.com and www.Shaebia.com, are respectively owned by the Ministry of Information and the sole party, the People's Front for Democracy and Justice (PFDJ), disseminate only government propaganda.

The regime has proven reluctant to accept Internet growth, fearing the Web's potential for disseminating independent information. The population might benefit from too broad an access to the external world and to foreign-based opposition. In this last African country to connect to the Net, the penetration rate hovers around 3%. In other words, virtually all of the population is excluded from the digital era. The government has chosen not to increase bandwidth speed – a major technical barrier to connection.

In the last few years, the government has been waging in the traditional media – over which it has total control – an anti-Internet smear campaign. The Minister of Information has asked his henchmen to participate in television programs in which they could accuse the Internet of being devoted to pornography and to media wars, challenging the country's cultural values, and creating security problems.

### SURVEILLANCE, BLOCKING AND CUTTING OFF ACCESS

The country's four service providers have obtained a licence from the Ministry of Information. They all must use the infrastructures of EriTel, which rents them its bandwidth and works in direct cooperation with the Ministries of Information and National Development. This has made network surveillance an easy task. When the regime feels threatened in periods of social unrest or during an international event that concerns it, the EriTel telecommunications firm, which owns the network's infrastructure, does not hesitate – when so ordered by Eritrean authorities – to cut off all connections to the Internet.

Although the government has not set up an automatic Internet filtering system, it nonetheless was not reluctant to order the blocking of several diaspora websites critical of the government. Access to these sites is blocked by two Internet service providers, Erson and Ewan, as are pornographic websites and even YouTube. The latter would require too much bandwidth, and the two ISPs would prefer to allocate it more efficiently and not have to argue with the government. Skype would be accessible, however. Sometimes surveillance and self-censorship suffice. The two other Internet service providers, EriTel and Tifanus, do not block opposition websites, since they know that the great majority of Eritrean surfers would never dare to openly consult them for fear of being arrested and imprisoned.

The few netizens and webmasters who are courageous enough to create or collaborate on developing an independent website are being threatened and closely monitored.

# Eritrea

## Cut off from the world

The forty-some Internet cafés, most of which are operating in Asmara, the capital, and in two or three other Eritrean cities, constitute the main access source for the Net, inasmuch as household use is very expensive and practically non-existent. These cafés are watched very closely, particularly during periods of social unrest, or when compromising news about the regime is circulating abroad. Such was notably the case when revelations were posted on diaspora websites about the President having a bank account in China.

# MALAYSIA

## Beware of the new media

For the time-being, there is no network censorship on the Malaysian agenda, but bloggers and online journalists are being harassed and the authorities are producing a proliferation of statements about their distrust of the new media.

### CREDIBILITY : THE NEW MEDIA'S PREROGATIVE

News websites and blogs have flourished as an alternative to the state-controlled traditional media. The new media have acquired genuine credibility and, keeping pace with their growth, a high-quality online journalism broaching important subjects has emerged on such sites as NutGraph, Malaysian Insider and Malaysiakini and on blogs like Articulations, Zorro Unmasked, People's Parliament and Malaysia Today.

The opposition was quick to permeate the new media, but the government and ruling party also followed the movement. The Barisan Nasional Party has organized a special unit responsible for disseminating ideas on the Net. The Internet created new opportunities for all political actors, and not just for parties. By allowing them to reach a heterogeneous audience, it is challenging traditional censorship barriers. However, the authorities have been producing an increasing number of statements calling into question the new media's legitimacy.

### HARASSED BLOGGERS AND WEBSITES

The regime is, indeed, showing a certain degree of exasperation toward bloggers and independent websites. It sometimes yields to the temptation of prosecuting them by using the legal weapons at its disposal. Some twenty-odd laws can be deployed to censor the media and the Internet. Most often enforced against netizens is the Internal Security Act (ISA), which allows them to keep an individual in custody for two years without a trial, the 1984 Press Law and publications, the Malaysian Communication and Multimedia Act of 1998, and the Sedition Act. The latter penalizes any expression likely to incite hatred or disaffection with regard to Malaysian authorities or between "races" and social classes, changing the established order, or challenging any sovereign right or privilege. Any person found guilty faces a potential prison term of up to five years and a fine of MYR 5,000 (about USD 1,475).

The Malaysiakini site is being investigated by the Malaysian Communications and Multimedia Commission for posting videos that authorities deemed shocking, but which, according to the site's chief editor, merely constituted coverage of events of general public interest, in this case demonstrations. Malaysiakini is extremely popular, with 37 million pages seen per month by 1.6 million single visitors.

Blogger Raja Petra Kamaruddin, better known by his acronym RPK, who is the director of the news site Malaysia Today, is the victim of a genuine judicial harassment campaign. He is the pet peeve of the authorities, whose acts of corruption he has denounced numerous times. He stands accused of sedition after having implied that the Prime Minister and his wife might be involved in the murder of a Mongolian interpreter within the scope of an explosive case concerning politics and arms sales. The authorities are now threatening to withdraw his Malaysian citizenship and to issue an international arrest warrant against him. In November 2009, the court had "suspended" his trial by granting him a discharge because he could not be located. But the accusations remain intact and he can be arrested again at any time.

Another blogger, Khairul Nizam Abdul Ghani, was accused of insulting the monarchy and should be tried by the end of March 2010. This freelance computer technician had posted on his blog, www.adukataruna.blogspot.com, critical comments about Sultan Iskandar Ismail of the state of Johor, who

# MALAYSIA



died this past January. He could be given a sentence of up to one year and pay a fine, even though he apologized and withdrew the incriminating article from his blog.

