THE INTERNET UNDER SURVEILLANCE

OBSTACLES
TO THE FREE FLOW OF INFORMATION
ONLINE

THE INTERNET UNDER SURVEILLANCE

REPORTERS WITHOUT BORDERS
2003 REPORT

With support from the French foreign ministry, the French Caisse des dépôts et consignations and the Fondation Hachette.

Population figures: L'état du monde 2003,

Internet figures: International Telecommunication Union.

Maps: L'atlas des drapeaux du monde, by Patrick Mérienne,

Design: Nuit de Chine
ndc@nuitdechine.com

ISBN: 2-90-8830-88-4

The Free Flow of Informations is not Free

BY VINTON G. CERF

Truth is a powerful solvent. Stone walls melt before its relentless might. The Internet is one of the most powerful agents of freedom. It exposes truth to those who wish to see and hear it. It is no wonder that some governments and organizations fear the Internet and its ability to make the truth known. The phrase "freedom of speech" is often used to characterize a key element of democratic societies: open communication and especially open government. But freedom of speech is less than half of the equation. It is also vital that citizens have the freedom to hear and see. It is the latter area in which many governments have intervened in an attempt to prevent citizens from gaining access to information that their governments wish to withhold from them.

The equation is even more complex than simply speaking and hearing or writing and reading. The Internet is much like a piece of paper. The paper is unaware of what is written upon it. The Internet is equally oblivious. It delivers information and misinformation with equal facility. Thus it can become a tool for the delivery of bad data. Worse, this effect may be propagated less by design than by ignorance. It surprises me how often I will find a strident warning in my email inbox forwarded to me by some who should know better, proclaiming that the post office is going to start charging for email or that Microsoft will pay for the forwarding of each copy of the enclosed message. These are all hoaxes but readers are too lazy or perhaps too stupid to take the time to check before they forward.

The antidote for bad information is not censorship but more and better information. Of course, this places a burden on the consumer of information to pay attention and to think critically about what is seen and heard. Surely this is what a responsible citizen should be doing. And surely this is what we should be teaching our children at home and at school.

Despite its great promise, the Internet is not, in and of itself, a guarantor of the free flow of information. George Soros, the well-known financier, takes pains to remind us that the freedom offered by the Internet can be taken away. Indeed, what you will read in the pages that follow illustrates exactly this point. Many governments do want to limit the information its citizens can reach. In some cases the motivations are understandable and even laudable. I can see no redeeming value in child pornography for example and I support efforts to expunge it from the Internet. But those of us living in free societies have been warned repeatedly that censorship is a slippery slope and must be treated with the greatest care.

Even in the worst cases of content abuse, the slope beckons. For example, attempts by governments to extend their jurisdiction beyond their national borders poses a significant threat. More than once, ISPs have been ordered by courts in country A to eliminate content on servers in country B. This extra-territorial gambit leads into a thorny legal thicket into which we should not want to go.

To borrow a phrase from the venture capital world, free citizens must exercise due diligence to assure that their governments are not hiding political censorship behind a putative moral facade. One is reminded of one government's attempt to shut down thousands of Internet cafes on the grounds that one of them had fire law violations and therefore all the others might also be hazardous. This struck me as disingenuous at best and insulting to the intelligence of the citizenry at worst.

I see many responsibilities on the table for effective use of the Internet. Citizens must do their best to guard against government censorship for political purposes. At the same time, they are responsible for trying to distinguish useful and truthful information from bad quality information and must therefore exercise critical thinking about what they see and hear. And that responsibility extends to all media, not only the Internet. Moreover, where disinformation or misinformation exists, thoughtful citizens have a responsibility to draw attention to the problem, possibly even to provide information to counteract the bad data. Furthermore, citizens must bear in mind that not all relevant information is online and that thoroughness dictates examination of material from other sources than the Internet before concluding that due diligence has been taken. One can imagine a briar patch of legal problems for medical caregivers should they rely solely on Internet-based informa-

tion in diagnosis and treatment of disease and injury. Nor should patients imagine that they have limned the standard of care with a casual web search or that they have uncovered a miracle cure in a web site that trumpets its obscure and unsubstantiated treatment.

There are no electronic filters that separate truth from fiction. No cognitive "V-chip" to sort the gold from the lead. We have but one tool to apply: critical thinking. This truth applies as well to all other communication media, not only the Internet. Perhaps the World Wide Web merely forces us to see this more clearly than other media. The stark juxtaposition of valuable and valueless content sets one to thinking. Here is an opportunity to educate us all. We truly must think about what we see and hear. We must evaluate and select. We must choose our guides.

In this 21st century information age, Internauts have significant responsibilities. They must guard against abusive censorship and counteract misinformation. They must take responsibility for thoughtful use of the Internet and the World Wide Web and all of the information services and appliances yet to come. Free flow of information has a price and responsible Internauts will shoulder the burden of paying it.

VINT CERF
McLEAN, VA

Afghanistan

POPULATION: 22,474,000
INTERNET USERS: N.A.
PRIVATELY-OWNED ISPS: YES

After 20 years of war, as well as fierce censorship by the Taliban, the Internet hardly exists. The new government that took power in November 2001 says it favours freedom of expression and media diversity. Growth of the Internet depends on the regime's ability to rebuild the communications infrastructure.

The Islamic state set up by the Taliban after their seizure of Kabul in 1996 brutally stamped out freedom of expression. The Internet was seen by these "theology students" as a heretical and dangerous medium. The 20 years of war that destroyed the country's phone network is another reason the Internet hardly exists. In 2000-2001, only leading Taliban and officials of government ministries and international humanitarian organisations, along with a few leaders of the opposition Northern Alliance, had access to it, via Pakistan or a satellite link.

The Internet was formally outlawed by the Taliban on 13 July 2001 to "prevent access to all vulgar, immoral or anti-Islamic material," as the foreign ministry put it. Six weeks later, a new decree by Taliban leader Mullah Omar banned government and non-government organisations, local and foreign, and all citizens from using it. The religious police were ordered to mete out Islamic punishment to offenders. Only the headquarters of the Taliban militia was allowed to use the Internet, to approve e-mail sent by government ministries.

The regime's collapse in November 2001 opened a new era. When he was sworn in on 22 December, the interim president, Hamid Karzai, stressed that freedom of expression and belief was the right of all Afghans and the government's job was to defend it. The road to widespread Internet access will be hard however.

There are no laws about the Internet, but the problem is logging on. The phone network is too dilapidated to be used for Internet connection, so no ISPs can operate in the country. Satellite phones are the only way to get online and are freely used by government officials, foreign journalists, NGOs and the army. But very few ordinary people can afford to use this very expensive means of communication.

The communications ministry and the UN Development Programme inaugurated the domain name "af" for Afghan Internet users in March 2003. "This is our flag on the Internet," said the minister. There is so far no regulation of the Internet, but the ministry, helped by international organisations, is drawing up a telecommunications law.

The first cybercafé was opened in Kabul in August 2002 by the Afghan Wireless Communication company. Soon afterwards, the media aid NGO Aïna opened an Internet centre for Afghan journalists. In March 2003, there were about five cybercafés in Kabul.

The Internet is a vital source of information however for the tens of thousands of Afghans who live in the United States, Canada, Australia, France and Germany. At the end of 2001, they decided to use the Internet to help rebuild the country and unite the scattered diaspora. Exiles working in California's Silicon Valley created a site called Virtual Nation, linking Afghans around the world and aid organisations seeking to help the country.

LINKS:

• www.virtualnation.org
Afghan Reconstruction Development Center

• http://francais.afgha.com
The *Afghanistan* news agency

• www.af-com-ministry.org
The ministry of communications

Algeria

POPULATION: 30,841,000
INTERNET USERS: 500,000
PRIVATELY-OWNED ISPS: YES

Unlike in neighbouring Tunisia, the Internet in Algeria is not controlled by the authorities. Laws give the government power to regulate and even monitor it, but they have not so far been used.

The daily paper *Liberté* reported in 2001 that a policeman in Boufarik, a small town west of Algiers, tried to get the owner of a cybercafé to note down the names and addresses of customers and the websites they connected to. The owner refused and filed a complaint. After this was reported by the media, the local police chief said it was a personal initiative of the police officer and that he had been suspended.

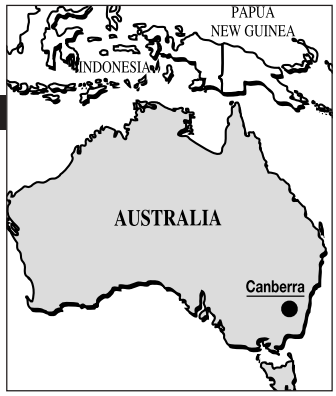
Since then, no cases of censorship have been recorded. However, article 14 of a 1998 telecommunications decree says ISPs "must take responsibility" for the content of sites and servers they run or host. They are also required to "take all necessary steps to ensure continuous monitoring" of content and servers accessible to their customers so as to block access to "material that undermines public order and morale."

In May 2001, parliament passed an amendment to the criminal code that caused outcry among journalists. Its article 144 (b) provided for prison terms of between two months and a year and fines of between 750 euros and 3750 euros in the event of "denigration of the president through insults or defamation," in writing, drawings or speech, through radio and TV broadcasts or electronic or computer means.

Offenders can be directly prosecuted by the government without a prior complaint being filed. For repeat offenders, the punishments are doubled. These sanctions also apply to such attacks on parliament, the armed forces and any other public body. Several journalists have been given prison sentences, but the measure has not so far hampered the growth of the Internet.

LINKS:

- www.algeria-interface.com: News site of *Algeria Interface*
- www.algeria-watch.de: The human rights group Algeria Watch
- www.maghreb-ddh.org: The Human rights in North Africa



Australia

POPULATION: 19,338,000
INTERNET USERS: 8,400,000
PRIVATELY-OWNED ISPS: YES

The Broadcasting Services Act, which came into force on 1 January 2000, spells out material to be banned from websites, including pornography involving children, bestiality, excessive violence, real sex acts and information about crime, violence and drug use. The arbiter of this is the regulatory Australian Broadcasting Authority (ABA), which asks the ISPs of sites concerned to take reasonable steps to bar access to them.

Civil liberty groups oppose these restrictions, as well as the obligation of ISPs to offer content filters to their customers. Most ISPs are refusing to comply and simply list sites that provide such products.

In October 2001, the Cybercrime Act came into effect, allowing judges to force suspects to reveal their encryption codes. A few months later, the federal senate, rejected an amendment to the telecommunications law that would have allowed the security services to intercept e-mail without court permission.

Eight major international media – including *Yahoo!*, *CNN*, *Reuters* and *The Guardian* – said on 28 May 2002 they would give legal support to an appeal by the Dow Jones US media group to the High Court against a libel conviction. The plaintiff was Australian businessman Joseph Gutnick, who said he had been libelled in an article on the website of the group's Barrons magazine. The Victoria state supreme court, saying the article could be read in the state, convicted Dow Jones, whose lawyer warned that the ruling was a serious precedent that would threaten the online media worldwide.

In November 2002, the ABA refused to censor three anti-globalisation sites that called on demonstrators against a World Trade Organisation meeting in Sydney that month to equip themselves with baseball bats and gas-masks. The authorities, especially the police, had asked for the censorship on grounds it was clear incitement to physically attack the police.
The government responded to the ABA's refusal by moving to set up a centre to combat high tech crime. The daily newspaper *The Courier-Mail* said it would give the federal government power to censor websites directly.

LINKS:

• www.efa.org.au/Analysis/aba_analysis.html
Electronic Frontier Australia, on Internet censorship

• www.aba.gov.au
The Australian Broadcasting Authority

• www.zdnet.com.au
Zdnet on new technology

Azerbaijan

POPULATION: 8,096,000
INTERNET USERS: 300,000
PRIVATELY-OWNED ISPS: YES

The high cost of computers and ISP subscriptions, as well as poor-quality phone lines and equipment, hamper growth of the Internet, though the cost of connection is getting cheaper (now less than $1 an hour). More and more Azeris are using cybercafés in big towns but connection is still difficult in country areas.

A dozen state and privately-owned ISPs are in operation, but the communications ministry takes a 51 per cent stake in all private ones, hands out operating licences to them and keeps control of transmission lines. The Internet is also overseen by the national security ministry, which monitors message activity by regime opponents, intellectuals and foreign businessmen. The state unofficially justifies this by a need to combat Armenian hackers, who have been targeting official Azeri sites for the past few years.

Access to the Russian-based news site *Virtualnyi Monitor* was temporarily blocked in March 2002 after it carried articles criticising the government.

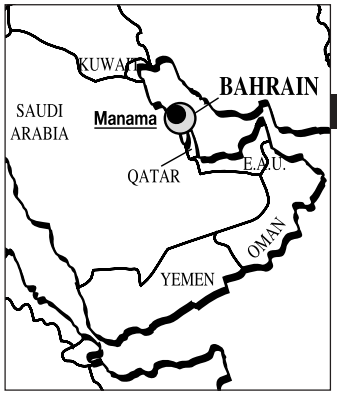
In July that year, the Azerbaijan Internet Forum launched an online protest against government censorship which hampers the growth of the Internet in the country.

LINKS:

• www.rferl.org/bd/az
The Azerbaijani service of *Radio Free Europe/Radio Liberty*

• www.eurasianet.org
The news site *Eurasianet*

• www.turaninfo.com
The independent news agency *Turan*



Bahrain

POPULATION: 652,000
INTERNET USERS: 165,000
PRIVATELY-OWNED ISPS: NO

On World Press Freedom Day (3 May) in 2003, the Association for Islamic National Reconciliation, the country's main opposition group (representing Shiites), denounced the government for blocking access to several pro-opposition websites. On 3 May a year earlier, Association supporters demonstrated outside the offices of the country's lone ISP, the Bahrain Telecommunications Company (Batelco), against the blocking and in favour of free expression. Batelco also monitors e-mail messages.

The information ministry said the sites had been censored because they had become platforms for spreading biased news, rumours and lies. The minister, Nabil el-Hamer, said in March 2002 that the ban would be lifted when the sites removed the offending material.

Among the sites blocked were the London-based Bahrain Freedom Movement's www.vob.org, as well as www.bahrainonline.org, the online newspaper *Al-Manama* (www.al-manama.net) and a site run by Islamic fundamentalist Abdel Wahab Hussein.

LINKS:

• www.batelco.com.bh
Bahrain Telecommunications Company

• www.gulfissues.net
News about countries of the Gulf (in Arabic).

• www.bahraintribune.com
Bahrain Tribune (English-language daily)

Bangladesh

POPULATION: 140,369,000
INTERNET USERS: 204,000
PRIVATELY-OWNED ISPS: YES

A dozen English- and Bengali-language newspapers are available online, but there are very few ISPs and Internet users for such a populous country. Police have stepped up their surveillance of the e-mail of some journalists and political .

A few hours after the 27 February 2001 launch of the human rights portal banglarights.com, the phone and fax links of DRIK, the NGO hosting the site, were cut off. The Bangladesh Telegraph and Telephone Board regulatory authority denied it was to do with DRIK's activities and said it was part of a government enquiry following complaints about ISPs.

DRIK also hosts meghbarta.com, the site of an anti-globalisation group very critical of the government. At the time of banglarights.com's launch, Meghbarta had posted articles about the local human rights situation and attacks on human rights activists which reportedly annoyed some politicians.

In November 2001, the government also cut off the phone lines of about 60 firms offering Internet services. The telecommunications minister said this was because the companies could not get their professional licences renewed. But the companies said it was done to stop people using the Internet to make cheap phone calls abroad instead of going through the state-owned phone company. This practice, common in Bangladesh and permitted in most countries, is not allowed by the government.

The police have stepped up their monitoring of e-mail of journalists and political activists. In early 2002, the Islamist newspaper *Inqilab* published private e-mail messages of journalist Shahriar Kabir that had clearly been intercepted by the security services. The pro-government daily was at the time attacking Kabir as a traitor in the pay of India. During a crackdown by the right-wing government at the end of 2002, police seized the computers of several journalists, including Saleem Samad, the Reporters Without Borders correspondent. A climate of fear developed and several reporters and human rights activists told Reporters Without Borders they no longer used e-mail addresses supplied by national ISPs because messages might be monitored by the police.

