

**THE INTERNET "BLACK HOLES"**



# 2006 Annual Report

# INTERNET

## EVERYONE'S INTERESTED IN THE INTERNET – ESPECIALLY DICTATORS

The Internet has revolutionised the world's media. Personal websites, blogs and discussion groups have given a voice to men and women who were once only passive consumers of information. It has made many newspaper readers and TV viewers into fairly successful amateur journalists.

Dictators would seem powerless faced with this explosion of online material. How could they monitor the e-mails of China's 130 million users or censor the messages posted by Iran's 70,000 bloggers? The enemies of the Internet have unfortunately shown their determination and skill in doing just that.

China was the first repressive country to realise that the Internet was an extraordinary tool of free expression and quickly assembled the money and personnel to spy on e-mail and censor "subversive" websites. The regime soon showed that the Internet, like traditional media, could be controlled. All that was needed was the right technology and to crack down on the first "cyber-dissidents."

The Chinese model has been a great success and the regime has managed to dissuade Internet users from openly mentioning political topics and when they do to just recycle the official line. But in the past two years, the priority of just monitoring online political dissidence has given way to efforts to cope with unrest among the population.

The Internet has become a sounding-board for the rumblings of discontent in most Chinese provinces. Demonstrations and corruption scandals, once confined to a few cities, have spread across the country with the help of the Internet. In 2005, the government sought to counter the surge in cyber-dissidence. It beefed up the law and drafted what might be called "the ten commandments" for Chinese Internet users – a set of very harsh rules targeting online editors. The regime is both efficient and inventive in spying on and censoring the Internet. Other governments have unfortunately imitated it.

## THE INTERNET'S JAILERS

Traditional "predators of press freedom" – Belarus, Burma, Cuba, Iran, Libya, the Maldives, Nepal, North Korea, Saudi Arabia, Syria, Tunisia, Turkmenistan, Uzbekistan and Vietnam – all censor the Internet now. In 2003, only China, Vietnam and the Maldives had imprisoned cyber-dissidents. Now more countries do.

A score of bloggers and online journalists have been thrown in jail in Iran since September 2004 and one of them, Mojtaba Saminejad, has been there since February 2005 for posting material deemed offensive to Islam. In Libya, former bookseller Abdel Razak al-Mansouri was sentenced to 18 months in prison for making fun of President Muammar Gaddafi online. Two Internet users have been jailed and tortured in Syria, one for posting photos online of a pro-Kurdish demonstration in Damascus and the other for simply passing on an e-mailed newsletter the regime considers illegal.

A lawyer has been in jail in Tunisia since March 2005 for criticising official corruption in an online newsletter. While a UN conference was held in Tunis in November 2005 to discuss the future of the Internet, this human rights activist was in a prison cell several hundred kilometres from his family. A grim message to the world's Internet users.

Censorship of the Web is also growing and is now done on every continent. In Cuba, where you need permission from the ruling party to buy a computer, all websites not approved by the regime are filtered.

The situation has worsened in the Middle East and North Africa. In November 2005, Morocco began censoring all political websites advocating Western Sahara's independence. Iran expands its list of banned sites each year and it now includes all publications mentioning women's rights. China can now automatically censor blog messages, blanking out words such as "democracy" and "human rights."

Some Asian countries seem about to go further than their Chinese "big brother." Burma has acquired sophisticated technology to filter the Internet and the country's cybercafés spy on customers by automatically recording what is on the screen every five minutes.

## COMPLICITY OF WESTERN FIRMS

How did all these countries become so expert at doing this? Did Burma and Tunisia develop their own software? No. They bought the technology from foreign, mostly American firms. Secure Computing, for example, sold Tunisia a programme to censor the Internet, including the Reporters Without Borders website.

Another US firm, Cisco Systems, created China's Internet infrastructure and sold the country special equipment for the police to use. The ethical lapses of Internet companies were exposed when the US firm Yahoo! was accused in September 2005 of supplying the Chinese police with information used to sentence cyber-dissident Shi Tao to 10 years in prison.

China is now passing on its cyber-spying skills to other enemies of the Internet, including Zimbabwe, Cuba, and most recently Belarus. These countries will probably no longer need Western help for such spying in a few years time.

Democratic governments, not just the private sector, share responsibility for the future of the Internet. But far from showing the way, many countries that usually respect online freedom, now seem to want to unduly control it. They often have laudable reasons, such as fighting terrorism, child sex and cyber-crime, but this control also threatens freedom of expression.

Without making any comparison with the harsh restrictions in China, the Internet rules recently adopted by the European Union are very disturbing. One of them, requiring Internet service providers (ISPs) to retain records of customers' online activity, is presently being considered in Brussels and seriously undermines Internet users' right to online privacy.

The United States is also far from being a model in regulation of the Internet. The authorities are sending an ambiguous message to the international community by making it easier to legally intercept online traffic and by filtering the Internet in public libraries.