In March 2009, eight Internet users were prosecuted for insulting the Sultan of the state of Perak, which was undergoing a political crisis. One of them, Internet user Azrin Mohd Zain, was sentenced to pay a fine of MYR 10,000 (about USD 2,950) by virtue of the Malaysian Communication and Multimedia Act of 1998. The seven others are awaiting trial.

Lawyer P. Uthayakumar, and a member of the Hindu Rights Action Force (HRAF), detained since December 2007 in the name of the Internal Security Act (ISA), was released in May 2009. The authorities accused him of having published on his Internet website (http://www.policewatchmalaysia.com), a letter to the British Prime Minister, Gordon Brown, asking him to support the adoption of a UN Security Council resolution condemning the "atrocities and persecutions" perpetrated by the Malaysian government against the Hindu minority and to refer the case for trial to the International Criminal Court.

## NO CENSORSHIP ON THE AGENDA?

The Malaysian Minister of Culture and Communication's proposal to install a Web filtering software system was rejected by the government in August 2009 after demonstrations protesting against this initiative. The Minister considered using, for example, the "Green Dam filtering software program" used by the Chinese, under the pretext that it was necessary to "maintain racial harmony in a multicultural nation."

In the last few months, the authorities have reiterated the promise made in 1996, during the launching of the Multimedia Super Corridor – a special economic and technological zone – not to censor the Internet. Notably in a letter sent to Reporters Without Borders in June 2009, they further explained that censorship was not on the table. But at the same time they warned citizens about engaging in "immoral online activities," they also advised them to allow themselves to be "guided by their cultural and moral values" in cyberspace.

# Russia

## Attempts at censorship ?

After the takeover by the Kremlin of the audiovisual media early in the Putin era, the Internet became the freest space for discussion and information-sharing in Russia. Yet its dependence is threatened by blogger arrests and prosecutions, and the blocking of independent websites labeled as "extremist." The Web has also become a first-rate sphere of activity for government propaganda and could become a political control mechanism.

Web access has spread extensively in the last few years, and with government support. The project to create a Russian Silicon Valley was launched by President Dimitri Medvedev's decree of December 31, 2009. This plan unveils the country's technological ambitions.

The Internet is regulated by the Federal Service for Communications Supervision, whose Director is appointed by the Prime Minister. The government secured the means to carry out Web surveillance from the very start. In 2000, all Internet service providers were required to install "Sorm-2" software, "SORM" being the Russian acronym for "System for Operative Investigative Activities." It enables the police and Federal Security Service (FSB) to have access to user surfing activity and email traffic. A 2007 law authorized the government to intercept Web data without a prior court order. Social networks such as Vkontakte and the blog platform Livejournal were bought out by oligarchs with close ties to the regime.

### "TROUBLING" WEBSITES BLOCKED, PROSECUTED OR HACKED

The Internet is not subject to an automatic filtering system, but independent sites and those with close ties to the opposition have been rendered inaccessible in the last few months. In 2008, the www.Kompromat.ru website was blocked by several Internet service providers prior to the presidential elections, and later unblocked. In December 2009, Garry Kasparov's websites (www.Kasparov.ru and www.Rusolidarnost.ru) and www.Nazbol.ru, the National Bolshevik Party's website, were blocked for Yota service provider users. Yota denied the allegations, citing technical problems, and the websites were finally unblocked. The management of the Skartel operator, which owns Yota, admitted that this company blocks websites that the Ministry of Justice classifies as "extremist." The list of "extremist" content, issued by the Attorney General, includes nearly 500 terms and is constantly being updated under the watchful eye of the "e-Centers" responsible for eliminating extremism. Article 282 of the Russian Criminal Code defines "extremism" as "xenophobia and incitement to hatred by means of a social group." These are the justifications given for shutting down the www.ingushetiya.ru website, the only news portal in the Ingush language. The website www.ingushetiyaru.org was then created. In the same context, in February 2010, Russian police opened an investigation into the www.Grani.ru portal, a platform for independent journalists and human rights activists. The same treatment was reserved for www.kompromat.ru and The Moscow Post website, which had reported a violent dispute between intoxicated senior police officials.

Often a call from authorities is all it takes to obtain permission to delete content, or to block a website. Aleksandr Ovchinnikov, Director of the Web hosting company Masterhost, admitted that this practice exists.

Cyber-attacks are commonplace. In January 2010, the www.Ingushetiyaru.org website was hacked just after it posted the last interview granted by Natalia Estemirova, the human rights activist murdered in July 2009. The same thing happened to the website of the Chechen magazine Dosh, just a few days after it was awarded the Reporters Without Borders Press Freedom Prize in December 2009. As for the Novaya Gazeta newspaper's website, it was rendered inaccessible for more than a week at the end of January following a "highly organized and powerful" cyber-attack."

# Russia



## PROPAGANDA AND INTIMIDATIONS

Vladimir Putin stated in January 2010 that "50% of Internet content is pornographic. Why, then, should we bother?" He denied Internet-relayed accusations that the October 2010 regional election results were falsified. Nonetheless, the government is omnipresent on the Web, and makes optimal use of the terrain. One of the star bloggers of RuNet – the Russian version of the Internet – is none other than President Dmitri Medvedev. In March 2008, local Ingush authorities created an Internet site with an address almost identical to that of the news site www.Ingushetiyaru.org in order to present a different version of the news that it was delivering.