LINKS:

• www.drik.net/html/home1.html
DRIK

• http://bangladesh-web.com/news
The daily *News from Bangladesh*

Belarus

POPULATION: 10,147,000
INTERNET USERS: 808,700
PRIVATELY-OWNED ISPS: YES

Although President Alexander Lukashenko is keen to encourage digital technology, his regime closely monitors the Internet. Local users suspect this is done through the obligatory "certification" of all modems by the communications ministry, which takes at least a week to "verify" them.

The state has a telecommunications monopoly through Beltelekom. Smaller privately-owned ISPs have sprung up, such as Global One (a subsidiary of the American firm Sprint) and Open Contact, but their traffic is handled by Beltelekom's Internet division, Belpak. Operating licences are only issued in exchange for signing up with Beltelekom, agreeing to surprise "technical inspections" by communications ministry officials and providing an annual list of subscribers. ISPs must also promise not to exchange traffic with each other. Independent websites are not censored, perhaps because Internet users are still few.

Parliament rejected a proposed "data security" law on 22 May 2002 which had been condemned by the Belarus Association of Journalists (BAJ) as tightening government control over the content and flow of information.

On 5 November 2002, police interrogated Iulia Doroshevich and Andrei Pachobut, two journalists on the daily paper *Pagonya*, which was banned in 2001, about the online version of the paper, which was still appearing. Pagonya's editor and one of its journalists were imprisoned at hard labour from September 2002 to March 2003 for "insulting" President Alexander Lukashenko in an article.

LINKS:

• baj.ru/indexe.htm
Belarus Association of Journalists (BAJ)

• www.article19.by/publications/instrumentscontrol/index.html
Survey of laws concerning freedom of expression, done by the organisation Article 19

Belgium

POPULATION: 10,264,000
INTERNET USERS: 3,400,000
PRIVATELY-OWNED ISPS: YES

Almost a third of the population uses the Internet, up from only half a million people in 1998. Ninety per cent are men between 24 and 45, two-thirds of them with a university degree or the equivalent.

This rapid growth is partly because Brussels, the capital of Europe and site of the European Union's major institutions, was a pioneer of introducing new technology. The growth of the Internet is also fed by the many commercial incentives offered by fiercely competing local ISPs.

Belgium is keen on free expression and human rights, but it was one of the first European countries to pass a law on retention of Internet connection data. In 2001, even before the 11 September attacks, such retention had been extended to a year. The concern to have and use this information is probably because the country has been traumatised in recent years by several paedophilia scandals and the exploitation of children through the Internet.

LINKS:

• www.ael.be
Electronique Libre association

• www.internet-observatory.be
Internet Rights Observatory

Burma

POPULATION: 48,364,000
INTERNET USERS: 10,000
PRIVATELY-OWNED ISPS: NO

Burma is one of the countries most shut off from the Internet. Its people have to make do with a local substitute, the Myanmar Wide Web, created by the military regime. The few thousand authorised e-mail accounts are monitored by the authorities. The government slightly eased restrictions in 2002 by allowing a second ISP to start up and a cybercafé to open in Rangoon.

The Internet situation has become a little easier since 2000, but only a few hundred hand-picked people – regime officials, top army figures and heads of export companies – are allowed full access to the Internet, though still closely monitored. Nearly 10,000 people are limited to e-mail activity but only for professional purposes and again strictly under the eye of the posts and telecommunications authority MPT and military intelligence officials, who reportedly use a Dans Guardian content filter.

A national intranet controlled by the army

Fewer than 10,000 people are allowed to use the substitute Internet, the local Myanmar Wide Web intranet set up by the regime, but only a few dozen mainly service or administrative sites, all government-approved, are accessible. Even that is hard to log on to, since until very recently, only one cybercafé, at the university, had free access to Myanmar Wide Web.

Only big hotels, travel agencies and foreign and local businesspeople can use e-mail, which arrives through a local server and is sorted and read by the MPT before being passed on to its destination. The MPT is thought to have signed up more than 5,000 people for e-mail accounts.

Prison awaits those do not comply

A 1996 law bans the import, possession or use of a fax machine or modem without official permission. Those who disobey risk up to 15 years in jail, as does anybody who uses the Internet to "undermine the state, law and order, national unity, national

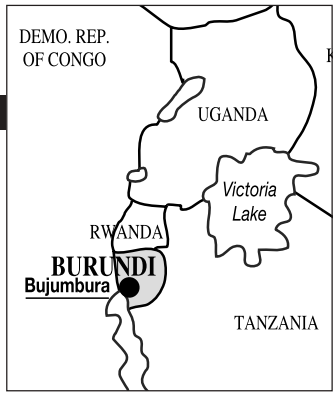
culture or the economy." Anyone who creates a link to an unauthorised website also faces a prison sentence. Since 20 January 2000, online political material has been banned and websites can only be set up with official permission. The rules ban any online material considered by the regime to be harmful to the country's interests and any message that directly or indirectly jeopardises government policies or state security secrets.
The measures to prevent people being freely informed and stop them looking at exiled opposition websites, which are very active, with the Free Burma Coalition site, for example, grouping several opposition movements.

Small steps forward

"Some people in the regime think the Internet is vital for economic development, but they also know the big danger of allowing access to diversity of news and culture," says one Burmese journalist. "So the debate is a heated and tricky one among them." Things are therefore moving forward very slowly.
The MPT's monopoly as the country's sole ISP was broken in spring 2002 when a second ISP, Bagan Cybertech, was authorised. But the break was a false one and the regime has little to fear since the new ISP is partly state-owned and its boss, Ye Naung Win, is the son of the country's powerful military intelligence chief, Lt. Gen. Khin Nyunt.
The new firm says the regime has approved creation of 10,000 new e-mail accounts and given permission for several thousand more people to have Internet access. It has reportedly already sold more than 3,000 subscriptions and says the national intranet should grow to several hundred sites quite soon.
The Thai-based monthly magazine *Irrawaddy* reports that all requests to open cybercafés have to pass through Bagan Cybertech. With the regime's permission, a private individual can buy Internet access for 260 euros. Companies have to pay 600 euros.
The Burmese business magazine *Living Color* announced in September 2002 that Rangoon's first cybercafé for the general public would soon open. But customers will not be able to get their e-mail there. They can do so in the very few "e-mail shops" in the capital, though this is illegal and barely tolerated by the regime.
Will the media benefit from this small opening? Most Burmese weekly and monthly publications put their contents on line in the course of 2001. But the independent press and opposition groups still have to set up and run their websites from outside the country.

LINKS:

- www.irrawaddy.org: Exiled opposition magazine *The Irrawaddy*
- www.myanmar.com: Official government site
- www.bma-online.net: Freedom of expression in Burma
- www.burmanet.org: *Burmanet News*
- www.firstmonday.dk/issues/issue6_5/krebs : A report on the Internet's impact in Burma



Burundi

POPULATION: 6,502,000
INTERNET USERS: 6,000
PRIVATELY-OWNED ISPS: YES

Several journalists from the online news agency *in-burundi.net* were beaten up by police in Bujumbura in early January 2002 while investigating the torture by state intelligence service agents of a watchman arrested in the previous month's murder of Kassi Malan, the World Health Organisation's representative in Burundi. The police warned the journalists they "could come to the same end."

The National Communications Council banned Burundian media websites on 26 August 2002 from posting material emanating from political groups "preaching hatred and violence." This was chiefly aimed at the *Rugamba* website of the *Net Press* news agency, which carried statements by opposition groups. The Council threatened to shut down *Net Press* if *Rugamba* did not stop posting material that "undermines public order and security."

LINKS:

• www.in-burundi.net
Online news agency *In-Burundi.net*

• www.netpress.bi
Rugamba (*Net Press* news agency)

Canada

POPULATION: 31,153,000
INTERNET USERS: 15,200,000
PRIVATELY-OWNED ISPS: YES

After the 11 September attacks, parliament passed an anti-terrorist law on 18 December 2001 that undermined the principle of protecting journalistic sources.

The law amended the Criminal Code, the National Defence Act, the Official Secrets Act and the law about individual freedoms. Changes to the Criminal Code extended electronic surveillance of criminal organisations to cover terrorist groups and police will no longer have to show that such monitoring is a last resort. The decision remains one for a Supreme Court judge to make but the maximum authorised period of it was increased from 60 days to a year.

A change in the National Defence Act allows the defence minister to authorise the Communications Security Establishment (CSE) to intercept private communications (including electronic ones) linked to activity defined by the defence minister (chapter 273.65.1). The confidentiality of e-mail communication, and with it the protection of journalistic sources, has clearly been destroyed. The CSE's rules, however, say it cannot monitor Canadians or people living in Canada.

The government began consultations on 25 August 2002 about adapting to new technology various laws allowing legal access by prosecutors to private documents in the interest of the security and welfare of Canadians. It proposed that all ISPs be obliged to ensure they had the technical means to provide legal access to their data by national security officials. In effect, they would have to retain and provide data about their customers.

The government noted that the Criminal Code banned deliberate interception of private communications. But, in an attempt to justify possible interception of e-mail messages, it argued that when a message was written down, it was no longer really private, since it could easily fall into the hands of someone else.

These views were fiercely attacked by Privacy Commissioner George Radwanski in a report in late January 2003. He accused the government of using the 11 September attacks as an excuse to collect and use more and more data about private individuals.

Such measures had no place in a free and democratic society and showed the government's contempt for privacy, he said

LINKS:

• www.efc.ca
Electronic Frontier Canada

• www.liguedesdroits.ca
Ligue des droits et libertés (in French)

• www.privcom.gc.ca
Privacy Commissioner of Canada

• www.cse-cst.gc.ca
Communications Security Establishment

• www.crtc.gc.ca
Canadian Radio-television and Telecommunications Commission

• www.parl.gc.ca/37/1/parlbus/chambus/house/bills/government/C-36/C-36_4/C-36_cover-E.html
The C-36 anti-terrorist law

• http://canada.justice.gc.ca/fr/cons/la_al
About legal access

China

POPULATION: 1,284,972,000
INTERNET USERS: 59,100,000
PRIVATELY-OWNED ISPS: NO
INTERNET USERS AND CYBER-DISSIDENTS IN PRISON: 42

The number of Internet users doubles nearly every six months and the number of websites every year. But this dizzying growth is matched by the authorities' energetic attempts to monitor, censor and repress Internet activity, with tough laws, jailing cyber-dissidents, blocking access to websites, monitoring online forums and shutting down cybercafés.

The tremendous growth of the Internet now makes it technically impossible for the authorities to monitor the content of all the millions of e-mail messages being exchanged around the country. But the regime is still banning users from looking at websites it considers endanger "the social order and the socialist system." The authorities have created a legal arsenal to punish cybercrime and cyber-dissidence.

The official news agency *Xinhua* announced in January 2001 that anyone involved in "espionage activities" such as "stealing, uncovering, purchasing or disclosing state secrets" using the web or other means risked the death penalty, or between 10 years to life in prison. The same month, the public security ministry set up a website giving information about currently laws and warning Internet users of the risks they would run if they circulated "subversive" information. This concerned both the 12 million Chinese who have a private Internet connection and those who use cybercafés.

The information and technology ministry introduced new rules on 14 January 2002 about monitoring the Internet. ISPs involved in "strategic and sensitive fields" such as news sites and forums would have to record details of their customers, such as their Internet ID, postal address and phone number. They were also required to install software to monitor and copy the content of "sensitive" e-mail messages. The ISPs are obliged to break off transmission of e-mails containing obscene or subversive material, advocating terrorism or threatening national security or national unity.

The authors of such messages are to be reported to the ministries of information and technology and of public security and to the department for protection of state secrets. The ISPs must also use official equipment that cannot be used for spying or

hacking, and foreign firms selling software to China must promise in writing not to install spying devices on Chinese computers.

ISPs and news site webmasters must themselves censor content that contravenes these rules and ferret out subversive comments or messages on major websites. Discussion forums are popular places to talk politics and criticise the government. If the ISPs do not censor the sites themselves, the authorities will. Access to the search-engine Google was blocked for 12 days in August 2002. The move drew sharp criticism from experts and from Chinese and foreign investors, who do not usually say much about the authorities' attitude to the Internet.

The government enacted a law on 15 November 2002 on the running of cybercafés, making owners responsible for the websites looked at by customers, on pain of being shut down or fined.

This dictatorial trend led to 18 Chinese intellectuals signing a "declaration of rights of Chinese Internet users" in July 2002, calling for freedom of expression (creating websites), freedom of online information (access to all websites) and freedom of association (opening cybercafés). One of the petition's organisers said that if major websites yielded to the Chinese government's pressure, it would "greatly reduce the power to resist" of NGOs that had found the Internet a place where they could express themselves. This founding document of Internet freedom in China was signed by thousands of the country's Internet users.

Faced with the spiralling growth of the Internet, the government abandoned its "Great Cyber Wall" strategy and began developing the top secret "Golden Shield" project put forward by the ministries of public security and information industry. Nearly 3,000 people were recruited to defend the government from Internet subversion.

In April 2002, public security minister Jia Chunwang called a meeting in Beijing to discuss the protection and security of government information. Ways of combating Internet offences, especially those considered subversive, were considered and the minister reportedly said Internet monitoring equipment had become "vital tools for national security, political stability and national sovereignty."

The authorities were disturbed at critical articles posted online by the Falungong spiritual movement and the Chinese Democratic Party and decided to step up recruitment of experts to combat "foreign forces" trying to "subvert China via the Internet."

At the end of December, the public security department in the southern province of Guangdong organised a conference on Internet development and security to assess the Internet's influence on "stability and public order," according to the provincial police chief.

Luan Guangsheng, head of the province's Internet police, told the Hong Kong daily *South China Morning Post* that the Internet had to be "very tightly controlled" and that users had to "take responsibility if they passed on dangerous material." He refused to say how many cyberpolice the province had but said the number was growing.

Crackdown on cyber-dissidents

The tough and repressive laws are not just aimed at cyber-dissidents but also at anyone using the Internet as a means of expression, freely obtaining information or criticising the government or the ruling Communist Party. At least 21 cyber-dissidents are in prison in China, 16 of them serving prison sentences.

In spring 2001, a shopkeeper, Liu Weifang, was jailed for three years by a court in the northwestern province of Xinjiang for alleged subversion for posting very critical articles about the Communist Party and the government's economic reforms on Internet forums in 2000 and 2001. Despite using a pseudonym, "Lgwf", police managed to identify him.

Lu Xinhua, a member of the banned Chinese Democratic Party (most of whose leaders are in jail), was picked up on 11 March 2001 in Wuhan and formally arrested for subversion on 20 April, according to the Information Centre for Human Rights and Democracy. When he was picked up, police ransacked his home and seized his computer. He had written and posted on foreign websites many articles about human rights violations in Wuhan and criticising Chinese President Jiang Zemin. In December, he was jailed for four years by the Wuhan intermediate court after a secret trial.

Yang Zili, founder of the website lib.126.com, was arrested in Beijing on 13 March as he left his home. His wife was arrested the same day and freed 48 hours later after being forced to promise in writing not to reveal what had happened. Yang, a graduate of Beijing University, wrote a number of theoretical articles posted on his website advocating political liberalism, criticising repression of the Falungong spiritual movement and deploring the problems faced by the peasantry. In a poem, he called for "a fatal blow" to be struck against "the ghost of communism."

Police refused to say where he was being held or why. Also on 13 March, three other people helping to run the website – Jin Haike, a geologist, Xu Wei, a journalist with the newspaper *Consumers' Daily*, and Zhang Honghai, a freelance journalist – were arrested in Beijing.

Together with Yang, they appeared on 28 September before the Beijing intermediate court. Only three members of the public were allowed to attend. Three of the four accused had lawyers and Zhang chose to defend himself. Jin Haike's lawyer, Liu Dongbin, said the prosecution witnesses were unreliable since they had already been used several times in similar cases.