Julien Pain  
Head of Internet freedom desk

## BAHRAIN

---

Except for pornographic sites, Bahrain does not censor the Internet much. But it has unfortunately begun to regulate it in ways that endanger freedom of expression. The government said in April 2004 that all online publications, including

forums and blogs, must be officially registered. Loud protests led to suspension of the measure but it is still on the books. Three editors of a forum were held for nearly two weeks in March 2005 for allowing "defamation" of the king to be posted.

# BELARUS

---

**T**he regime uses its monopoly of the communications system to block access to opposition websites when it chooses, especially at election time.

President Alexander Lukashenko dislikes criticism, as shown by the harassment in August 2005 of youngsters who were posting satirical cartoons online.

## BURMA

---

This country is among the very worst enemies of Internet freedom and in many ways its policies are worse than China's. The price of computers and a home Internet connection is prohibitive so Internet cafés are the target of the military regime's scrutiny. As in neighbouring Vietnam and China, access to opposition sites is

systematically blocked, in this case with technology supplied by the US firm Fortinet. Burma's censorship is special – Web-based e-mail, such as Yahoo! or Hotmail, cannot be used and all Internet café computers record every five minutes the screen being consulted, to spy on what customers are doing.

## CHINA

---

China was one the first repressive countries to grasp the importance of the Internet and of controlling it. It is also one of the few countries that has managed to “sanitise” the Internet by blocking access to all criticism of the regime while at the same time expanding it (China has more than 130 million users). The secret of this success

is a clever mix of filter technology, repression and diplomacy. Along with effective spying and censorship technology, the regime is also very good at intimidating users and forcing them to censor their own material. China is the world's biggest prison for cyber-dissidents, with 62 in prison for what they posted online.



## CUBA

---

President Fidel Castro's regime has long been good at tapping phones and these days is just as skilled when it comes to the Internet. The Chinese model of expanding the Internet while keeping control of it is too costly, so the regime has simply put the Internet out of reach for vir-

tually the entire population. Being online in Cuba is a rare privilege and requires special permission for the ruling Communist Party. When a user does manage to get connected, often illegally, it is only to a highly-censored version of the Internet.



## EGYPT

---

The government has taken steps since 2001 to control online material. Though censorship is minor, some criticism of the government is not welcome. The government seems unsure what to

do about the explosion of blogs, being more used to pressuring the traditional media. A blogger was arrested for the first time in late October 2005 because of the content of his blog.

## EUROPEAN UNION

---

The EU is responsible for regulating the Internet and rulings often apply to member-states. A European directive on 8 June 2000 about e-commerce proved a threat to freedom of expression, by making ISPs responsible for the content of websites they host and requiring them to block any page they consider illegal when infor-

med of its existence. This creates a private system of justice, where the ISP is called on to decide what is illegal or not. Technicians thus do the job of a judge. The EU is now studying a proposal to oblige ISPs to retain records of customers' online activity. The proposal could limit Internet users' right to privacy.

# IRAN

---

The information ministry boasts that it currently blocks access to hundreds of thousands of websites, especially those dealing in any way with sex but also those providing any kind of independent news. A score of bloggers were thrown in pri-

son between autumn 2004 and summer 2005. One of them, Mojtaba Saminejad, 23, has been held since February 2005 and was given a two-year sentence in June for supposedly insulting the country's Supreme Guide, Ayatollah Ali Khamenei.

# KAZAKHSTAN

---

The media here, including the Internet, are under official pressure and control of online publications has become a key issue because many government scandals have been exposed on websites. President Nursultan Nazarbayev's regime

added new sites to its blacklist in January 2005, including that of a democratic opposition party. In October, an opposition site was forced to give up its national domain name (.kz) after officially-inspired legal action.

## LIBYA

---

**W**ith nearly a million people online (about a sixth of the population), Libya could be a model of Internet expansion in the Arab world. But it has no independent media, so the Internet is controlled, with access blocked to dissident exile sites by filters installed by the regime, which is also

now targeting cyber-dissidents, with the January 2005 arrest of former bookseller Abdel Razak al-Mansouri, who posted satirical articles on a London-based website. He was sentenced in October to 18 months in prison for supposed "illegal possession of a gun."

# MALAYSIA

---

**G**overnment intimidation of online journalists and bloggers has increased in the past three years, notably of *Malaysiakini*, the country's only independent online daily whose journalists have

been threatened and its premises searched. Summonses and questioning of bloggers has been stepped up recently, leading to self-censorship that harms democracy.

# MALDIVES

---

The archipelago is a paradise for tourists but a nightmare for cyber-dissidents. The 25-year regime of President Maumoon Abdul Gayoom cracks down harshly on freedom of expression. Several opposition websites are fil-

tered and one of four people arrested in 2002 is still in prison for helping to produce an e-mailed newsletter. A British company, Cable & Wireless, controls Internet access in the country.



# NEPAL

---

King Gyanendra's first reflex when he seized power in February 2005 was to cut off Internet access to the outside world. It has since been restored, but the regime continues to control it and most online opposition publica-

tions, especially those seen as close to the Maoist rebels, have been blocked inside the country. Bloggers discussing politics or human rights do so under constant pressure from the authorities.