Government supporters are quick to react to criticisms posted online, "drowning" the latter in a sea of positive comments. The most virulent among them formed a group called the "Brigade," of which some of them are paid members. They notably infiltrate discussion forums and sometimes discuss matters very harshly, not even hesitating to use insults and threats. In June 2009, economist Evgeni Gontmakher disclosed in The Moscow Times that he had been the target of "massive attacks" by bloggers paid by the government, after he criticized Vladislav Surkov, the First Deputy Chief of the Presidential Staff. In his opinion, "The modern Russian propaganda machine permeates nearly every major media outlet and even extends to the blogosphere."

## BLOGGERS INCREASINGLY PERSECUTED

In July 2008, blogger Savva Terentyev was charged with "belittling the human dignity of a social group" (in this instance, the police) and given a one-year probation. Irek Murtazin got a 21-month prison term for "defamation and incitement to hatred" for having posted a message implying that Mintimer Shaimiev, who was Tatarstan's chief executive at the time, had died. The case was appealed to the Russian Supreme Court. Blogger Dimitri Soloviev was investigated for having "inciting hatred against the police and the FSB." Charges were dropped in January 2010 after two years of legal proceedings. On September 1, 2009, the Ministry of the Interior of the Republic of Khakassia (in southwest Siberia) dropped the charges against Mikhail Afanasyev, editor of the Novy Focus website, who was accused of spreading "false rumors." He had published news about the fatal explosion of a turbine at the Sayano-Shushenskaya power plant, which led to the death of 73 employees, and relayed criticisms of the manner in which the authorities had handled this tragedy.

In December 2009, blogger Ivan Peregorodiev was arrested and indicted for "disseminating false information related to an act of terrorism" because he had discussed rumors on his blog, according to which victims of the A (H1N1) virus had actually died of the plague. Blogger Dmitri Kirilin, on the other hand, was charged with calling for "the overthrow of the existing political order, and making disrespectful comments about incumbent officials, notably Prime Minister Vladimir Putin.

Aleksey Dymovsky, a police officer who denounced police corruption in a video message distributed over the Internet, became the subject of a criminal investigation in December 2009 for "abuse of power and fraud," according to the public prosecutor's office. He faces up to six years in prison.
Vadim Charushev – The creator of Vkontakte, one of the country's most popular social networks – was confined against his will in a psychiatric hospital in March 2009.

# Russia



## Online journalist killed

Magomed Yevloyev, one of the creators and the owner of the Ingush news website, http://ingushetiyaru.org, was killed in August 2008 while detained by the Ministry of the Interior's security agents. The journalist had been arrested at the Nazran airport shortly after landing there. The airplane he had flown was also carrying the then-President of the Republic of Ingushetia, Murat Zyazikov. A few hours later, Magomed Yevloyev, who had been shot in the head, was admitted to the hospital where he later died on the operating table. This murder remains unpunished.

## A dynamic blogosphere

In November 2009, bloggers Oleg Kozyrev and Viktor Korb launched a "bloggers' union" to protect netizens' rights and freedoms. They have also conducted campaigns on behalf of imprisoned or prosecuted bloggers.

Sometimes the Internet can fill the void left by traditional media outlets. In 2008, a report on the demolition of historic Moscow buildings whose residents were displaced to make room for new offices and business centers was partially censored by the authorities, and confidentially broadcast on the NTV channel. The video, on the other hand, was posted on RuTube (a YouTube clone), where it became a huge success, receiving over 200,000 hits in just a few days.

The Internet is also a space for political mobilization. Roman Dobrokhotov, leader of the young Russian democrats movement "My" ("We"), an opposition party, stated that all of his activities are performed over the Internet via a Google group. It is easier to mobilize people online than it is in the street.

The Internet has become a space in which people can denounce the corruption of Russian officials. Marina Litvinovitch, one of the leaders of the Civic United Front (CUF), an opposition party, posted on her blog an article objecting to the impunity enjoyed by a civil servant's daughter in the Irkutsk region. She had caused a fatal car accident in December 2009, but had been treated as if she were only a witness in the case. Marina Litvinovitch launched an appeal to other bloggers, asking them to distribute that information by creating a link to her article or by reposting it, which many Internet users agreed to do. This initiative had the merit of making the public aware of this tragedy, and the blogger believes that the courts will no longer be able to avoid taking this matter seriously.

For the moment, the impact of these online mobilizations, blogs and new media on Russian society is still relatively limited. The authorities' attitude in the months to come will determine if the acts of censorship or intimidation and arrests are, or are not, indicative of a deliberate attempt to gain complete control of the new media. The introduction of Internet censorship in Russia would be that much more harmful in that it would spread throughout the region, with negative consequences on the right to inform and be informed in the Caucasus as well as in Central Asia, where censored netizens sometimes have access to the Russian Internet.

# South Korea

## The most "connected" country in the world has not been spared by Net surveillance

Close to 90% of South Korean households have Web access via the world's best network infrastructure. However, concerned about maintaining order in a period of social unrest, the government has been attempting to strengthen censorship by resorting to excessive means and a liberticidal legislative arsenal that is inducing netizens to practice self-censorship – all that in the name of the fight against dissemination of "false information."

The new media are having a considerable impact on South Korean society, culture, and policies. Some highly independent bloggers are being read daily by hundreds of thousands of people, and discussion forums are buzzing with activity. The e-zine www.ohmynews.com publishes articles written by ordinary netizens. It is known to have influenced the outcome of elections and has been under scrutiny by the conservative government, which is trying to muffle its criticisms.