Yang said the charges "in no way imply any plan to subvert the government. When we speak of freedom and liberalisation, we believe this will come about through reforms. Is it not evident that the last 20 years of reform and conciliatory policies have led China towards liberalisation?" he asked.

The four cyber-dissidents denied they were setting up branches of their group throughout the country by posting articles on the Internet and setting up websites. Zhang said nothing in the public prosecutor's address proved they were planning to overthrow the government. "We didn't even have the 300 yuan we needed to launch the website. How can all this be seen as undermining the state's authority?"

The prosecutor then charged that the articles published on the Internet, including "Be a New Citizen, Reform China," and "What Needs to Be Done," were subversive because they accused the government of "practising a false form of democracy," advocated "an end to an obsolete system" and expressed a desire to create "a new China." After a four-hour hearing, the court rose without giving a verdict.

Chi Shouzhu, a worker and former political prisoner, was arrested at the railway station in the northeastern town of Changchun on 17 April. He had just printed out at a friend's home material from a foreign-based opposition website. Chi, 41, had already spent 10 years in prison for his involvement in the 1989 Beijing Spring unrest. A native of the northeastern province of Jilin, he had gone to Changchun for treatment of illnesses he had developed in prison.

Leng Wanbao, a dissident also from Jilin, was interrogated for two hours on 18 April by police who accused him of posting "subversive material" on the Internet.

Wang Sen, a member of the Chinese Democratic Party, was arrested on 30 April in Dazhou, in the southwestern province of Sichuan. In an article posted on the Internet, he allegedly accused a state clinic of selling anti-TB medicine donated by the Red Cross. On 30 May 2002, he was jailed for 10 years by the people's intermediate court in Dazhou for "trying to overthrow the government." The court also said he had organised a workers' protest at a iron and steel factory in the city.

CDP member Wang Jinbo, was arrested on 9 May 2001 in Junan, in the eastern province of Shandong. Police reportedly told his father that he was being held for two weeks because he had insulted the local police on the Internet. Wang, who had already been arrested several times for political activities, was tried in November for "subversion" and jailed for four years on 13 December by the Linyi intermediate court for e-mailing articles criticising the government's attitude towards the 1989 pro-democracy movement. He began a hunger-strike on 28 February 2003 to mark the opening of the People's National Assembly in Beijing and to protest against his imprisonment, former political prisoner Ren Wanding told foreign journalists in Beijing. He began eating again a week later. His family said his health had deteriorated in 2003.

Businessman and webmaster Hu Dalin was arrested on 18 May in the southwestern town of Shaoyang for posting on the Internet anti-American articles written by his father. He was not been charged and police told his family he had been picked up for "subversive activity" on the Internet. His parents and girlfriend were not allowed to visit him in the first months of his detention.

At about the same time, Guo Qinghai, a bank clerk, was jailed for four years by a court in Cangzhou, south of Beijing, for alleged subversion. His family was not told of the trial beforehand. He is believed to be in prison in Cangxian, near Cangzhou. He had been arrested in September 2000 for putting material on foreign websites advocating political reform and calling for the release of cyber-dissident Qi Yanchen. He used a pseudonym but police managed to identify him.

In June, Li Hongmin was arrested in the southern city of Canton for disclosing by e-mail the 2001 Chinese version of the Tienanmen Papers, which accuses top Chinese officials of being behind the June 1989 Tienanmen Square massacre. The US-based dissident website *VIP Reference* said he was freed a few weeks later but had been sacked from his job at the insistence of the authorities.

At the end of June, the authorities announced that the trial of Huang Qi, founder of the website 6-4tianwang.com, who had been arrested in June 2000 for putting supposedly subversive material on the site, had again been postponed indefinitely by the intermediate court in the southwestern city of Chengdu because of the Communist Party's 80th birthday celebrations. Many people said it was really to avoid bad publicity on the eve of the decision about where the 2008 Olympics Games would be held.

The trial had earlier been postponed on 13 February 2001 because of Huang Qi's poor health. His wife said he had been beaten in prison and had a scar on his forehead and had lost a tooth. She was not allowed to visit him and his lawyer Fang Jung was only permitted to see him once in the course of seven months.

In mid-August, his lawyer announced that the trial had taken place in great secrecy and had lasted only two hours and verdict had not been disclosed. No family members were allowed to attend. Huang's wife managed to take a photo of him as he arrived at the court but police seized her camera. The trial is the first of the creator of a website for having posted "subversive" material.

On 11 July, the day after the 2008 Olympics Games were awarded to Beijing, Yan Peng, a computer salesman and dissident, was arrested in the southern province of Guangxi and his computer seized. The Information Centre for Human Rights and Democracy said Yan, one of the first people to use the Internet to oppose the Chinese Communist Party, was returning from a trip to Vietnam and was accused of violating immigration laws. On 16 July, three dissidents from Qingdao, including Mu Chuanheng, tried to get him released, but police refused to see them. Yan had been jailed several times since 1989. In September 2002, he was jailed for 18 months by a court in Qingdao.

In mid-August 2001, Mu Chuanheng, a lawyer who has been banned from practising for the past 15 years, was arrested in the eastern city of Qingdao for publicly calling for the release of Yan Peng. A dozen police raided his home and seized his computer and articles he had written. Mu was active in the 1979 Beijing Spring and contributed often to the cultural website xinwenming.net, which was banned in August 2000 by the state security ministry. Mu was jailed for three years by a Qingdao court in September 2002.

In September 2001, Zhu Ruixiang, a lawyer, co-founder and formed chief editor of *Radio Shaoyang*, was found guilty of subversion by a court in Shaoyang, in the south-eastern province of Hunan, for sending to a dozen friends copies of articles from the pro-democracy website *VIP Reference* (www.bignews.org) criticising the government. He was at first sentenced to nine months in prison but the authorities called for a harsher punishment and he was eventually jailed for three years. When he was arrested on 8 May, all his belongings, including his computer, were seized.

On 27 April 2002, Yang Jianli, chief editor of the US-based dissident online magazine *Yibao* (www.chinaeweekly.com), was detained at the airport in Kunming, in the southern province of Yunnan, and then formally arrested on 2 June. He was returning to China for the first time since his expulsion in 1989, with a passport borrowed from a friend because the Chinese authorities had refused to renew his own. He had been on the authorities' black list for several years and was returning clandestinely to investigate workers strikes in the northeast of the country. He is reportedly being held in prison in Beijing. His brother Yang Jianjun went to Beijing in June but police refused to tell him anything about his detention. Married with two children, he lives in Brooklyn, Massachusetts.

Former policeman Li Dawei was jailed for 11 years on 24 June by a court in the north-western province of Gansu. The Information Centre for Human Rights and Democracy said he was convicted of subversion for downloading more than 500 articles from foreign-based Chinese pro-democracy websites which he then published in the form of books. He was also accused of being in contact with foreign-based "reactionary" groups. He was arrested in April and his trial began in May. His lawyer, Dou Peixin, said the provincial supreme court had agreed to hear his appeal.

In August, journalist Chen Shaowen was picked up in Lianyuan, in Hunan province, and formally arrested in September for what an official said was posting "many reactionary articles" on the Internet. Chen has written regularly for several foreign-based Chinese-language websites about social inequality, unemployment and pitfalls in the legal system.

Wan Yanhai, founder of the Aizhi Action Project and the website www.aizhi.org, which has fought since 1994 against discrimination against HIV/AIDS sufferers and for Internet freedoms, disappeared in Beijing on 24 August while attending a film about homosexuality. Some people at the occasion said he had been followed by public security ministry officials.

The Project helped expose a blood transfusion scandal in the central province of Henan by publishing on its website the names of the peasants who had died of AIDS after selling their blood. The site, which is still accessible, also contains moving descriptions of the plight of HIV-positive people in China. In July, the university that hosted the Project closed the offices of the group, which was then outlawed.

On 17 July, Wan signed a "declaration of rights of Chinese Internet users" calling for online freedom of expression. In early August, after a law banning information about AIDS came into force, he repeated his desire to continue his AIDS campaign on the Internet. With few exceptions, AIDS is a taboo subject in China, especially in Henan province. Dozens of Chinese and foreign journalists have been prevented from investigating the country's epidemic.

In early November, Li Yibin, a computer science graduate, was arrested in Beijing. Human Right Watch in China said he had been picked up for involvement in the online magazine *Democracy and Freedom*, using the pseudonyms "Springtime" and "Spring Snow."

On 7 November, on the eve of the opening of the 16th Communist Party congress, cyber-dissident Liu Di, a 22-year-old psychology student, was arrested on the Beijing University campus. Her family only learned she had been picked up when police arrived at their apartment and searched through her possessions, taking away her books, notes and computer. Her parents took a change of clothes to the police station but were told they could not see her.

The dissident organisation China Labor Watch said police told one of her teachers she had been arrested because of her links with an "illegal organisation." However her father said it was probably because of her postings on the Internet. Under the pseudonym of The Stainless Steel Mouse, she had urged Internet users to "ignore government propaganda" and "live in freedom." She also criticised the arrest of imprisoned website founder Huang Qi.

Teacher Ouyang Yi, who runs a website and is a member of the banned Chinese Democratic Party, was arrested on 4 December in Chengdu, capital of the southwestern province of Sichuan, according to China Labor Watch. It said Ouyang's wife had learned of his arrest when local police came to search the family home in Suining, nearly 200 kms from Chengdu, on orders from the provincial capital's police.

Ouyang is well-known to the authorities as one of the 192 signatories of an open letter in November to the 16th Communist Party congress calling on it to reverse its condemnation of the 1989 Tienanmen Square demonstrations in Beijing. In his web-site articles, he wrote about the 1989 dissidence (known as the second Beijing Spring), the failure of the government's economic policies and the need for reforms in the state structure. He was arrested in 1996, 1998, 1999 and earlier this year for his dissident activities, but had not been held longer than 48 hours.

Cyber-dissident Liao Yiwu was arrested on 18 December at his home in Chengdu, but released a few hours later after the house had been searched. The writer and poet began putting his writings on the Internet after they were banned from normal publication by the authorities. He has been regularly harassed by the authorities for this.

In early March 2003, Qi Yanchen, was said to be in bad health in prison no. 4 in Shijiazhuang (in Hebei province, south of Beijing). He has several serious ailments, including colitis, and has only been getting medicine through his wife, Mi Hongwu, who is only allowed to visit him every two months. She said he was "very weak" last time she saw him in mid-January. He has been in jail since 1999 and was sentenced in September 2000 to four years in prison after putting online long extracts from his book "The Collapse of China," which the prosecutor at his trial said was "subversive."

Zhang Yuxiang was arrested at his home in Nanjing (in the eastern province of Jiangsu) on 12 March and interrogated at length about articles he had posted on the Internet. The police tried to make him confess having contacts with other cyber-dissidents. Human Rights in China said he had been put under house arrest in a public building in the Siyang district, but this could not be confirmed. His wife has not had news of him since he was arrested or received any official document about his detention. Zhang, a former armed forces propaganda department official in Nanjing, had already spent two years in prison for helping the dissident Chinese Democratic Federation. After he was freed, he had continued regularly posting political articles online and signing petitions.

A Public Security Bureau official in Beijing confirmed on 25 March the arrest and indictment of cyber-dissident Jiang Lijun, who had disappeared without trace since 6 November 2002. Police had secretly held him at Qincheng prison, near Beijing, where the most important political prisoners are reportedly held. He was said to have been charged on 14 December 2002 with inciting people to overthrow the government, but police did not provide his wife, Yan Lina, with any document. Jiang is considered by the police to be head of a small group of cyber-dissidents. His wife hired a Beijing lawyer, Mo Shaoping, who has already defended several dissidents in court.

Blocking access to "subversive" websites

Apart from arrests and heavy jail terms for cyber-dissidents, the authorities also block access to websites they consider "dangerous" or "subversive." This includes not just the rare sites that try, from inside the country, to push progressive ideas, but foreign news sites as well. With the help of Western firms, including Cisco, Nortel and Sun, the government has obtained state-of-the-art technology to block Internet access. Internet firms established in China have applied the government's censorship orders without argument. Yahoo, for example, signed an agreement in 2002 to eliminate "subversive" material.

A survey done by Harvard University's Berkam Centre between May and November 2002, showed that more than 50,000 out of 204,000 websites normally accessible

through the Google and Yahoo search-engines were blocked at least once from at least one point inside China. Apart from explicitly pornographic sites, the most censored (when searched for on Google) included those dealing with Tibet (60 per cent censored), Taiwan (47 per cent) and democracy.

Websites about democracy and human rights, such as Amnesty International, Human Rights Watch and Hong Kong Voice of Democracy, are especially targeted by the censors. Education sites are also strictly monitored, particularly US ones such as Columbia University and the Massachusetts Institute of Technology (MIT), because they host sites run by pro-democracy groups. Sites about religion or health in China are also blocked.

The websites of 923 media, including the *BBC*, *CNN* and *Time magazine*, are regularly blocked, along with the sites of governments, such as Taiwan.

In late March 2001, Internet users in the Shanghai region were banned from putting radio or TV programmes on the Internet without government permission. A month earlier, the public security ministry announced introduction of new software called "Internet Police 110" designed to block sites containing religion, sex or violence. In early May 2001, the state-owned Xinjiang Telecommunications said Internet portals that were not officially registered would be automatically shut down.

The online magazine *Hot Topic* was suspended on 18 June after four years, during which it had posted anti-government articles for its 235,000 subscribers.

The Australian foreign ministry (www.dfat.gov.au), which had been inaccessible from China for more than a year, was unblocked briefly in June during the visit to China of the communications minister Richard Alston. A Chinese government spokesman denied any censorship and said the site had been inaccessible for technical reasons. However, material on the site about human rights and risks of conflict in some parts of China was seen as the true reason for the blocking. In July, the site was again accessible, after the Australian foreign minister protested to the Chinese chargé d'affaires in Canberra.

For several weeks in July, the pages in Mandarin of the *Radio France International* (*RFI*) website were inaccessible and RFI asked the Chinese government for an explanation.

In August two websites close to the Chinese Communist Party – the political newsmagazine *China Bulletin* and *Tianya Zongheng*, an Internet forum based in Haikou (Hainan province) – were shut down for posting criticism of President Jiang Zemin and his policy of economic liberalisation.

The sites of the US TV network *CNN*, the daily paper *International Herald Tribune*, the French radio *RFI*, the British radio *BBC*, the US section of Amnesty International and links on Chinese portals to humanitarian groups such as Doctors Without

Borders were blocked on 4 September on the eve of president Jiang's visit to China's ally North Korea. The sites contained news about famine and repression in that country.

The online newsletter *Baiyun Huanghe* (bbs.whnet.edu.cn) of the Science and Technology University in Huazong (central China) was closed by the government on 6 September after students posted on it articles about the 1989 Tienanmen Square massacre. The site, founded five years earlier, had 30,000 subscribers and focused heavily on politics and corruption. Until it closed, students had been able to discuss on the forum such forbidden topics as the Beijing Spring.

In October, the authorities blocked the websites of hrichina.org (the Human Rights Watch site in China), hrw.org (the main Human Rights Watch site), amnesty.org, amnesty.org.uk and amnestyusa.org (Amnesty International), freetibet.org (the organisation Freetibet), tibet.com (the Tibetan government in exile), *cnn.com* (*CNN*), *bbc.co.uk* (the *BBC*), *washingtonpost.com* (*The Washington Post*), 6-4tianwang.com (the site of cyber-dissident Huang Qi) and *bignews.com* (the dissident online newspaper *VIP Reference*).

The online journalists' forum Zhejiang, hosted by the website Xici.net, was closed by the authorities on 16 October for "putting out subversive information" and "defaming politicians and state institutions." The forum's moderator was dismissed after official pressure and the site managers were obliged to tighten their surveillance of their other forums. The authorities refused to answer questions from foreign reporters about the closure, which happened during the Asia-Pacific Economic Cooperation (APEC) forum in Shanghai.