# NORTH KOREA

---

The country is the most closed-off in the world and the government, which has total control of the media, refused until recently to be connected to the Internet. Only a few thousand privileged people have access to it and then only

to a heavily-censored version, including about 30 sites praising the regime. Among these is [www.uriminzokkiri.com](http://www.uriminzokkiri.com), which has photos and adulation of the "Dear Leader" Kim Jong-il and his late father Kim Il Sung.

# SAUDI ARABIA

---

The government agency in charge of “cleaning up” the Web, the Internet Service Unit (ISU), boasts that it currently bars access to nearly 400,000 sites with the aim of protecting citizens from content that is offensive or violates Islamic principles and

social standards. The sites blocked deal mainly with sex, politics or religion (except those about Islam that are approved by the regime). This censorship regularly affects blogging, and blogger.com was made inaccessible for several days in October 2005.

# SINGAPORE

---

**T**he government does not filter the Internet much but is good at intimidating users and bloggers and website editors have very little room

for manoeuvre. A blogger who criticised the country's university system was forced to shut down his blog in May 2005 after official pressure.

## SOUTH KOREA

---

The country is the fourth most-wired country in the world but it excessively filters the Internet, blocking mainly pornographic sites but also publications that supposedly "disturb public order," including pro-North Korean sites. The

government is very sensitive to political opinions expressed online and punishes Internet users they consider go too far. Two users were briefly detained and then fined in 2004 for posting pictures online making fun of opposition figures.

## SYRIA

---

The accession to power of President Bashar el-Assad in 2000 raised hopes of greater freedom of expression, but these were disappointed. The regime restricts Internet access to a minority of privileged people, filters the Web and very closely monitors online activity. A Kurdish

journalism student is in prison for posting photos on a foreign-based site of a demonstration in Damascus. Another Internet user was freed in August 2005 after more than two years in prison for simply passing by e-mail on a foreign-produced newsletter. Both were tortured in prison.

# THAILAND

---

The government filters the Internet as part of its fight against pornography and has used it to extend censorship well beyond this. The method employed is also sly, since when a user tries to access a banned site, a message comes

back saying "bad gateway," instead of the usual "access refused" or "site not found." In June 2005, the websites of two community radio stations very critical of the government were shut down after it pressed their ISP to do so.



# TUNISIA

---

President Zine el-Abidine Ben Ali, whose family has a monopoly on Internet access inside the country, has installed a very effective system of censoring the Internet. All opposition publications are blocked, along with many other news sites. The regime also tries to discourage use of webmail because it is harder to spy on than standard mail programmes that use Outlook. The Reporters Without Borders site cannot be seen inside Tunisia. The government

also jails cyber-dissidents and in April 2005, pro-democracy lawyer Mohammed Abbou was given a three-and-a-half-year sentence for criticising the president online. Yet Tunisia seems well thought-of by the international community for its management of the Internet since it has been chosen the International Telecommunication Union to host the second stage of the World Summit on the Information Society (WSIS) in November 2005.

# TURKMENISTAN

---

No independent media exists here under the dictatorship of megalomaniac Stalinist President Nepharmurad Nyazov. As in Cuba and North Korea, the regime takes a radical attitude to the Internet and keeps virtually all citizens away

from it, with home connections not allowed. There are no Internet cafés and the Web is only accessible through certain companies and international organisations. Even when connected, it is only to a censored version of the Internet.

# UNITED STATES

---

US policy towards the Internet is important because it is the country where the Internet began. But its laws about interception of online traffic do not provide enough privacy guarantees for users. Leading US Internet firms such as Yahoo!, Cisco Systems and Microsoft are also wor-

king with censorship authorities in China, thus throwing doubt on the US commitment to freedom of expression. The United States, home of the First Amendment, the Internet and blogs, should be a model for respecting the rights of Internet users.

## UZBEKISTAN

---

President Islam Karimov proclaimed the “era of the Internet” in his country in May 2001. Online facilities have expanded rapidly but so has censorship of them. The state security service frequently asks ISPs to temporarily block access to

opposition sites. Since June 2005, some Internet cafés in the capital have displayed warnings that users will be fined 5,000 soms (4 euros) for looking at pornographic sites and 10,000 (8 euros) for consulting banned political sites.

# VIETNAM

---

The country closely follows the Chinese method of controlling the Internet, but though more ideologically rigid, the regime does not have the money and technology China has to do this. It has Internet police who filter

out "subversive" content and spy on cybercafés. Cyber-dissidents are thrown in prison and three have been in jail for more than three years for daring to speak out online in favour of democracy.

# ZIMBABWE

---

The local media says the government is about to take delivery of Chinese equipment and technology to spy on the Internet. The state telecoms monopoly TelOne asked ISPs in June 2004 to sign contracts allowing it

to monitor e-mail traffic and requiring them to take steps to stop illegal material being posted. Since political opposition seems to be regarded as illegal by President Robert Mugabe, this is bad news for the country's Internet users.