### A NET TAKEOVER IN REACTION TO SOCIAL UNREST AND CRITICISM OF THE AUTHORITIES

In June 2008, President Lee Myung-bak clearly expressed his distrust of the Web: "The Internet should be a space of trust. Otherwise, the force of the Internet could turn out to be venomous rather than beneficial." The government was attempting to cope at the time with a wave of demonstrations over the scandal of the beef imported from the United States – demonstrations provoked, according to the authorities, by Internet users via the well-known Agora discussion forum, which has become the government's pet peeve.

The authorities are using the criminalization of defamation against their critics and do not hesitate to make examples of them. Since June 2008, a dozen Web surfers have been briefly arrested and interrogated for having posted online comments critical of the government within the context of these demonstrations.

The widely popular blogger Minerva has learned, at his expense, that the government values protecting the financial markets more highly than defending freedom of expression. In 2007, Minerva was arrested for having undermined the foreign exchange markets," as well as the nation's credibility," because of articles he had posted on the discussion forum of Daum – one of the country's biggest Web portals. The government objected to his criticisms of its economic policies and for announcing the fall of the won. Accused of "disseminating false information," the man nicknamed "President of the Economy" since his prediction that Lehman Brothers would collapse, could have faced up to five years' imprisonment and a fine of KRW 50 million fine (USD 42,500). He was acquitted in April 2009, but the public prosecutor lodged an appeal. A case worth following up.

### SELECTIVE FILTERING

South Korea is blocking about forty Internet websites that extol the Pyongyang regime, as well as some online betting sites and sites that promote suicide. As provided under the National Security Law, any individual who publicly supports North Korea can be charged with "anti-statist activity" and can face up to seven years behind bars. This law applies to traditional media as well as online media.

Website blocking is carried out by access providers acting under the order of an administrative authority, the Korea Communications Commission, which is also in charge of Web surveillance.

# South Korea

The most "connected" country in the world has not been spared by Net surveillance

## SEVERAL WORRYING LAWS

Censors have several legal options at their disposal to ensure Internet control. Article 47 of the Telecommunications Code states that it is illegal "to disseminate false news intended to damage the public interest." The penalty for any violation can mean up to five years in prison.

The electoral law was amended in 2004 to prohibit dissemination, via the Internet, of defamatory statements about politicians running for office during an electoral campaign. The country's penal code, notably the provisions against insult and defamation – even for comments that turn to be true – is also used against Web surfers (Article 307).

Article 44-7 of the Act on the Promotion of Information and Communications Network Utilization and Information Protection (the Network Act) prohibits the exchange of electronic information that compromises national security or is considered to be defamatory, even if such content is true.

## COMPROMISED ANONYMITY

Article 44-5 of this same Act requires that Internet users register under their real names and provide their national ID card number when visiting portals with over 100,000 members. On the other hand, only the users' pseudonyms appear online. YouTube has refused to apply this measure. Consequently, since April 2008, YouTube users who identify themselves as based in Korea cannot upload or download their videos on the website.

Since February 2009, one of the country's main portals, Nate, has been requiring surfers to display their real name in order to leave comments online

Despite the government's constant pressure, South Korean netizens are very active and willing to mobilize online via forums and discussion sites. By persisting in following this repressive policy, the government is taking the risk of alienating part of the population, as well as potential investors. Its drastic rules with regard to Web user registration and surveillance are considered by such international websites as YouTube, Facebook and Twitter as a deterrent with regard to their entry into the South Korean market.

# Sri Lanka

## The pretext of war

In the wake of the military victory over the Tamil Tigers and presidential elections held in an environment of propaganda and intimidations, Sri Lanka is re-emerging with a government visibly determined to intensify its control of Internet-based information.

Despite the end of the bloody civil war that has decimated the country for decades, the repression of dissident voices continues, and may well become commonplace.

### Independent news websites blocked a few hours before presidential election results were announced

Even though the blocking had so far been mainly limited to sites sympathetic to the Tamil Tigers, the Lankaenews, Lankanewsweb, Infolanka and Sri Lanka Guardian independent websites were rendered inaccessible on the island by the primary Internet service provider, Sri Lanka Telecom (SLT) on February 26, 2010. The free circulation of information at election time is nonetheless one of the rare guarantees against massive voting fraud. Such censorship has shown the government's unease and attempts at manipulation. The Lankaenews offices were surrounded by police and its director received a death threat at the end of January. The newspaper's website had already been temporarily blocked in July 2009 after covering incidents that occurred in the displaced civilians' camps during the military offensives.

### One online journalist missing and netizens threatened

Political analyst and cartoonist Prageeth Eknaligoda, a journalist for the news site Lankaenews, has been reported missing since the night of January 24. He had told a close friend that he thought he had been followed for several days. When contacted by Reporters Without Borders, one of his colleagues confirmed that he was being threatened because of his political analyses. Just before the elections, he had indicated his preference for the opposition candidate, General Fonseka.

The Sri Lankan journalists recall the traumatizing experience of the TamilNet website, whose director had been abducted and then killed in Colombo in 2005. The site had been subsequently blocked. The murderers are still at large.

### International community watch

This summer, Sri Lanka will be temporarily removed from the list of countries benefiting from the GSP+, a treatment that grants preferential rates within the European Union to certain developing countries practicing sustainable development and good governance. This will be done in expectation of an improvement in the country's human rights situation and, in particular, that of freedom of expression.