At the end of US President George Bush's official visit to China on 29 October, the authorities again blocked access to the websites of several US media, such as CNN and *The Washington Post*. However the sites of *The New York Times* and *The Washington Post* were made accessible on 16 October when the APEC forum opened in Shanghai

The Chinese Internet Association, which nationally responsible for supervising the Internet, announced on 16 March 2002 a "self-discipline pact" whose signatories would be banned from producing or passing on material "harmful to national security and social stability." In July, the official *Xinhua* news agency reported that the main Chinese-based websites, including Yahoo, had signed the pact, along with ISPs.

In April, the webmaster of *Voice of America*'s Chinese-language Internet site said it had been attacked from China. E-mails containing specially-designed viruses had been sent to the site and attempts made to hack into it. Dissident websites, such as the Falungong movement and pro-Tibet organisations, were also attacked. Some of the attacks were traced back to accounts belonging to provincial offices of the state-owned China Telecom.

The Australian TV network *ABC* said on 23 April that its website had been blocked by the Chinese authorities and the network filed a complaint with the Chinese foreign ministry against the public security ministry. An Australian embassy official in Beijing said the blocking had been decided at the highest level, but a Chinese government spokesman denied this. The Tibetan Dalai Lama's visit to Australia in May is thought to have been why the site was blocked.

The websites of foreign media, including *Reuters* news agency, *CNN* and *The Washington Post* were accessible again in Beijing and Shanghai on 16 May, though the sites of the *BBC*, *Time magazine* and *The Voice of America* were still blocked. A Western diplomat in Beijing said the Chinese authorities may have realised how easy it was to get round the blocks and that it made more sense for them to allow free access and then watch who consulted them.

In early June, three websites – Tom.com, Sina.com and FM365.com – were reprimanded by the authorities for posting "unsuitable material" about the June 1989 Beijing Spring crackdown. *The Beijing Daily* said the move came after police inspected the offices of nine major Chinese Internet portals. *The Beijing Youth Daily* said police planned to check the content of the 827 main Chinese portals three times a week for the next three months.

Access to the Google search-engine, which had become very popular, was blocked in China on 31 August. Protests filled online forums from people who said they used it to do research, not politics. Chinese and foreign business interests, normally silent about Internet censorship, joined the criticism. "They shot themselves in the foot," said one European working for the Chinese government. Google negotiated with the authorities about the blocking, the reasons for which remained a mystery. Some noted the 14th listed result of a search for the term "Jiang Zemin," which was an interactive game site called "Kill the nasty dictator Jiang Zemin."

Access to another search-engine, Altavista, was blocked on 6 September.

From 7 September, Chinese Internet users trying to access Google were redirected to Chinese search-engines, such as Tianwang and Baidu.

Access to Google from China was restored on 12 September but is now censored. The widespread protests and pressure from business interests is thought to have got the ban lifted. An official spokesman said the ministry of the information industry had "received no information about the blocking of Google and knows nothing about access being restored." Altavista, along with dozens of other sites, is still inaccessible.

Users noticed in September that new detection software had been installed to block access to some pages (about Tibet, Taiwan and human rights) on certain sites. *The South China Morning Post*, published in Hong Kong, reported on 27 September that this censorship also applied to e-mail sent through servers such as Hotmail, search-engines including Google and foreign news sites such as *CNN*. Most of the pages

listed by Google for the Falungong movement were inaccessible. The authorities denied having installed such censorship.

In October, the cybercrime department in the central province of Jiangxi ordered more than 3,000 cybercafés in the province to sell customers access cards, enabling police to check the websites they looked at. One official said the experiment would help prevent crime and spot criminals on the Internet.

In early January 2003, the authorities blocked access to the US site blogspot, which specialises in posting personal diaries and is seen by more than a million people around the world. Site chief Jason Shellen said there were no technical problems and that it was clearly a bid to stop Chinese Internet users looking at the site. But one Chinese fan of blogspot told Reuters news agency the censorship would not work and that bloggers who had something to say would find a way round the ban.

On 14 April, Internet users said the Reporters Without Borders site had become inaccessible in China. This may have been due to the posting of a press release about the lengthy imprisonment of young cyber-dissident Liu Di.

Filters, cleaning and surveillance of online discussion forums

The main news websites have free discussion forums that are visited by hundreds of thousands of people. But the Chinese authorities are turning them into traps for Chinese visitors, who are sometimes arrested after posting anti-government material on them.

Chinese discussion forums use filters to single out and put aside messages containing forbidden words. The poster gets an automatically-generated reply saying (as on xinhuanet.com) that the message has been accepted but will take a few minutes to be revised before being posted. The webmasters are supposed to check to see if the message really is unfit to post, but in practice, such filtered messages hardly ever make it to the forum. "We rarely have time," an official of the sina.com forums told Reporters Without Borders. But "politically-correct" messages containing banned words such as Falungong get through because they criticise the spiritual movement.

A message with a list of words being censored appeared on a sina.com.cn forum on 11 March 2003. The poster had inserted asterisks into each word so it would not be blocked by the filter. The list included "4 June" (date of the 1989 Tienanmen Square massacre),"human rights,""independence of Taiwan,""pornography,""oral sex,""BBC" and "Falungong." The message was removed after only a few minutes.

Messages not containing banned words are posted on the forum and can be seen by everyone. But a group of two or three "ban zhu" (webmasters) check their content at the same time as they run the forum. They are not police or even site employees. Most are young people, sometimes students and usually volunteers. But they have full authority to delete messages considered undesirable. Above them are the "guan

li yuan" (forum administrators), whose job is to ensure good behaviour on the forums. They can suspend or ban users they judge to be rude or politically incorrect. One sina.com.cn official told Reporters Without Borders he preferred to warn users by e-mail first. If they did not change their ways, they were suspended for a week.

At the top of the hierarchy are the Internet monitoring services in the provincial public security departments. It is very hard to find out officially how many clerks, police and computer technicians are involved in such cyber-policing.

An April 2003 survey by Reporters Without Borders showed that two-thirds of all messages submitted were posted on the discussion forums. This dropped to 55% of messages with political content. Of that 55%, more than half were deleted by the web-masters. So only a third of all polemical messages were accepted.

Cybercafés under surveillance

China's semi-legal cybercafés, known as "wang ba," are the most recent targets of the authorities and a vast inspection campaign was launched in early 2001 because only half of them had installed filters (obligatory under the 2000 Internet legislation) to block access to banned websites. The campaign was stepped up in June 2002. Most of the cybercafés (officially put at 200,000) have now been inspected and more than half of them penalised by the authorities. The official *Xinhua* news agency said on 26 December the authorities had shut down 3,000 cybercafés for good and 12,000 temporarily since the start of the inspections.

Red tape and corruption makes it very hard to get licences to run cybercafés, so most are semi-legal.

The deputy head of Feiyu, the country's biggest network of cybercafés (more than 400), said on 5 February 2001 that the network had been ordered to close for three months for failing to hand over to the authorities, as required, records of customers' online activity, including the accessing of pornographic sites, which the regime considers "dangerous." The move followed police investigations in the Beijing suburb of Haidan, where Feiyu has two very big cybercafés, each with more than 800 computer terminals.

On 14 April, the government suspended the opening of new cybercafés for three months to give it time to better regulate Internet access.

On 29 April, the authorities shut down cybercafés on Beijing's main avenue and within a radius of 200 metres around schools and Communist Party buildings in the city.

Police said on 2 July that at least 8,014 cybercafés had been shut down over the previous two months and 56,800 inspected. On 20 November, the newspaper *Wen Hui Bao* reported that more than 17,000 cybercafés had been closed for not having barred access to allegedly subversive or pornographic sites.

The official *Chinese People's Daily* said on 22 August that the culture ministry had asked local authorities to launch a "spiritual cleansing" campaign, partly aimed at shutting down clandestine cybercafés. During a conference in Beijing two days earlier about cracking down on the spread of "corruption and decadence," provincial officials were asked not to issue new cybercafé licences and to punish illegal activity in existing ones.

On 1 February 2002, police in the southwestern city of Chongqing forced cybercafé owners to install filters to block access to websites considered as undermining "public morality."

Between late April and early May, more than 200 cybercafés were shut down in Shanghai for not having licences, according to the official news agency *Xinhua*. Nearly 3,000 cybercafés in the city were inspected.

On 1 May, the government launched a campaign to "restore order" by tracking down "harmful material" on the Internet, mainly by monitoring cybercafés, saying illegal online activity was on the rise.

Officials in the southern city of Guangzhou closed nine unauthorised cybercafés on 3 June and seized their computers.

After a fire at an illegal cybercafé in Beijing killed 24 people on 16 June, the government began a nationwide licence inspection campaign. Thousands of cybercafés were closed and thousands more forced to get new licences. The campaign, officially to check safety regulations, turned into a huge repressive operation that prevented millions of Chinese from going online.

A few hours after the cybercafé fire, for which the two young Internet users accused of being responsible were jailed for life, Beijing mayor Liu Qi ordered all the city's 2,400 cybercafés to close. "Our world has shrunk," said one user during the shutdown, which lasted several weeks. The official *Chinese People's Daily* justified the measure with the headline "Don't let cybercafés destroy our children."

The Beijing Evening News asked its readers to tell the authorities about illegal cybercafés and illegal video parlours. About 30 cybercafés were allowed to reopen on 17 July after publicly promising not to admit users under the age of 18, to close between midnight and 8 a.m. and forbid betting and violent video games.

The city council in Tianjin, north of Beijing, began inspecting all cybercafés on 17 June and the authorities in the southern province of Guangdong suspended granting of new cybercafé licences. In Shanghai, the head of the city's commerce and industry department, Wei Yixin, told the newspaper *Shanghai Daily* that police would swiftly shut down unlicensed cybercafés.

The Information Centre for Human Rights and Democracy said on 28 June that the

authorities were now requiring cybercafé owners to install filters to bar access to as many as half a million websites and to tell police about anyone who looked at allegedly subversive sites. Experts in Beijing said this might refer to the "Filter King" software which is part of the "Golden Shield" project to control the Internet. The public security ministry reportedly plans nationwide installation of the software, which was tested in the northwestern province of Xian in 2001.

A culture ministry official announced on 29 June that all the country's cybercafés would have to register again with the authorities by 1 October or else they would be closed and their owners prosecuted.

On 10 July, the 528 cybercafés in the northern province of Hebei were shut down by the local authorities for what the *Beijing Morning Post* said were security problems. A total of 3,813 cybercafés had reportedly been inspected since 17 June and 2,892 did not conform to security regulations, it said.

On 12 August, the culture and public security ministries, as well as the industry and trade department, banned the opening of any new cybercafé in China but experts said this measure would be hard to apply for very long.

Prime minister Zhu Rongji enacted a new cybercafé law in late September, banning minors and smoking and requiring them to close between midnight and 8 a.m. Owners were also made responsible for what their customers looked at online. It noted that it was a crime to "create, download, copy, send, distribute or look at" material considered "anti-constitutional and harming national unity and the sovereignty and territorial integrity" of China. Owners were required to record and keep for two months the names of their customers and the sites they looked at, or risk fines of up to 2,000 euros. The law came into effect on 15 November.

The Shanghai newspaper *Wenhui Bao* reported on 16 October that 90,000 cybercafés had been shut down throughout the country since the inspection campaign started in June. It quoted the culture ministry as saying that only 46,000 cybercafés had registered so far and that inspections would continue until the end of the year.

Members of Falungong movement persecuted

Followers of the Falungong spiritual movement, dubbed a "satanic sect" by President Jiang Zemin, have protested noisily since the movement was banned in 1999. The authorities have cracked down on it with unusual violence, arresting, torturing and "re-educating" thousands of members, especially those who used the Internet to spread the words of the movement's leader, Li Hongzhi. But the Falungong are very well organised online, both inside China and abroad. At least 16 of its members have been arrested for putting out or having looked at material on the Internet about the movement. Two died of torture while in detention.

Wang Zhenyong, an assistant psychology professor at the Southwestern University,

was arrested on 2 June 2001 after e-mailing four articles about the movement that he had downloaded from foreign websites in December 2000 and sent to a friend who had then posted them elsewhere online.

Falungong member Li Changjun died on 27 June in detention after being tortured, according to the Information Centre for Human Rights and Democracy. He was arrested on 16 May for downloading and printing out material about Falungong. He worked at a tax office in Wuhan (Hubei province) and had been arrested several times already for belonging to Falungong. His mother said he was covered with scars and bruises and was very thin.

Another Falungong member, Chen Quilan, died of a heart attack on 14 August at a detention centre in Daging, in the northeastern province of Heilongjiang. He had been arrested in July for putting material about Falungong on the Internet.

Six members of the movement were convicted on 13 December for posting "subversive material" (about Falungong) on the Internet. Yao Yue, a micro-electronics researcher at Tsinghua University, in Beijing, was jailed for 12 years. Two university teachers, Meng Jun and Wang Xin, were sentenced to 10 and nine years in prison respectively. Dong Yanhong, a university employee, and her husband Li Wenyu, were given five and three years. Wang Xuefei, a student from Shanghai, was jailed for 11 years.

The official news agency *Xinhua* reported on 27 December that Falungong member Quan Huicheng had been sent to prison for three years for downloading, photocopying and passing on material from foreign-based Falungong websites. He had been arrested in October near a cybercafé in Dongfang, on the southern island of Hainan.

The authorities announced on 18 February 2002 that the trial of Tsinghua University students Lin Yang, Ma Yan, Li Chunyang, Jiang Yuxia, Li Yanfang and Huang Kui for posting Falungong material on the Internet would not resume until after US President George Bush's visit to China. Their trial reportedly began in September 2001 before a court in the southern city of Zhuhai.

Cyber-dissidents in prison for disseminating material considered "subversive" by the authorities:

1. Huang Qi
2. Yan Peng
3. Qi Yanchen
4. Yang Jianli
5. Liu Weifang
6. Hu Dalin
7. Wang Jinbo
8. Wang Sen
9. Guo Quinghai
10. Lu Xinhua
11. Chi Shouzhu
12. Yang Zili
13. Jin Haike
14. Xu Wei
15. Zhang Honghai
16. Jiang Shihua
17. Wu Yilong
18. Mu Chuanheng
19. Zhu Ruixiang
20. Li Dawei
21. Chen Shaowen
22. Liu Di
23. Ouyang Yi
24. Li Yibin
25. Jiang Lijun
26. Zhang Yuxiang

LINKS:

• http://iso.hrichina.org/iso
The organisation Human Rights In China

• www.xinhuanet.com
The official news agency *Xinhua*

• www.6-4tianwang.com
Site of jailed cyber-dissident Huang Qi

• www.hrw.org/asia/china.php
Human Rights Watch reports and press releases about China

• www.rand.org/publications/MR/MR1543
"You've Got Dissent! Chinese Dissident Use of the Internet and Beijing's Counter-Strategies"

• dfn.org/focus/china/chinanetreport.htm
News about repression of cyber-dissidents

• www.ichrdd.ca/english/commdoc/publications/globalization/goldenShieldEng.html
Report on the Golden Shield project

• www.faluninfo.net
The Falungong news site

Cuba

POPULATION: 11,237,000
INTERNET USERS: 120,000
PRIVATELY-OWNED ISPS: NO

Internet use is very restricted and under tight surveillance. Access is only possible with government permission and equipment is rationed.

The government says development of computers and Internet resources is a national priority. Computers and communications minister Roberto Ignacio González Planas said in October 2002 that the number of computers in the country had tripled in two years and that fibre-optic cable now linked Havana and Camagüey and would soon reach Santiago, at the other end of the island.

But material restrictions are still the main obstacle to major public expansion of the Internet. There are only four phone lines for every hundred people and the high cost of international calls ($2 a minute to the United States) and the rarity of lines to the outside world, which are assigned on a political basis and closely monitored, effectively prevent any connection through a foreign ISP.

Luis Fernández, spokesman for the Cuban government's Cuban Interests Section in Washington, blames the long-standing US embargo of Cuba for the dearth of equipment. "If we didn't have to cope with that, everyone would have computers by now," he says.