The weekly Sunday Times, in its February 14 edition, revealed that Chinese IT experts will be visiting Sri Lanka in March 2010 to advise authorities on how to set up an Internet censorship system aimed at blocking "offensive" websites. Also according to the weekly, the Telecommunications Regulatory Commission will introduce legislation to make registration with the institution mandatory for all websites. Measures will also be taken to impose controls on the Google search engine. On February 17, the news website Lanka News Web, stated that the President had allegedly asked the Chairman of the Regulatory Commission to wait until the general elections were over to set up a Net filtering system. Websites that get more than 200,000 visitors a day will be required to register with the Ministry of Information.

# Sri Lanka

## The pretext of war

However, the Telecommunications Development Program is financed by the World Bank via the Institutional Development Fund (IDF). The World Bank reacted quickly, on February 15, explaining that the grant agreement "has no provision or scope to utilize these funds to implement an Internet censorship program," and went on to say that "the Bank would not approve any such provision."

The April parliamentary elections will represent the next test for freedom of expression in the country. The international community should keep a close watch on the situation in order to ensure that Sri Lanka does not end up taking permanent control of the news media, particularly online.

# Thailand

## The crime of lèse-majesté

Thai authorities strictly control the dissemination of information on the Internet under the pretext of protecting the King and the royal family. This censorship affects thousands of Web pages and has turned into a political tool. A dozen Internet users are currently being prosecuted for the crime of lèse-majesté.

### THE KING: A TABOO TOPIC

It can be dangerous to discuss the King and the royal family in Thailand. Anyone who dares to do so will inevitably find himself accused of "lèse-majesté." Article 112 of the Thai Penal Code provides for jail terms of three to fifteen years for anyone who "defames, insults or threatens the king, the queen, the heir to the throne or the Regent."

The Internet is controlled and monitored by the Thai Ministry of Information and Communications Technology (MICT), which blocks websites deemed to be offensive, particularly those which fall under the "lèse-majesté" charge. However, since this crime constitutes – according to the authorities – an offense against national security, the army as well as the police are involved. In January 2010, the Thai Defense Minister ordered all military units to monitor and contain any "subversive" action against the monarchy; whether taking place online or during political demonstrations.

MICT data shows that 16,944 URLs were blocked in July 2009. Close to 11,000 constituted a threat to national security, 5,872 allegedly contained socially or culturally inappropriate content, and 72 adversely affect the country's economy. Although 71 news sites sympathetic to the so-called "red-shirt" political activists were unblocked in April 2009, certain Internet service providers rendered the Freedom against Censorship in Thailand (FACT) organization's website inaccessible in the country.

YouTube is still blocking or removing videos deemed disrespectful of the King. In August 2007, the Thai government lifted a four month-old ban against accessing the video portal, once it received YouTube's assurance that the clips offending the King would no longer reside on the site.

Moreover, the 2007 Computer Crime Act vests authorities with the power to verify Internet users' personal data without the need for a court order.

Finally, denunciations are encouraged. Some individuals are voluntarily monitoring the media and the Internet to report any "inappropriate" content to the Cultural Surveillance Department. It is thought that close to 1.3 million people have already collaborated voluntarily with the censors. Internet users can report any website believed guilty of a "lèse-majesté" crime. All they need do is dial 1111 – the number of the Prime Minister's cabinet.

### A DOZEN INTERNET USERS CAUGHT IN A VICIOUS JUDICIAL CIRCLE

One netizen is currently behind bars. Blogger Suwicha Thakor was sentenced on April 3, 2009 to ten years in prison for a "lèse-majesté" crime, despite the lack of evidence against him. Neither a politician nor a militant, Suwicha Thakor claims that he never criticized the King. He was arrested in January 2009 by the Department of Special Investigations (DSI) while staying at the home of friends in the country. His computer's IP address showed that his domicile might match the location from which content deemed defamatory to the King and his staff was posted.

# Thailand

## The crime of lèse-majesté

At least a dozen Internet users are being prosecuted for the crime of "lèse majesté," including: Jonathan Head, British BBC correspondent in Southeast Asia, Giles Ji Ungpakorn, Professor of Political Science and two bloggers, Nat Sattayapornpisut and Praya Pichai. As for Tasaparn Rattawongsa, a Thon Buri Hospital doctor, Somchets Ittiworakul, Theeranan Wipuchan, a former UBS Securities Group executive, and Katha Pajajiriyapong, KT ZMICO brokerage house employee, they all charged with having violated Section 14 of the 2007 Computer Crime Act by posting online "false information endangering national security." The Web users had laid the blame for the decline in the Bangkok Stock Exchange on the poor state of health of King Bhumibol Adulyadej, who had been hospitalized since September 2009.

This proliferation of prosecutions is also meant to intimidate other Internet users inclined to criticize the King and induce them to rely on self-censorship. While other netizens have been briefly arrested or interrogated, but it is difficult to quantify their exact number, because many cases are not being publicized for fear of reprisals. A few cases of Thai surfers based in foreign countries, harassed for having mentioned the kingship online, have been brought to Reporters Without Borders' attention.

### CENSORSHIP AS A TOOL FOR POLITICAL CONTROL

King Bhumibol Adulyadej is revered by the Thai population, who consider him to be the guarantor of national unity for a country prone to changes of government. He himself stated on December 5, 2005, on the occasion of his birthday: "In reality I am not above criticism…for if you say the king cannot be criticized, it means the king is not human."