This dodges the fact that the necessary equipment, including the most modern, is available in special government-run shops but only for authorised people. It also ignores the internal trade ministry's January 2001 ban on the sale to individuals in these state-run shops of computers, printers, copying machines and "all other means of large-scale printing." If such a purchase is deemed vital, permission must be sought from the ministry. The general sale of modems was banned. So the Internet in Cuba is a very limited affair, even though Cuban computer firms are perfectly familiar with all aspects of the technology.

Priority for institutions

The government passed laws as soon as the Internet appeared in Cuba. In June 1996, Decree 209 (entitled "Access to the World Computer Network from Cuba") said it

could not be used "in violation of the moral principles of Cuban society and its laws" and that Internet messages must not "endanger national security."

Cuban who want to log on to it or use public access points must have official permission, and give a "valid reason" for wanting to and sign a contract listing restrictions. Decree 209 says access is granted "with priority given to bodies and institutions that can contribute to the life and development of the country." Apart from embassies and foreign companies, this means political figures, top officials, intellectuals, academics, researchers and journalists working for the government, managers of cultural bodies geared to exports, computer firms and the Catholic hierarchy. Cuban export firms have access to national e-mail and the local Intranet.

A ministry of computers and communications was set up on 13 January 2000 to "regulate, manage, supervise and monitor" Cuban policy on communications technology, computers, telecommunications, computer networks, broadcasting, radio frequencies, postal services and the electronics industry.

Beatriz Alonso, head of Citmatel, one of the country's two ISPs, said in the official daily *Granma International* on 18 June 2001 that "Internet use by our institutions means having access to information we need in today's world. We don't have the sites about pornography, terrorism and other evils that are common in capitalist countries, especially the United States. Internet use in Cuba is based on ethics and humanism. We encourage exchange of information for our professionals and technicians, publicise Cuba's development achievements and give our schoolchildren and students sources of knowledge."

The country's two servers are Citmatel and CenaInternet, a branch of the ministry of science, technology and the environment, and Infocom, which belongs to the Italian-Cuban telecommunications firm Etecsa.

E-mail under close scrutiny

A black-market in e-mail addresses has developed for the few Cubans who have a computer. A Monitoring and Supervision Agency was set up on 1 January 2001 in the ministry of computers and communications to track down people who "improperly" used the Internet. Its head, Carlos Martínez Albuerne, said in an article in the daily paper *Granma* on 23 April 2003 that in 2002, sanctions had been taken against 31 people for this reason or for "using e-mail addresses that did not belong to them." He did not say what the punishment was.

Where e-mail is concerned, obeying the rules means agreeing to be monitored. Since September 2001, Cubans have been able to access from the Etecsa centres a special national e-mail service without connecting to the Internet. An ID card to use this service costs $5 for four hours (the average Cuban monthly wage is about $10). The applicant must prove identity, fill in a long form and give an address. The ISP can thus monitor beforehand all messages being sent or received and decide whether to

deliver them. Some users have noticed delays in their e-mail, which sometimes even "disappears," especially when sent or received from abroad.

Vicenç Sanclemente, former Havana correspondent for the Spanish TV station *TVE*, tells how in 1999, he was worried he had not received any e-mail at his office because he was expecting an important message from the Dominican Republic. He contacted the communications ministry technician who had set up his e-mail connection, fearing there had been a technical problem. The official told him he had not turned on the computer at his home for the past few days and informed him that waiting for him on it were "three messages from the Dominican Republic, two from Barcelona, one from Montse and another from Margaret."

Access to cybercafés is restricted for Cubans. Visiting foreigners who show their passports can now access the Internet in Havana's two cybercafés, while nearly all the city's big hotels have an Internet centre. Etecsa is also increasing the number of phone and Internet access points in Havana and provincial towns for use by foreigners and authorised Cubans. Web-surfing is unrestricted at these access points, although ISPs can, and do from time to time, block access to some sites.

Modem links are adequate but the cost of connection is prohibitive – at least $8 an hour, compared with the Mexico and the Dominican Republic, where high-speed links cost only $2. So very few people go online.

Members of the National Writers' and Artists' Union (UNEAC) have their own cybercafé, El Aleph, at the Book Institute in Havana, where they can do e-mail and access a national Intranet which carries officially-approved websites.

The government is setting up through youth organisations about 300 Internet clubs around the country and increasing the number of computer training courses. When these centres are connected up, Internet access will be restricted to the officially-approved sites.

A window of freedom...

Despite the very tight control, the Internet is opening a window of freedom in Cuba and the audience of the country's independent journalists has expanded. The creation abroad (mainly in Miami) of websites or web pages carrying news they send out by phone or fax means wide distribution for material they still cannot publish in Cuba. Their articles are now stored and accessible to the whole world when before they were only to be fleetingly heard on *Radio Martí* (US government-funded and operating from the US), which is not picked up easily in Cuba.
News such as the arrest of a regime opponent, a social trend among the population or initiatives by civil society groups – things that used to be ignored abroad – are thus now immediately reported to the outside world and increasingly reproduced by the international media, a sign of the independent journalists' growing credibility and professionalism.

However, the spread of even a small amount of new technology and Internet access has led to a limited but well-organised black market. Some registered users rent out their log-on names and passwords for about $60 a month (equal to about six months salary), while others bring customers to their private point of access and charge for time online. Staff at the Etecsa centres, who have a password to connect up tourists and registered users, give friends and relatives demonstrations of the Internet and sometimes charge for it.

Some Internet users have reportedly managed to smuggle into the country receiver dishes and modems to connect to big US-based satellite ISPs such as Starband and DirecPC, with the cost paid by relatives in the US ($500 for signing up and $100 a month subscription).

...closely watched

José Orlando González Bridón, secretary-general of the illegal Cuban Democratic Workers' Confederation (CTDC), was arrested on 15 December 2000 and became the first opposition activist to be sent to prison for publishing something on the Internet. In an article that had appeared on 5 August that year on the Florida-based *cubafreepress.org* site, he had blamed police for the death of the CTDC's national coordinator, Joanna González Herrera. He was accused of "subversion" for also having sent the article to a Miami radio station.

He was freed on parole on 22 November 2001 three weeks before the end of his sentence, officially for "good behaviour." He said he thought he was really released then because the government wanted to make a public relations gesture on the eve of the 23-24 November Ibero-American Summit in Peru of 23 heads of state from Latin America, Spain and Portugal. He was also let out a week before a meeting in Havana to restart political talks with the European Union (EU), which since 1996 has conditioned its aid to Cuba on increased respect for human rights and political freedom. At the time, Cuba was keen to join the Cotonou Agreement between the EU and the Africa-Caribbean-Pacific (ACP) group of countries.

González Bridón said he was held in prison at Combinado del Este (Havana province) in a punishment cell where the toughest prisoners were normally sent for maximum three-week periods. He was kept apart from other prisoners for 10 months and his only piece of furniture was a bed brought to his cell at 6 in the evening and taken away again at 6 in the morning. His wife Maria Esther Valdés was only allowed to visit him every three weeks. The prison authorities refused to give him a special diet he needed to control his high blood pressure, but he managed to avoid serious health problems.

He said he had witnessed brutal treatment of prisoners and had denounced corruption at the prison, where prisoners paid guards to get better conditions or obtain drugs. His trial took place on 24 May 2001 after several postponements. Foreign media and regime opponents were kept away by heavy security and only his family was allowed

to attend. The rest of the public gallery was filled with police. He was sentenced on 2 June to two years in prison for "putting out false news harming the reputation and image of the Cuban state" with "clear intent to collaborate with a foreign power."

At an appeal hearing on 21 August, the charges against him were altered to "denigrating institutions, organisations and heroes and martyrs" and the sentence was reduced to a year's imprisonment. Friends said the Internet article was used as an excuse by the authorities to punish him for his overall anti-government activity.

LINKS:

Sites carrying articles by independent journalists inside Cuba:

- www.cubanet.org
- www.nuevaprensa.org (in Spanish)
- www.cubaencuentro.com (in Spanish)
- www.cartadecuba.org (in Spanish)

- www.cubaweb.cu/esp/categorias/categories.asp?categoryID=60
Government "Internet and Institutions" portal

- www.cubaweb.cu/esp/categorias/categories.asp?categoryID=20
Government media portal

Denmark

POPULATION: 5,333,000
INTERNET USERS: 2,500,000
PRIVATELY-OWNED ISPS: YES

In October 2001, soon after the 11 September attacks, the government moved to fight terrorism with a legislative package that rewrote laws about justice, internal affairs, the economy and taxes.

It asked the justice ministry to take steps to legalise retention of phone, e-mail and Internet connection data and to see that police had faster and easier access to such personal information. The 31 May 2002 anti-terrorist law extended the minimum time for data retention to a year and allowed police and intelligence agents to look at such material with court permission where serious crimes were involved and to install on ISP servers software similar to the US Carnivore system to record key-strokes and intercept e-mail.

The Danish presidency of the European Union (EU) tried to impose this approach on other member-states when it made a proposal on 24 June 2002 called "information technology related measures concerning the investigation and prosecution of organ-ised crime." It said all member-states would soon have to take steps to oblige phone companies and ISPs to retain all their traffic records "so security services can readily consult it in the course of their investigations."

In September 2002, the government tempered its restrictive measures by setting up a commission to safeguard citizens' computer rights which was due to make proposals in June 2003.

LINKS:

• www.digitalrights.dk
The organisation Digital Rights

• www.datatilsynet.dk
The data protection agency Datatilsynet

Egypt

POPULATION: 69,080,000
INTERNET USERS: 600,000
PRIVATELY-OWNED ISPS: YES

The authorities tightened their control of the Internet in 2002 by setting up a government department to investigate online crime.

The Internet has grown faster in Egypt than in most Middle Eastern countries. Introduced in 1993, it has been available to the public since 1995 and since then has steadily grown more popular.

The communications and information technology ministry ended the monopoly the state had exercised through Telecom Egypt and opened up the sector in early 2002 with a scheme allowing ISPs to assign special phone numbers to users with a computer and modem. The customers were not obliged to commit themselves to one ISP. The aim was to boost the number of Internet users and get Egyptians used to new technology.

The country's traditional media is closely watched, but until recently no specific laws applied to the Internet. But in September 2002, the interior ministry set up a department to investigate computer and Internet crime and its director, Ahmed Essmat, told *Al Ahram* that his staff monitored the Internet daily.

At the end of 2001 and early 2002, Internet users were warned off taboo issues (such as relations between Copts and Muslims, publicising terrorist ideas, human rights violations, criticising the president, his family and the army and promoting modern versions of Islam) and told that too much outspokenness was unwelcome.

Moreover, when 52 homosexuals were tried by the state security court at the end of 2001, the gay community's websites were targeted by police. One even put a notice on its homepage saying: "Guess who's watching us? The state security police!"

Traps were set up by the police. Two men made rendezvous with visitors through gay sites who turned out to be policemen, who arrested them.

In mid-December 2002, the Egyptian Initiative for Personal Rights (EIPPR) expressed concern about a new communications bill, noting that its article 65 was

very vague in allowing the army, police and state security officials to access any communications network "for reasons of internal security." These objections resulted in amendments to the bill, which was adopted at the end of the month. Article 65 now says citizens have a right to privacy and says security agencies can only intercept private communications "in accordance with the law." They must obtain a court order to do so which is limited to 30 days and is only to be granted in connection with serious crimes or offences punishable by more than three months in prison.

Tried for putting a 30-year-old poem online

Shohdy Surur, webmaster of the English-language *Al Ahram Weekly*, was sentenced to a year in prison on 30 June 2002 for posting on another website a sexually-explicit, socially critical poem written by his late father 30 years ago.

Article 178 of the penal code forbids possession of material for sale or distribution "with intent to corrupt public morals." Surur had posted on wadada.net, which is partly devoted to the work of his poet and actor father Naguib, a poem called Kuss Ummiyat, which contained passages said to be "an affront to public morals."

The poem was written by the elder Surur in earthy and sexually-explicit language, as a criticism of Egyptian society and culture after the country's defeat in the 1967 Six-Day War with Israel. He several times likened Egypt to a prostitute. Since no law refers to the Internet, the state brought charges under the law on public morals.

The poem had been on the US-based wadada.net for the previous three years. Its author, who died in 1978, was never prosecuted for writing it. Shohdy Surur was arrested on 22 November 2001 at his home, which was searched and his computer seized. Police interrogated him for three days. The prison sentence on Surur, who has dual Russian and Egyptian nationality and lives in Russia, was confirmed by an appeals court on 14 October 2002.

A 19-year-old student, Andy Ibrahim Shukri, was arrested, tried and sentenced in April 2002 to a month in jail for "putting old false information" after he had sent e-mail messages about a serial killer on the loose in Cairo.

LINKS:

• www.eohr.org.eg/
The Egyptian Organisation for Human Rights

European institutions

The European Union was once firmly opposed to any form of large-scale generalised or exploratory electronic surveillance, but it changed its position after the 11 September attacks. Its Council won a battle to impose the views of the 15 member-states on the European Parliament and push through laws to require systematic retention of data about telecommunications and Internet activity.

Until late summer 2001, the official policy of the 15 member-countries of the European Union (EU) about regulation of cyberspace dismissed any idea of systematic retention of Internet connection records and monitoring Internet activity. The 11 September attacks changed that.

In mid-October, US President George W. Bush urged Belgian prime minister Guy Verhofstadt, who was EU president at the time, to get a proposed amendment to the Directive on Protection of Telecommunications Data and Information altered to require "preventive retention" of data on Internet activity (traffic logs) as a means to fight terrorism. Bush expressed support for the British government (which, like the French, has introduced such data retention) and various EU police officials calling for new powers to monitor phone and Internet activity more effectively.

Bush told Verhofstadt the United States was against automatic deletion of Internet connection records, a principle that was upheld in the proposed amendment. This position clashed with that of the European Parliament's Citizens' Freedoms and Rights Committee, which in July 2001 had approved a preliminary report by Radical MEP Marco Cappato for strict supervision of police access to traffic logs retained by phone companies and ISPs.

Surveillance forbidden

The Cappato report said that if such practices were to be allowed, EU member-states should be obliged to act under "a specific law comprehensible to the general public." The measures would have to be "entirely exceptional, authorised by the judicial or competent authorities for individual cases and for a limited duration, appropriate, proportionate and necessary within a democratic society." They should also be in line with EU human rights rulings, which forbid all forms of "wide-scale general or exploratory electronic surveillance."

But under intense pressure from the Council of the European Union (that groups all

member-states) and despite energetic lobbying by many NGOs, Euro MPs approved the amended directive on 30 May 2002. Its article 15.1 obliges governments that do not yet have such legislation, to pass laws (within 15 months) to force ISPs and phone companies to retain all records of e-mails, Internet activity, faxes and phone calls that have passed through their hands and guarantee the police, the courts and some government bodies free access to it.

A report by the Council of 15's legal department released on 15 October 2001 had said however that EU governments already had the necessary powers to intercept telecommunications to fight terrorism.

Convention on Cybercrime

The first International Convention on Cybercrime was opened for signature in November 2001 in Budapest. It details various procedures, such as searching computer networks and intercepting messages. The pact, which was four years in the making, comes into effect when ratified by at least five countries, three of them Council of Europe members. It has so far been signed by 34 countries, including the United States, Canada, Japan and South Africa, but only two (Albania and Croatia) have ratified it.

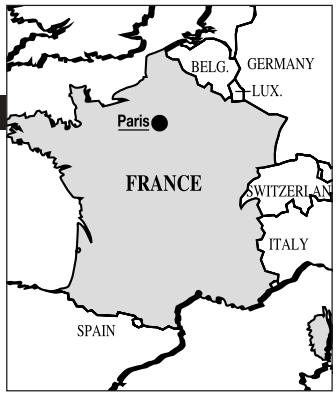
The agreement was attacked by civil liberties campaigners, ISPs and cyberspace experts who called it anti-freedom, meddling and likely to encourage a new era of generalised surveillance. Especially criticised were its articles 19, 20 and 21, which give details of how to gather private Internet data and traffic logs and information of interest to security services for their investigations; gather records kept by ISPs; search websites and their ISPs and extend such searches to other computer networks if necessary; store the data seized; and if necessary gather in real-time records and traffic logs (with legal officials able to require ISPs to do this work themselves).

"Generalised surveillance" of Europeans

The situation may get even worse. The Danish presidency of the EU proposed a measure on 24 June 2001 that the Council of the European Union might adopt. It was called "information technology related measures concerning the investigation and prosecution of organised crime" and said that "in the near future, all member-states will need to have adopted suitable measures to oblige telephone companies and ISPs to retain all records of their traffic so security services can readily consult it in the course of their investigations." The proposal also aims to standardise the laws of all European countries, including those seeking to join the EU.

LINKS:

- www.europarl.eu.int: The European Parliament
- www.coe.int: The Council of Europe



France

POPULATION: 59,453,000
INTERNET USERS: 18,716,000
PRIVATELY-OWNED ISPS: YES

New laws to fight terrorism and cybercrime are threatening the protection of news and journalistic sources.

The government's anti-terrorism measure, the Law on Everyday Security (LSQ), urgently approved almost unanimously by parliament without discussion on 15 November 2001, extended to a year the minimum period ISPs must keep a record of their customers' Internet activity and e-mail traffic.

The law allows judges to use "secret methods that cannot be revealed for reasons of national defence" to decode e-mail messages and requires encryption firms to hand over their codes so the authorities can read the messages. Campaigners for freedom of expression protested against such hasty passage of a measure that had not been discussed or negotiated and which threatened the principle of confidentiality of professional and private communications.

Another measure, the Internal Security Policy and Planning Law (LOPSI), passed on 31 July 2002, allows police detectives to make remote online searches of ISPs with prior court permission and have "direct access to data considered necessary to establish the truth."

A bill on the digital economy (LEN), presented on 15 January 2003 to incorporate into French law the 2000 European directive on e-commerce, contains a clause about the civil and criminal responsibility of ISPs that France's Constitutional Court had struck out of a bill on the information society drafted by the previous government in 2001.

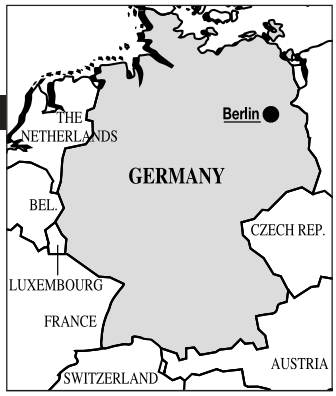
The clause (article 2) relieves ISPs of civil and criminal responsibility if they had "no knowledge of illegal activity or material" or if they "acted promptly to remove or block access to it as soon as they discovered it." ISPs are also exempted from civil responsibility if they "have no knowledge of how the illegal activity or material arose." These conditions encourage harassment by pressure groups and open the way to private censorship and self-censorship by ISPs. The bill was passed on a first reading by parliament on 25 February.

LINKS:

• www.iris.sgdg.org
The organisation Iris (“Let’s Imagine an Internet of Solidarity)

• www.cnil.fr
National Commission on Cyber-freedoms

• www.internet.gouv.fr
Key official documents



Germany

POPULATION: 82,007,000
INTERNET USERS: 35,000,000
PRIVATELY-OWNED ISPS: YES

The Internet For All programme launched in 2000 by Chancellor Gerhard Schroeder is a big reason for the broad success of the Internet, but this concerted effort is accompanied by strict laws.

A July 1996 law requires ISPs to give the secret services access to their Internet traffic and one in August 1997 makes them responsible for the content of the sites they host, although only if they are aware of it.

The G-10 law, which limits protection of communications, was amended in 2001. ISPs were asked to give the secret services every facility to monitor or intercept national or international electronic or voice communications. The ISPs were also strongly advised to "police" the content of websites. The law includes a long and generalised list of crimes justifying Internet surveillance covering not only suspects but anyone who might have had contact with them.

The 11 September attacks led to an anti-terrorist law pushed through parliament by interior minister Otto Schily at the end of 2001. The Telecommunications Interception Order, which came into force in January 2002, allows intelligence officials and police to access traffic records stored in digital form, including details of services used by customers, e-mail exchanges, data enabling senders or users to be identified and the records of telecommunications firms.

Twenty or so civil rights, freedom of expression and personal data protection organisations formed a coalition to condemn such surveillance. They said the law would not stop terrorism and criticised the legal concept behind the measures.

The media revealed in June 2001 that the government had allowed the country to become a link in the US Echelon electronic spy network. The Bavarian daily paper *Merkur*, which published a US military intelligence report, said the US base at Bad Aibling (Bavaria) housed one of Echelon's biggest European electronic monitoring and interception centres, after the US base at Menwith Hill, in Britain. It enabled the US to spy on e-mails sent from much of Europe, including all the former Soviet bloc.

The disclosure caused an especially big stir in Germany because the country was not

a signatory of the UKUSA agreement, which organises the sharing out of surveillance work between the US, Britain, Canada, Australia and New Zealand.

The North Westphalia provincial authorities began compiling a blacklist of websites in October 2001 and asked more than 80 local ISPs to block access to them using software developed by the firms Bocatel, Intranet and Webwasher. On 8 February 2002, for example, they asked for two US-based neo-Nazi websites to be blocked. The German Association to Protect Electronic Rights (FITUG) and many Internet users have protested at this censorship, which affects communication infrastructures themselves more than it does the authors of website material that violates the Constitution or human rights. Internet users fear the filtering will be extended to other parts of the Web. The blocks are easily got round by accessing the sites from another province in Germany.

LINKS:

• www.bundesregierung.de
The federal government

• www.fitug.de
The German Association to Protect Electronic Rights (FITUG) (in German)

India

POPULATION: 1,025,096,000
INTERNET USERS: 16,580,000
PRIVATELY-OWNED ISPS: YES

The Internet's promising future in India is hampered by poor quality phone lines and pressures from the government. Two laws, one of them passed after the 11 September attacks, allow monitoring of the Internet and criminalises much activity by users.

Parliament approved the Information Technology Act in May 2000 to crack down on cybercrime, which it defines as unauthorised access to electronic data. Hacking is punishable by up three years in prison and heavy fines. Cybercafés and the homes of Internet users can be searched at any time without a warrant if cybercrime is suspected and those who set up "anti-Indian" websites can be jailed for five years.

The press revealed in March 2001 that police and government agencies were regularly harassing ISPs to provide personal information about their customers. The head of one of the biggest ISPs, Rediff.com, said he was being approached about once a month but refused to cooperate. The boss of Satyam Infoway, another major ISP, said he was under constant pressure of this kind.

Registration of cybercafé customers

The strict legal regulation of the Internet allows prosecution of anyone violating what the government considers moral and political rules. In April 2001, police investigated pupils at one of New Delhi's biggest schools, accusing them of creating a "pornographic" website featuring their teachers and classmates. The probe began after the father of one pupil saw the name of his daughter on the site.

The authorities regularly condemn pornographic sites as the plague of the Internet, but they are hugely popular with customers of the cybercafés that are opening everywhere in major cities. Cybercafé owners make a goodwill gesture to the government by displaying warning notices to discourage their young customers.

Police in Mumbai announced in May 2001 that anyone wanting to use a cybercafé there would need to show an ID, driving licence or student card or for foreigners a

passport or plane ticket. Customers deemed bona fide would be given a special card they could use on each visit. Cybercafé owners opposed the measure, but the authorities argued that they received some 50 complaints a day about credit card fraud, hacking, supposed terrorist activities or pornography on the Internet.

In June 2002, the Indian Intelligence Bureau reportedly asked the American FBI to help it develop software to tap into mobile phones and e-mail messages of members of criminal and terrorist groups. The news site rediff.com said talks were going on to establish this link between the two intelligence agencies.

Confidentiality of journalists' sources under threat

In November 2001, an anti-terrorist law (the Prevention of Terrorism Ordinance – POTO) was passed in the wake of the 11 September attacks, allowing the government to monitor all kinds of electronic communications, including personal e-mail, without legal restriction. Evidence gathered this way can be used in court against a suspect. In an attempt to justify its anti-terrorist and anti-cybercrime policy, the government said it would share this information with the US intelligence services.

As important users of the Internet, journalists were especially targeted in the first draft of the new law, which proposed jail terms of five years for failure to give the authorities information about terrorists or terrorist organisations. After protests by the opposition and human rights and freedom of expression activists, this clause, obliging journalists to reveal their sources, was dropped and law adopted for a period of three years instead of five.

Tehelka brings down the defence minister

This attempt to control the Internet did not however prevent people from using it as a new vehicle of press freedom. In March 2001, a news site called *Tehelka* (which means "great excitement" in Hindi) lived up to its name. Investigative journalists, equipped with video cameras and pretending to be arms merchants, revealed that politicians, civil servants and top army officers had accepted bribes and the services of prostitutes in exchange for helping businessmen get government and especially military contracts. This corruption enquiry rocked the political class and the government itself and defence minister George Fernandes and the president of the ruling Bharatiya Janata Party, Bangaru Laxman, were forced to resign.

The scandal highlighted the possibilities of the Internet as a new medium, but also drew a repressive reaction. The editor of *Tehelka* complained of efforts by the prime minister's office to discredit the site, accusing it being in the pay of Pakistani intelligence and organised crime. The journalists who broke the scandal were physically threatened and had to be given heavy police protection.

About 20 intelligence agents from the Central Bureau of Investigation (CBI) searched the New Delhi offices of *Tehelka* on 26 June 2002, as well as the home of one

of its journalists, Kumar Badal. He was accused of hiring two poachers to film and kill two of a protected species of leopards in the jungle in Saharanpur, in the northern state of Uttar Pradesh. But the CBI could not produce any incriminating evidence from among the material they had seized in their searches.

However, the agents reportedly confiscated papers about the founding of the website, including e-mails from Shankar Sharma, owner of the company First Global and the first to bankroll the operation, who is now in prison.

The searches were ordered a few hours before the website's chief editor, Tarun Tejpal, was due to give evidence to the Venkataswami Commission set up by the government to look into the corruption revealed by the site. The hearing of Tejpal, set for the same day as that of the former president of the Samata party, Jaya Jaitly – the alleged contact between the defence minister and the arms dealers – was postponed.

The website's lawyer, Kavin Gulati, said the enquiry had reached a crucial moment of cross-examining witnesses, which suggested that the date of the search was deliberately chosen. A CBI spokesman said it was "sheer coincidence."

Badal was arrested on 3 July and went on hunger strike for several days in protest against his imprisonment. He was being held under the Wildlife Protection Act and was humiliated in various ways. "I've been subjected to all this just because I work for *Tehelka*, which is determined to expose high-level corruption," he said.

He was freed on 13 January 2003 on bail of 50,000 rupees (nearly 1,000 euros) by a simple decision of the supreme court. But federal police vainly tried to block his release, saying investigations were not yet complete. Badal was put under house arrest in New Delhi and has to report to the CBI on the first Monday of each month. He was also banned from going to the Saharanpur district, where the complaint against him was filed.

The harassment of *Tehelka* partly explained why the site announced in early 2003 it could not longer keep up a daily edition. Tejpal said that despite the reputation the site had gained and the praise it had received, *Tehelka* had been relentlessly victimised because of its revelations about the military. For two years, the staff had been harassed and arrested, and had shrunk from 120 to three, and the site's debts had mounted. He said he hoped the site would eventually return to help build free media in India.

Journalist jailed for downloading material from the Internet

Police in New Delhi charged journalist Iftikhar Gilani, New Delhi bureau chief of the *Kashmir Times* and correspondent for the Pakistani daily *The Nation*, with spying for Pakistan on 7 September 2002 by passing on details to Pakistani officials of the position of Indian troops and paramilitary forces in Kashmir. The charges were based on clauses of the Official Secrets Act and also articles of the Penal Code relat-

ing to criminal conspiracy and pornography. He had been arrested on 9 June.
After first accusing him of financial irregularities, spying and involvement in pornography, police then said he had downloaded a document from the Internet about the fighting in Kashmir and had admitted it was to be handed to Pakistan. This material was available to any member of the public, but the judge in charge of the case said she had not had time to look at the website in question to check. Gilani said he had been beaten by other detainees at Tihar prison, near New Delhi, and refused access to the library. His several requests for release on bail were rejected.

An army intelligence official told a judge on 23 December that no secret information had been found on Gilani's computer, obliging the government to drop prosecution of him and ask for his release. When he came out of prison on 13 January 2003, he called on journalists and politicians to see that the state secrets law was repealed.

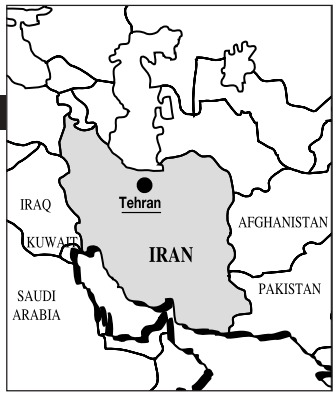
LINKS:

• http://tehelka.com
The independent news site *Tehelka*

• www.dotindia.com
The Department of Telecommunications

• www.flonnet.com
The independent magazine *Frontline*

• www.dqindia.com
The computer magazine *Dataquest*



Iran

POPULATION: 71,369,000
INTERNET USERS: 1,005,000
PRIVATELY-OWNED ISPS: YES

With the regime's closure of nearly 100 newspapers since April 2000, the Internet has become the means for journalists to speak out freely and call for more freedoms and reforms in the country. Both the regime's hardliners and the reformers, horrified by the new tool, have strengthened their control of the Internet. Several people running websites have been arrested since January 2003, along with Internet users.

Privately-owned ISPs began operating timidly in 1994 in the shadow of the big government-controlled ISP, Data Communication Company of Iran (DCI), run by the intelligence ministry. Internet fans were heartened when the reformist Mohammad Khatami became president in 1997.

With the shutdown of nearly 100 newspapers since April 2000, the reformists set up websites such as *Emrooz*, *Rouydad* and *Alliran*. Women's sites, such as Zanan Iran and Zan, were also founded. In 2002, Iranians, especially young people and women, became enthusiastic about weblogs, personal sites where they can get round the censors by using a false name. This passion for the Internet (with at least 1,500 cybercafés in Teheran alone) quickly scared the regime, which took steps to control it.

Privately-owned ISPs must get permission to operate from the ministries of intelligence and Islamic guidance and use filters on website viewing and e-mail messages. Each user has to sign a statement promising not to look at "non-Islamic" sites.

Owners of cybercafés, which are very popular with young people, students and intellectuals, especially in the capital, ask their customers to disconnect if they catch them looking at "non-Islamic" sites. Anti-government sites are based abroad and are much visited by Iranians who manage to get around the censorship.

Measures to stifle the Internet

The regime stepped up its control of cybercafés in May 2001, closing 400 of them in Teheran. Some have since reopened, but in November that year, the Supreme Council of the Cultural Revolution, chaired by President Khatami but dominated by

hardliners, ordered all privately-owned ISPs to shut down or put themselves under government control.

Intelligence minister Ali Yunessi, on 2 January 2003, denounced the "underground war" he said was being waged through websites that "put out rumours and disinformation about all government bodies and their officials."

A commission of officials from the culture and intelligence ministries and the state-run radio and TV was set up that month to compile a list of news sites considered "illegal." It was to be handed to the posts and telecommunications ministry, which would pass it on to ISPs, who would block access to them. The list is thought to contain between 100 and 300 websites, most of them sources of news.

In early May, the country's prosecutor-general, Abdolnabi Namazi, announced a new commission to deal with offences committed online. He said people who posted material on sites created in Iran "must respect the Constitution and the press law or else risk being prosecuted. Until we have a law about Internet offences," he said, "courts can use the press law," which provides for heavy prison sentences. The commission's main job is to draft an Internet law.

Deputy posts and telecommunications minister Massud Davari-Nejad said in May that the ministry had moved to block access to "immoral sites and political sites that insult the country's political and religious leaders." So when people try to access an "illegal" site, they are cautioned that "on orders from the posts and telecommunications ministry, visiting this site is not permitted."