The King's state of health is causing serious concern. The media are practically not mentioning the subject, choosing self-censorship for fear of being accused of "lèse-majesté," but everyone is thinking about it. The Economist magazine was banned in the country in January 2009 following publication of an article criticizing the fact that resorting to talk of "lèse-majesté" allows the country to avoid necessary debate on the King's succession and the Thailand's political future.

Lèse-majesté seems to be an anachronic law, and Thailand is one of the last countries on the globe to enforce it. However, it is more timely than ever in that the government's executive branch uses it as a tool to crack down on political dissent. The various governments – including Vejjajiva's – have been bolstering Internet filtering efforts since the 2006 coup, relying more and more often on accusations of "lèse-majesté" against their critics..

The majority of the population does not contest this law. However, on a global level, the authorities are on the defensive. A "campaign to educate foreigners about the crime of lèse majesté" was launched in January 2009. The international community must keep exerting pressure on a country that wants to maintain the positive image that the tourism industry is cultivating.

In January 2010, the Thai government announced that it intended to set up a committee to examine accusations of "lèse-majesté" in order to prevent "abuses." If these efforts do not produce improvements in the near future, Thailand is in grave danger of toppling from the "Countries under surveillance" category into that of "Enemies of the Internet."

# Turkey

## Censorship in the name of the Founder of the Republic

Ataturk, the Army, the issue of minorities (Kurds, Armenians, etc.) and the Nation's dignity are all taboo subjects in Turkey. Several thousand websites are blocked, including the well-known YouTube, raising protests within the country. Bloggers and surfers who express their views freely on such topics are running the risk of reprisals.

### THOUSANDS OF BLOCKED WEBSITES

Currently, some 3,700 sites are allegedly blocked in Turkey, some for "arbitrary and political reasons," according to the Organization for Security and Cooperation in Europe (OSCE) (www.osce.org). Among them are many foreign websites, news sites about the Kurd minority, and EU gay websites, thereby muzzling any opportunity for debate.

The most widely publicized example of online censorship is undoubtedly the blocking of YouTube, which has once again been rendered inaccessible since May 2008 because of the dissemination of videos considered disrespectful toward the Founder of the Republic and the Turkish nation, despite the fact that YouTube had withdrawn some of these videos. From March 2007 to June 2008, several courts had issued seventeen orders to block the website. A related lawsuit on this matter was lodged with the European Court of Human Rights (ECHR) by the Society for Internet Technology (INETD), based in Ankara, for violating freedom of expression. In September 2008, MySpace.com was also blocked for "violating intellectual property rights," then unblocked in October 2009.

### A LEGISLATION-BACKED CENSORSHIP?

Law 5651 on the prevention of Crime Committed in the Information Technology Domain permits this mass blocking. The OSCE thus urged Turkey to implement reforms to demonstrate its commitment to freedom of expression. Article 8 of this Law authorizes blocking the access to certain websites if there is even a "adequate suspicion" that any of the following eight offenses are being committed: encouraging suicide; sexual exploitation or abuse of children, facilitating the use of narcotics; supply of unhealthy substances; obscenity; online betting, or anti-Ataturk crimes. It is this latter provision that creates problems. Websites hosted in Turkey are often shut down, and those hosted abroad are filtered and blocked by Internet service providers. Denunciations are encouraged: there is a hotline for reporting prohibited online content and illegal activities. Over 80,000 calls were recorded in May 2009, as opposed to 25,000 in October 2008.

Site-blocking is carried out by court order or by administrative order of the Supreme Council for Telecommunications and IT. Such administrative decision is arbitrary and precludes the possibility of a fair trial. This entity, which was created in 2005 in the aim of centralizing surveillance and the interception of communications (including on the Internet), has not issued its blacklist of blocked websites since May 2009 – indicating a troubling lack of transparency.

According to the OSCE, over 80% of the blockings tallied in May 2009 were the result of administrative orders. The majority of them were made on the grounds of "obscenity" and the "sexual exploitation of children." However, in addition to these site blockings, 158 examples of "illegal" Ataturk-related content have allegedly been removed at the request of the Telecommunications Presidency. By virtue of Article 9 of Law 5651, individuals who feel that their rights have been violated may request that the site or its host remove the incriminated content.

# Turkey

## Censorship in the name of the Founder of the Republic

Most importantly, nearly 200 court decisions were recorded in 2009 ordering website blockings related to matters beyond the scope of Law 5651, therefore making the blockings unjustified. For example, the independent news site www.istanbul.indymedia.org was suspended for "insulting Turkish identity" – a crime that falls within the jurisdiction of the Turkish Penal Code (TPC) and not Law 5651. Other counts of indictment used were "dissemination of terrorist propaganda" (by virtue of the Anti-Terrorist Law), and "incitement to hatred" by virtue of Article 216 of the Turkish Penal Code. Some websites were also rendered inaccessible as the result of libel suits.

Moreover, Turkish law does not oblige the authorities to inform those charged of the rulings rendered, and the sites often find out for themselves that they are blocked. Rather than to legally contest the blocking decisions, which has rarely occurred, some sites change their domain names to circumvent the censorship. For example, the website of the daily Gündem has been blocked since March 2008, but their new site, www.gundem-online.net, remains accessible.

Most importantly, censorship can be circumvented via proxy servers or VPNs, and blocked websites are often accessible on Blackberrys and iPhones.