Measures were also taken against ISPs. Five privately-owned ones in the northern city of Tabriz were shut down in early May because they had not installed filters against banned sites. Most of the ISPs still operating there were government-controlled. At least seven ISPs were also closed down in Teheran for the same reasons.

The hardliners were not the only ones trying to control the Internet. In May, two reformist figures, government spokesman Abdollah Ramezanzadeh and posts and telecommunications minister Ahmad Motamedi, warned ISPs to apply the new rules and said the system of filters was quite legal.

Webmasters and Internet users arrested

Javad Tavaf, editor of the news website *Rangin Kaman*, which for a year had been criticising the Guide of the Islamic Revolution, Ali Khamenei, and was very popular, was arrested at his home on 16 January 2003 by justice ministry officials. He was freed two days later.

Mohamed Mohsen Sazegara, editor of the news site *Alliran*, was arrested on 18 February at his home by plainclothes state security agents and his house and office searched and a large amount of written material seized. A week earlier, he had

posted an article on his website calling for a reform of the Constitution. He also wrote that the wishes of Iranians had been "hijacked by six religious figures on the Council of Guardians," a body controlled by hardliners and appointed by Khamenei, which supervises elections and ratifies laws. He was freed a few days later.

Nearly 70 schoolchildren were arrested in Teheran in March for using the Internet to organise dates and forbidden sexual relations. They were freed a few days later.

Sina Motallebi, a journalist with the reformist daily *Hayat-é-No* and editor of the website *Rooznegar*, was arrested on 20 April after being summoned the previous day by the Teheran police's morality section, Adareh Amaken, which is close to the intelligence services. After the closure of the paper in January, he had revived the website and used it to defend one of the paper's journalists, Alireza Eshraghi, who had been arrested on 11 January. The site, which especially defends imprisoned journalists, had angered some legal officials and also a number of reformists by criticising them for their silence about the arrests of journalists. He was freed on 12 May.

The Internet also used as a propaganda tool

The hardliners' distrust of the Internet does not stop them using it to spread their own propaganda, with sites such as daricheh.org and jebhe.com. The religious city of Qom also turns out several thousand students each year trained in computers and the Internet who are supposed to use their knowledge to serve the country and further Islam.

LINKS:

News sites:

- www.daricheh.org
- www.jebhe.com (in Persian)
- www.emrooz.org (in Persian)
- www.rouydad.com (in Persian)
- www.alliran.net (in Persian)
- www.ranginkamaan.blogspot.com (in Persian)

Women's sites

- www.womeniniran.com/english.htm
- www.zan.org

Iraq

POPULATION: 23,584,000

The fall of President Saddam Hussein's dictatorship in April 2003 after the US-British invasion raised many hopes of change for the country's media, especially concerning Internet activity.

Under the old regime, all news was controlled by the authorities and the media was censored. Internet access was likewise the monopoly of the country's sole ISP, Uruklink, which was an arm of the ministry of culture and information.

Iraqis could only go online at 26 "Internet centres" around the country. Private or home connections were not available. Foreign experts said this was because the authorities had not yet mastered the use of programmes to screen and block access to websites.

Staff at the "Internet centres" told foreigners not to try to connect to their personal e-mail sites, since Hotmail and a very large number of foreign sites and portals were inaccessible, according to a *BBC* journalist, who said looking for a way round this was a real challenge. Officials from the government's Internet department prowled the centres and if they spotted anyone trying to connect to a banned foreign site, they cut off the line and asked you to leave.

But the regime's main weapon in curbing Internet access was the high cost of connection. An hour online cost one dollar, and someone who worked for the government (the main source of employment) only earned five dollars a month.

In the Kurdish part of the country, the situation was very different, with much greater media freedom and much more Internet activity and access.

LINK:

• www.iraqpress.org
Independent news agency

Italy

POPULATION: 57,503,000
INTERNET USERS: 17,000,000
PRIVATELY-OWNED ISPS: YES

After the 11 September attacks, government efforts to reform the country's intelligence services and fight cybercrime led to a substantial increase in monitoring of the Internet.

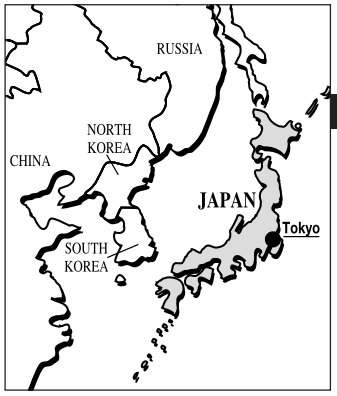
The government pushed through parliament at the end of 2001 a reform of the national intelligence services, which allowed the civil (SISDE) and military (SISMI) secret services, as well as the carabinieri and the regular police, to install phone and electronic taps simply with permission from the state prosecutor. The inherent secrecy of these special services hides the exact nature of the surveillance, but privacy and confidentiality protection organisations have strongly criticised the measure.

Italy, which held the presidency of the informal G8 group of countries at the time of the 11 September attacks, also laid the first stone, in a government statement on 19 September 2001, of a policy of "fighting Internet and high tech crimes." This led to strengthening the powers, resources and activities of the G8 group.
Experts at the June 2002 G8 meeting in Canada of eight heads of government said the G8 network of originally 16 (now 26) countries enables speedy cooperation between international police forces when urgent response is required to high tech crimes, including e-mail messages between terrorists and other criminals.
The G8 meeting noted that legal experts and police had developed ways to detect the origin, destination and routing of terrorist and criminal messages on the Internet, ways to get electronic proof of it and to ensure retention of such evidence so that it was not deleted or altered.

Internet freedom organisations have especially protested about the controversial amendment of the European Directive on Protection of Telecommunications Data and Information (see section on the European institutions) approved on 30 May 2002 and authorising member-states to retain phone and Internet connection records (traffic logs).

LINKS:

• www.alcei.it: Electronic Frontier Italy
Association for Interactive Electronic Communication Freedom (ALCEI-EFI)



Japan

POPULATION: 127,335,000
INTERNET USERS: 57,200,000
PRIVATELY-OWNED ISPS: YES

The huge success of the Internet, especially via mobile phones, has been spoiled by disclosure of the country's participation in the US electronic spying network Echelon and by creation of software to intercept e-mails.

The Japanese, famously passionate about communications, gadgets and digital technology, enthusiastically took to the Internet early on. As well as subscriptions to ISPs, cybercafés are everywhere and the arrival of i-mode, launched by Do Co Mo, a subsidiary of the big Japanese mobile phone company NTT, has started a new way of surfing the Web.

I-mode is the first successful link-up between mobile phones and the Internet, allowing phone calls, watching high-definition videos, listening to MP3 music and accessing a range of Internet services. Between 15 and 20 million people, mostly young people between 15 and 34, have taken to it.

Ironically, the country is not as advanced as other rich countries when it comes to speedy connections in homes and government offices, notably the education ministry. In March 2001, the government unveiled a catch-up plan called "e-Japan strategy" to build an infrastructure over five years giving 30 million Japanese homes high-speed Internet access and 10 million others very high-speed access.

Both accomplice and victim of spying

Japan was rocked in 2001 by the revelation that the government was taking part in the electronic spy network Echelon set up by the US National Security Agency. The network's giant dishes, monitoring and interception centres at strategic points around the globe (the US, Britain, New Zealand, Japan and elsewhere), can pick up, sort out and analyse traffic sent via fixed-line and mobile phones, satellite, optic-fibre lines and microwaves.

The scandal broke on 20 June, when a delegation of several NGOs, led by the Networkers against Surveillance Taskforce (NaST) which has campaigned since 1997 against generalised surveillance through new communications technology, for-

mally asked parliament to clarify Japan's role in the Echelon network. Japan had allowed the US to build a monitoring centre at its military base at Misawa, in northern Honshu island, but was Japan itself was a victim of this spying, as senior finance and foreign trade ministry officials repeatedly insist.

The daily paper *Mainichi Shimbun*, found some answers. It reported on 26 June that New Zealand was the key ally of US spying on Japan through Echelon. This was backed up by Duncan Campbell, an expert with the investigation into Echelon set up by the European Parliament. He cited examples of US spying on Japan during Japanese trade negotiations.

The Japanese government was especially embarrassed by the revelations because they were accused of complicity. As well as participating in Echelon, the government has built up its own monitoring capacity. The magazine *ZDnet* quoted a Japanese military source as saying Japan had equipped a fleet of five EP-3 planes with electronic interception and monitoring equipment. The data gathered is processed at the Tokyo headquarters of the Japanese Defence Agency, it said.

Parliament voted in March 2001 to spend more than a million dollars to create an e-mail monitoring software called "Kari-no-mail." It was ready by the end of that year and is reportedly being installed on the country's ISPs. But Japanese security officials have never told the politicians exactly how far things have gone. Freedom of expression and civil liberties organisations are demanding openness about it and demanding that use of the software be stopped.

LINKS:

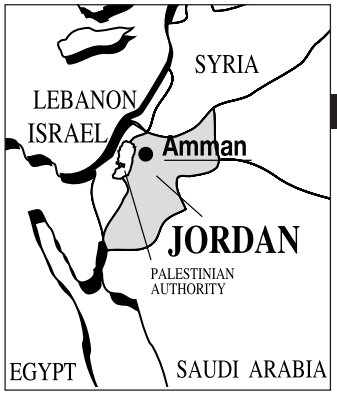
• www.echelonwatch.org
About the Echelon network

• www.jca.ax.apc.org/privacy
Networkers against Surveillance Taskforce (in Japanese)

• www.nttdocomo.com/top.html
DoCoMo, inventor of the "i-mode"

• www.kantei.go.jp/foreign/it/network/0122full_e.html
Details of the "e-Japan strategy"

• www.zdnetasia.com
The Asian edition of *Zdnet*



Jordan

POPULATION: 5,051,000
INTERNET USERS: 234,000
PRIVATELY-OWNED ISPS: YES

The Internet is a part of everyday life for Jordanians living in the capital and major towns. A street in the northern city of Irbid even tried in January 2001 to get into the Guinness Book of Records for having 105 cybercafés along a stretch of less than a kilometre.

Until 2001, Internet access was unrestricted and unmonitored but things have changed sharply since then. Fear of seeing the second Palestinian Intifada "contaminate" the kingdom, together with fallout from the 11 September attacks, led the authorities to warn people against any attempt to challenge the country's security and stability.

In early October 2001, curbs on the media, including the Internet, were introduced, providing for temporary or permanent closure of newspapers if they published what was termed libellous or false news that harmed national unity or the image of the state or encouraged strikes or illegal gatherings that disturbed public order. Penalties for insulting the king and queen or the crown prince were increased. Offenders became liable to prison sentences of between one and three years instead of just fines. The law said electronic material would be treated the same way as any other written material.

In December 2001, the king set up a Higher Media Council to reform the country's media policy and an attack on the Internet soon followed. Former TV journalist Toujan el-Faisal, who was Jordan's first female member of parliament, was sentenced to 18 months in prison on 16 May 2002 by the state security court for publishing false information abroad harming the image of the state and its officials.

In an open letter posted on the website of the Houston (Texas)-based *Arab Times* (www.arabtimes.com) on 6 March that year, she had claimed prime minister Ali Abu Ragheb profited financially from a government decision to double vehicle insurance rates. El-Faisal was also accused of insulting the country's judiciary in an interview with the Qatari TV station Al-Jazeera in which she denounced the corruption of Jordan's courts.

The court's presiding judge said she had made statements and published articles to stir up unrest in Jordan. She was pardoned by the king on 26 June 2002.

LINKS:

• www.jordantimes.com
The English-language daily *Jordan Times*

• www.petra.gov.jo
The official news agency *Petra*

• www.al-mashreq.org
Al Mashreq Al I'lami, independent newspaper specialising in media affairs (in Arabic)

• www.cdfj.org
Center for Defending Freedom of Journalists (in Arabic)

Kazakhstan

POPULATION: 16,095,000
INTERNET USERS: 150,000
PRIVATELY-OWNED ISPS: YES

The online opposition media is perhaps the liveliest in Central Asia but the government intelligence service monitors ISPs and access to opposition websites is frequently blocked.

Kazakh law treats websites the same as the written media and they are not therefore required to register with the authorities. The government set up a state body in 1999 to monitor all telecommunications networks. ISPs have to register with it and their lines are tapped by intelligence officials. Opposition websites are blocked by most ISPs, a consequence of the battle between the government and the independent media. To get round this, Internet users can use foreign-based proxy sites, though this takes longer.

Since it was created in September 2001, the website *kub.kz*, which is close to the opposition Democratic Choice of Kazakhstan party, has received anonymous threats from people warning it not to post anything about President Nursultan Nazarbayev, who is being legally investigated from abroad for embezzlement of state funds. Access to the site was blocked by the ISPs Kazakhtelecom, Nursat and Arna-Sprint during the first quarter of 2002.

Sergei Duvanov, who wrote an article that appeared online on 6 May 2002 criticising the president for fraud, was interrogated by secret service agents and is being prosecuted for "harming the honour and dignity" of the president. He was severely beaten by thugs on 28 August and the next day, *Kub*, which had published his article, was blocked. He was sentenced on appeal on 11 March 2003 to three and half years in prison for alleged rape of an under-age girl. The many irregularities that marred the investigation and trial, as well the harassment Duvanov was subjected to, suggest the prosecution was politically inspired.

Access to the *Respublika* site was blocked by Kazakhtelecom and Nursat between March and May 2002 and several other times during the year. The site contained news about the legal action being taken against the two main leaders of Democratic Choice of Kazakhstan.

The independent online newspaper *Navigator* was unavailable from 20 May 2002 for supposed technical and administrative reasons after it posted an interview with the former state prosecutor of Geneva, Bernard Bertossa, who confirmed that top Kazakh officials, including President Nazarbayev, had Swiss bank accounts.

Access to zhakiyanov.info, the official website of Democratic Choice of Kazakhstan leader Galymzhan Zhakiyanov, who is serving a seven-year prison sentence, was blocked by Nursat in several parts of the country on 4 September 2002.

Experts called in by Yuri Mizinov, editor of the online newspaper Navigator, reported in April 2003 that the country's main ISP, the state-owned Kazakhtelecom, had blocked access to the website.

LINKS:

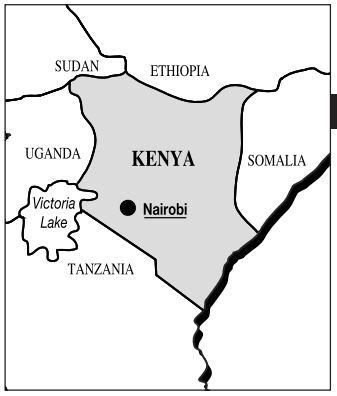
• www.rferl.org/bd/ka/index.html
Kazakh service of *Radio Free Europe / Radio Liberty*

• www.eurasianet.org
The news site *Eurasianet*

• www.adilsoz.kz/english/index.htm
The International Foundation for the Protection of Freedom of Speech "Adil Soz"

• www.bureau.kz/index_eng.shtml
Kazakhstan International Bureau for Human Rights and Rule of Law

• www.kub.kz/hot.php
The news site *Kub*



Kenya

POPULATION: 31,293,000
INTERNET USERS: 500,000
PRIVATELY-OWNED ISPS: YES

The Internet has been available since 1995, earlier than in most other African countries, and is not regulated. The number of users, mostly from the educated and upper classes, increases greatly every year. Despite there being no Internet law, the government, which has tense relations with the media, watches online activity closely. In late August and early September 2001, police searched two cybercafés in Nairobi and arrested several foreigners who were accused of distributing secret defence documents.

LINKS:

• http://allafrica.com/stories/200303040359.html
"The future of the Internet in Kenya," article in the regional daily *The East African Standard*

Kuwait

POPULATION: 1,971,000
INTERNET USERS: 200,000
PRIVATELY-OWNED ISPS: YES

Kuwait has plenty of cybercafés (more than 300) and many people have home connections, but the country is still under the influence of Islamic fundamentalists, who are suspicious of the Internet.

A hardline Islamist member of parliament called at the end of December 2000 for censorship and for ISPs to block access to sites with pornographic or "immoral" material. In May 2002, the government closed about 50 cybercafés as part of an anti-pornography drive and their operating permits were suspended by the communications ministry.