### NETIZENS "HARASSED" FOR EXPRESSING THEIR OPINIONS

Prison terms were pronounced in absentia on March 2, 2010 against three online journalists from Adiyaman Province (in southeastern Turkey). Journalist Haci Bogatekin, chief editor of the www.gergerfirat.net news site, was sentenced to five years in prison, and denied his civil rights for insulting and defaming Sadullah Ovacikli, a local prosecutor. His son, Özgür Bogatekin, owner of the online news site, www.gergerfirat.net, received a one year and two-month prison term on the grounds that he intervened when two policemen were assaulting someone in the street. Cumali Badur, an editor of the same news site, www.gergerim.com, was fined EUR 1500 (about USD 2,050). A column posted on the latter website in January 2008 had mentioned that Prosecutor Ovacikli had ties with Fethullah Gülen, a religious community leader. The three journalists have appealed their cases and are not currently behind bars.

Baris Yarkadas, an online journalist working for the newspaper Gercek Gündem ("Real Agenda") may be facing a prison term of 5 years and 4 months by virtue of Article 299, paragraph 2, of the Turkish Penal Code. His trial, which began on March 3, 2010, will reconvene on June 9. The Presidential administration has charged him with "insulting the President of the Republic," and with not withdrawing from his newspaper's website a critical article posted by an Internet user. The journalist is facing multiple lawsuits. On June 21, 2010, he must also appear before the same court, this time on charges brought by Dr. Nur Birgen, Chair of the Institute for Forensic Medicine's Third Specialization Board, who accused him of "personally insulting" her by reporting in an article allegations that human rights NGOs had made against her.

After ten months of detention pending trial, Aylin Duruoglu, Director of the Vatan website (www.gazetevatan.com) and Mehmet Yesiltepe, an employee working for the magazine Devrimci Hareket ("revolutionary movement") were granted a conditional release. They remain charged with being members of the armed military group "Revolutionary Headquarters" ("Devrimci Karargah"), an accusation that Aylin Duruoglu firmly denies.

Another form of online harassment involves the Internet website of the weekly founded by Hrant Dink, the Turkish-Armenian journalist fatally shot in 2007, Agos, which was hacked in February 2010 by individuals who admired the killer, even as setbacks and legal complications pile up during the trial of the alleged perpetrators of this crime.

# Turkey

## Censorship in the name of the Founder of the Republic

Internet censorship is truly raising concern in Turkish society. The blogosphere has been protesting against the blocking of YouTube, and the mobilization campaign was relayed by the traditional media after an article on the subject was published in The Wall Street Journal. Virulent editorials have appeared in Turkish newspapers. One of them, printed in the Milliyet daily of February 17, 2010, was headlined: "Let's take away Istanbul's status as the European Capital of Culture" – a status granted by the European Union in 2010 in order to recognize Turkey's cultural development.

# United Arab Emirates

## A "two-facetted country": technological leader and zealous Internet censor

Despite the fact that the United Arab Emirates are experiencing the highest penetration rate in the Arab world, the authorities have implemented an extensive system to filter sensitive subjects, backed by repressive laws. Netizens are increasingly resorting to proxy servers to access thousands of banned websites.

### PROMOTING INTERNET ACCESS

The United Arab Emirates are playing a technological leadership role in the Arab world, thanks mainly to Dubai Media City and Dubai Internet City – tax-free zones in which major companies in the media and IT sector have set up their operations. In March 2009, the authorities decided to use the country's domain name in Arabic in order to foster the use of the language on the Internet. They plan to invest several billion dollars to expand Internet infrastructures and access, particularly in government agencies and schools.

Over 50% of the Emirates' population are connected to the Internet. An extremely active community of netizens has developed. Bloggers are broaching topics of general interest, but they are often pressured to use self-censorship. Some of them, however, do tackle controversial subjects, only to face the consequences. The owner of the www.majan.net forum and one of his colleagues spent several weeks behind bars in late 2007 for covering a corruption case in the medical community. The public prosecutor dropped the defamation charges in 2008.

### PERVASIVE FILTERING POLICY

Although the authorities are in favor of letting their citizens have access to the Net, they insist on "guiding" them in the process. Under the pretext of fighting online pornography, several thousand Internet sites totally unrelated to this subject have vanished from the Web (blocked sites such as http://www.emarati.katib.org/node/52, for example). Taboo subjects include: alternative political views, non-orthodox opinions about Islam, and criticisms of the social situation, especially of the royal family. The economy is still a very sensitive topic. Mujarad Ensan's blog (www.mujarad-ensan.maktooblog.com) was blocked after he mentioned what repercussions the royal economic crisis has had on the Kingdom. Finally, sites that provide content considered "obscene," or censorship circumvention tools, are not accessible either. Censors also target any site denouncing human rights violations in the country. The UAE Torture website (www.uaetorture.com), for example, is blocked.

Authorities have allegedly blocked five hundred keywords. The decision to render websites inaccessible is made by the Telecommunications Regulatory Authority (TRA) in cooperation with the Minister of Communications and Internet Technology, and implemented by the country's two Internet access providers, Etisalat and Du. They use the SmartFilter software program produced by Secure Computing, which was bought out in 2008 by the American firm, McAfee.

Censorship affecting social networks, participating websites and blog platforms is not uniformly applied. Forums are filtered according to the topics discussed by surfers. Only a few pages or posts are made unavailable. The very popular www.uaehewar.net forum was recently blocked in its entirety. YouTube is partially blocked: a campaign launched in 2009 by Dubai's Chief of Police, to block all access to the site, failed. Currently, the country has several hundred Internet cafés. Yet they are not the primary point of access for the country's citizens, who consult the Web from their homes or workplaces. New rules require that users present an ID card and register their personal data, but they are allegedly not being enforced.

# United Arab Emirates

## A "two-facetted country": technological leader and zealous Internet censor

Cell phones are also being filtered. The latest victim is the Blackberry, whose Internet access has been filtered since December 2009. Authorities tried to install spyware on smartphones in July 2009, but users raised such an uproar that they finally abandoned the plan.

### CYBER-LAWS AND CYBER-POLICE

Since December 2008, UAE cyber-police have been in charge of monitoring the Web and keeping an eye on its users. According to the authorities, they processed over 200 cases in 2009, mainly related to cyber-crime and hacking.

Intensified surveillance has been coupled with liberticidal laws. By virtue of Article 20 of the 2006 law against cyber-criminality (the Computer Crime Act), an Internet user may be imprisoned for "opposing Islam," "insulting any religion recognized by the state," or "violating family values and principles."

Another victim of the censors, the website www.Hetta.com, has been targeted by judicial harassment. Its chief editor, Ahmed Mohammed bin Gharib, was sentenced to a fine of AED 20,000 (about USD 5,400) for "defaming," "insulting," and "humiliating" the Abu Dhabi Media Company, a state-controlled media outlet for publishing an article in May 2009 in which journalists denounced the company's "administrative corruption" and "embezzlement" practices. The appeal hearing upheld this penalty on January 13. Ahmed Mohammed bin Gharib lodged an appeal with the Court of Cassation..

### INTENSIFYING CYBER CENSORSHIP AND CIRCUMVENTION EFFORTS

Despite the fact that, based upon a poll published by the newspaper Khaleej, 95.5% of the respondents opposed the current filtering system, the latter has been intensifying in the last few months according to the OpenNet Initiative. Dubai Internet City and Dubai Media City, which, until now, had been spared by censorship, are now being filtered despite the promises made to investors. Yet UAE netizens are not easily dissuaded: increasing numbers of them are discovering how to circumvent the censorship and regain Internet access.

# Glossary

WORLD WIDE WEB (WWW): The worldwide system of Internet sites and pages that are interconnected by means of hyperlinks.

BLOCKING: Rendering a website inaccessible. Two methods are possible:
- preventing certain IP addresses from accessing the site (URL or domain name), from opening it or from downloading information or content from it either temporarily or permanently
- rendering the site inaccessible for the entire Internet. The site is surrounded by "barriers" that prevent anyone anywhere on the Internet from accessing it.

FILTERING: Using a filter to selectively block access to sites/blogs/domain names/URLs etc that have certain content. The filter may be constructed on the basis of human or computer language keywords. If the site contains the keywords, the filter blocks access for certain IP addresses or at the data transfer level.

OVER-BLOCKING: An undesired filtering result in which legal or innocent sites are completely blocked because of a few words in their content that the filter is using. For example, a site that talks about contraception is blocked by a filter targeted at pornographic and paedophile sites.

UNDER-BLOCKING: An undesired filtering result in which a filter fails to block a targeted site because its computer or human language does not contain the keywords. For example, a filter intended to block pornographic and paedophile sites fails because they avoid the expected words and use such random words as "sunflower" or "house" to identify photos of naked children.

ENCRYPTION: A system of encoding emails or online content to make them incomprehensible to everyone except the person to whom they are intended. A "key" is needed to decrypt the encrypted information and render it readable by a human being or computer programme.

HACKERS: The term is used in different ways but it usually refers to people with exceptional IT skills who can break into websites, blogs, online accounts and computers via the Internet.
white hats: hackers who – with or without prior permission – break into websites, blogs, online accounts and computers solely to expose their flaws to their owners and help them to improve security.
black hats: hackers who break into websites etc in order to do harm.

CYBER-ATTACK: The action of "hacking" or breaking into a website, blog, online account or computer via the Internet without the owner's knowledge and consent in order to seek, copy or withdraw information or introduce a virus or content. The target may be modified in such a way that – again without the knowledge and consent of its owners or editors and sometimes even after it has been disconnected from the Internet – content is suppressed or blocked or it is infected with a virus that may delete content or infect visitors.

ISP: Internet Service Provider. A company that provides individuals with access to the Internet via a telephone line or TV cable in exchange for payment (usually charged monthly).

NETIZENS: "Internet citizens," people who express their views online, either regularly as bloggers or website editors, or occasionally by posting comments or articles.

# Glossary

**CYBER-DISSIDENTS:** Dissidents whose dissenting activities and views are expressed on the Internet.

**INTRANET:** A network similar to the Internet but much smaller, closed off and accessible only to those who have access codes or IP addresses that are registered as part of the network. For example, company internal networks and Free-Nets.

**DDOS:** A Distributed Denial of Service attack is a form of cyber-attack in which an online service is rendered unavailable by using multiple systems, such as a network of zombie computers, to flood its bandwidth or resources. It is often used as a way of extorting payment from a company whose services are attacked. Web servers, email distribution and file servers are the typical targets of this kind of attack.

**PROXIES:** Programmes or servers that allow you to visit websites and send email messages anonymously. By using a proxy, you can surf the Internet using a different IP address from your own. Proxy servers act as intermediaries between Internet users and the sites they visit.

**VPN:** A virtual private network offers a way of circumventing censorship. Using so-called "tunnelling" protocols and equipment, which is quite costly, the virtual private network is created as a distinct and separate entity existing within the public network, the Internet, in order to extend the local, physical and private networks, interconnected by this technic, and taking advantage of their security system. Traffic through the VPN is encrypted and security is enhanced by authentication mechanisms at the tunnel endpoints.