Inspections were begun after reports or complaints that some cybercafés had allowed customers to log on to pornographic sites. The ministry said new rules would be introduced to clamp down on such activity and that the closed cybercafés would not be allowed to reopen until then. However, they have since reopened and the new rules are being hotly debated, mostly under pressure from Islamist MPs.

LINKS:

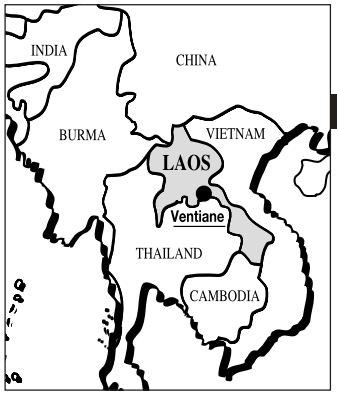
• www.kuwaitonline.com
News site

• www.kuwaittimes.net
The English-language daily *Kuwait Times*

• www.kuna.net.kw
The official *Kuwait News Agency*

• www.alwatan.com.kw
The Arab-language daily *Al-Watan*

• www.gulfissues.net
News about countries of the Gulf (in Arabic).



Laos

POPULATION: 5,403,000
INTERNET USERS: 15,000
PRIVATELY-OWNED ISPS: NO

The regime does not allow a free media or permit new information technology to be used to spread democracy.

Since the country went online in 1996, the government has controlled the ISPs and Internet use has grown only slowly. Connection time is expensive and Laotians are afraid to use a media they know the government and its agencies closely monitor.

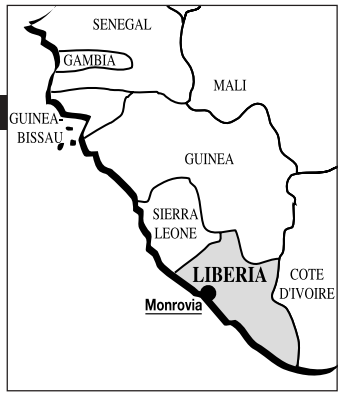
There are only about 50 cybercafés in the capital, Vientiane, and Laotians mainly use the Internet just to send and receive e-mail. They can only access websites approved by the government, which has blocked the opposition site *Vientianetimes*, based in the United States and a major irritant for the regime (and not to be confused with the site of the same name set up the government). Anyone who tries to reach the site gets a message back warning that the attempt has been "recorded."

The government set up an Internet Committee of Lao in 2000, which includes three ministries – information and culture, posts and telecommunications and transport and science – and has drawn up rules for Internet users, banning online publication by Laotians at home or abroad of any material likely to "harm national unity."

The official news agency *KPL* said in October 2000 that people who used the Internet in "the wrong way" by lying or getting people to protest against the government could be prosecuted or deported. The country's main ISP, Lao Telecommunications, says a journalist can publish material if he has permission from the Internet Committee and the appropriate ministry.
E-mail is also tampered with and many people complain that messages do not reach their intended recipients in Laos. When then do, the authorities may have changed the content, since Laotians must provide their passwords when they open an account with a Laotian ISP.

LINKS:

- www.laotel.com: The ISP Lao Telecommunications
- www.vientianetimes.com/headlines.html: Dissident news site (based in the US)



Liberia

POPULATION: 3,108,000
INTERNET USERS: N.A.
PRIVATELY-OWNED ISPS: NO

After years of devastating civil war, Liberia is trying to rebuild its basic infrastructure. The Internet is not a priority at all and facilities hardly exist.

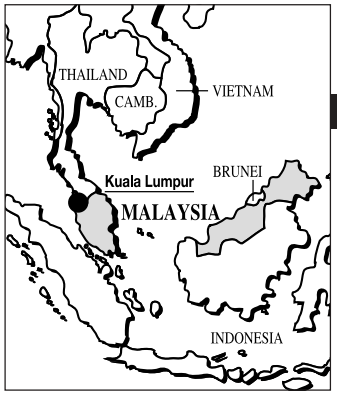
This does not stop President Charles Taylor from attacking the Internet in the same way he attacks the opposition press. He charges that exiled opposition journalists putting out news about the situation in Liberia are waging a "war" against him on the Internet.

The country's lone ISP, Data Tech, is accused of cutting off access when websites run by Liberians abroad contain too much anti-government material. The government launched a website in 2001 called allaboutliberia.com to counter these diaspora sites.

LINKS:

• www.allaboutliberia.com
Government news site

• www.theperspective.org
Opposition news site



Malaysia

POPULATION: 22,633,000
INTERNET USERS: 6,500,000
PRIVATELY-OWNED ISPS: YES
INTERNET USERS AND CYBER-DISSIDENTS IN PRISON: 1

Malaysia has invested enormously in the Internet and new technology to boost its economy, but the government harasses the independent online media and exerts heavy pressure on opposition websites.

Like all the big countries of Southeast Asia, Malaysia has enthusiastically embraced new information technology and the Internet. To counter the decline of the traditional economy, prime minister Mahathir Mohamad (in power since 1981) announced plans in 1996 for a Multimedia Super Corridor (MSC) as the core of a technology-based industrial revolution. He promised to protect the rights of users of the Internet and not censor it.

The MSC is a 50 km corridor 15 kms wide that will surround the new Kuala Lumpur international airport and new national capital of Putra Jaya. The government wants to attract major offices and research labs of large transnational computer and multi-media companies.

Harassment of the online daily *Malaysiakini*

The government may believe in the economic benefits of the Internet, but it is afraid the new media will destroy its tight control of the country's media. After promising not to censor the Internet, the government targeted the only independent and critical online daily newspaper, *Malaysiakini*. Its journalists cannot get official press cards and the government regularly challenges the stories on the paper's website and accuses it of wanting to damage the regime's credibility. Such verbal intimidation has proved ineffective and reporters have been individually harassed.

Malaysiakini journalists were allowed by parliamentary security officials on 3 April 2002 to attend sessions of parliament provided they did not ask questions at press conferences or approach MPs of the ruling UMNO party. A security officer said the professional status of the *Malaysiakini* journalists was unclear. The information ministry had refused to accredit them for two years. Two other news websites, *Radiqradio* and *Agendadaily*, were also refused accreditation.

In October 2002, *Malaysiakini*, which says it gets 100,000 visitors a day, was forced to introduce paying access for want of advertising revenue, according to editor Stephen Gan. The many verbal attacks by the authorities, especially the prime minister, have discouraged many local and foreign investors from advertising on the independent sites.

Police seized about 20 computers and a number of files in a raid on *Malaysiakini*'s offices on 20 January 2003 in response to a complaint filed by UMNO's youth wing for "sedition" and "incitement to racial hatred." Gan said it was an attempt to close the site down. The authorities demanded to know who had posted an anonymous article on the site on 9 January criticising the government's granting of special rights to the country's ethnic Malay majority and comparing the UMNO to the racist American Ku Klux Klan. Gan refused as a matter of journalistic principle to say who had written it.

The site was ordered on 22 January to leave its offices before the end of February by its landlord, the firm PC Suria, which is owned by the government-controlled body NASCOM. Gan denounced this as a new bid to close down the site by government pressure on PC Suria. *Malaysiakini*'s chief executive, Premesh Chandran, said finding new offices cost about 100,000 ringgits (26,000 euros) and disrupt its activities for at least two weeks. "It will also mean a loss in subscription revenue and a loss of confidence among our readers and subscribers," he said.

The staff said on 5 February they would defy the eviction order, noting that the lease did not expire until December 2004. Gan wrote to PC Suria's lawyer saying they would not leave because they had not violated any terms of the lease. As a result of local and foreign protests, pressure on *Malaysiakini* then subsided.

The opposition, which uses the Internet as a public platform, is also regularly harassed. In March 2001, the computers of the opposition National Justice Party's website were seized. Police searched the home of the site's editor, Raja Petra Kamaruddin, saying the site contained "seditious" material. The party has since transferred it to a host outside the country.

Cyber-journalist in prison

One of *Malaysiakini*'s journalists, Hishamuddin Rais (also a documentary film-maker), and five other dissidents, all of them arrested in April 2001 and jailed without trial for two years for "attempting to overthrow the government," began a hunger strike on 10 April 2002 to protest against their imprisonment under the Internal Security Act in Kamunting prison, at Taiping, in the northern state of Perak.

Rais and one of the other five, Badrulamin Bahron were taken on 16 April to the prison hospital, where they still refused to eat and were put on a drip. After eight days without food, they had won support from human rights activists, regime opponents and jailed former vice-premier Anwar Ibrahim, who also went on hunger strike for several days in solidarity. The state-run or pro-government media did not report their protest, which they halted after 11 days.

Rules for website content being drawn up

The energy, communications and multimedia ministry announced on 30 May 2001 that a National Internet Advisory Committee would be set up to coordinate and supervise Internet use and draw up laws to regulate it.

The same day, the ministry's parliamentary secretary, Chia Kwang Chye, said that in the absence of laws applying specifically to the Internet, its users must obey the Communication and Multimedia Act, which allows anyone who puts false or defamatory information on the Internet to be jailed for up to a year and heavily fined.

After strong pressure from online publications and the political opposition, the government announced in March 2002 it was dropping plans to regulate the Internet. However, a month earlier, *Malaysiakini* editor Gan said the government was keen to introduce rules about what could be put online and that the ministry was drafting a reform of the government's licensing system. Gan said the aim was clearly to weed out any opposition material or criticism of the government.

LINKS:

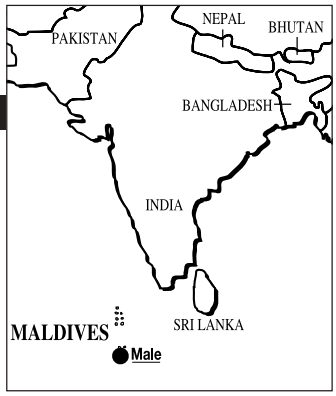
• www.malaysiakini.com.my
The online daily *Malaysiakini*

• www.aliran.com
The human rights organisation Aliran

• dapmalaysia.org/english
The opposition Democratic Action Party

• www.mcmc.gov.my/mcmc
The Communications and Multimedia Commission

• www.ktkm.gov.my
Ministry of energy, communications and multimedia



Maldives

Population: 300,000
Internet users: 15,000
Privately-owned ISPs: no
Internet Users and cyber-dissidents in prison: 4

President Maumoon Abdul Gayoom, who has ruled since 1978, refuses to allow his critics to use the Internet to oppose him. He made this brutally clear in 2002 when he had the editors of an e-mailed newsletter jailed for life. Meanwhile his government pushes an image of the country as a paradise through many tourism websites.

Freedom of expression, especially on the Internet, is restricted by several laws. One passed in 1968 bans speeches and articles that are against Islam, harmful to national security or insulting. However, at least two privately-owned newspapers criticise the government.

Mohamed Nasheed, an independent journalist and opposition member of parliament, was arrested on 8 October 2001 after posting several articles online. He had also signed a petition in February that year asking for permission to start an opposition party. After being held secretly for a month in the capital, Malé, he was sentenced at hasty trial to be banished for two and a half years to the remote island of Raa for alleged theft. The High Court confirmed the sentence on 13 March 2002 at a hearing without his lawyer present. It decided not to send him to prison but put him under house arrest in Malé and bar him from parliament.

In January 2002, businessmen Mohamed Zaki, Ibrahim Luthfee and Ahmad Didi, along with Luthfee's assistant, Fathimath Nisreen, were arrested for distributing anti-government articles in their e-mailed newsletter *Sandhaanu*. The Divehi-language publication contained no call to violence, according to Amnesty International. They were held in secret for two weeks in Malé and then transferred to a detention centre on Dhoonodhoo island.

In May, they were charged with defamation and allegedly trying to overthrow the government by what they published in *Sandhaanu*. They were refused the right to consult lawyers or receive family visits. In June, they were transferred to Mafushi island and put in small cells. On 7 July, the three businessmen were sentenced to life imprisonment. Nisreen, aged 21, was sentenced to 10 years in jail for allegedly

expressing dissatisfaction with government policies and supporting the authors of the website articles. The authorities refused to allow appeals.

During the trial, Luthfee (37) and Didi (50) admitted writing *Sandhaanu* and said Zaki (50), who lives in Malaysia, was in charge of e-mailing it to people who asked for it. Luthfee told the court he was ready to provide proof of all the things he accused President Gayoom of.

They are still being held on Mafushi island in poor conditions among drug offenders and thieves. Their cells have little air and they have only five litres of water a day to drink and wash in. Their families are only allowed to visit them once a month.

LINKS:

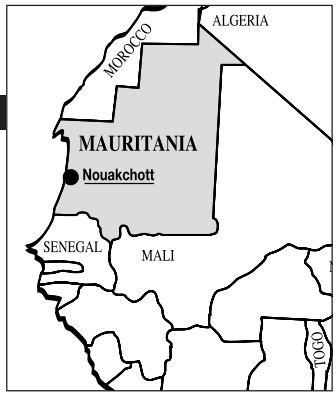
• www.maldivesculture.com/main.html
Foreign-based news site

• www.haveeru.com.mv/english
The daily paper *Haveeru*

• www.geocities.com/CapitolHill/Lobby/2311
Opposition human rights site

• www.presidencymaldives.gov.mv/v3
Office of the presidency

• www.dhivehinet.net.mv
The country's only ISP



Mauritania

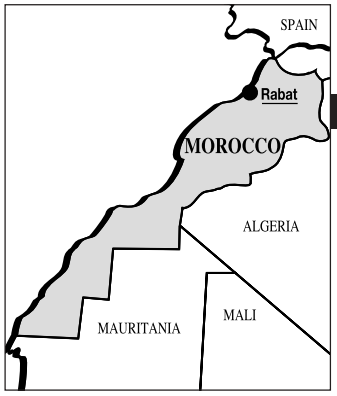
POPULATION: 2,747,000
INTERNET USERS: 10,000
PRIVATELY-OWNED ISPS: YES

The country went online in 1997, but most people use cybercafés, since the high cost of computers, ISP subscriptions (about 30 euros a month) and connections discourage logging on to the Internet from home.

Despite its small audience, the authorities have already circumscribed the Internet, with most privately-owned ISPs in the hands of pro-government businessmen. Cybercafé owners are obliged, if asked by state security officials, to submit copies of e-mail messages received or sent from their premises.

LINKS:

• www.maghreb-ddh.org
Human rights in North Africa



Morocco

POPULATION: 30,430,000
INTERNET USERS: 500,000
PRIVATELY-OWNED ISPS: YES

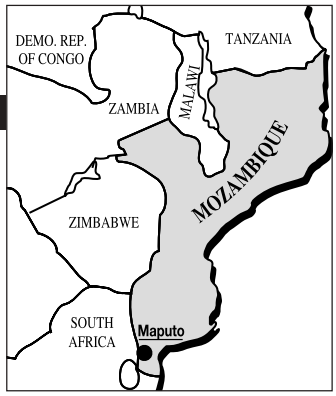
Until 2001, the Internet in Morocco was one of the freest in North Africa, with no curbs or blocking of sites such as those close to the Polisario Front. There are no laws about the Internet.

The Moroccan media uses the Internet to get round censorship. In December 2000, three weeklies were shut down for reporting a scandal involving the then prime minister, Abderrahmane Youssoufi. The three editors responded by posting the offending articles on the Internet, mainly on French websites.

Access to the site of the weekly *Rissalat al-Foutouwa*, run by the student section of the Islamist group Al-Adl Wal Ihsane (Justice and Spirituality), was blocked by the authorities in April 2001 but restored in 2002.

LINKS:

• www.maghreb-ddh.org
Human rights in North Africa



Mozambique

POPULATION: 18,644,000
INTERNET USERS: 30,000
PRIVATELY-OWNED ISPS: YES

The Internet is steadily growing despite the country's poor phone lines. The killers of journalist Carlos Cardoso, editor of the daily paper *Metical*, which was distributed only by e-mail or fax, were given prison sentences in 2003.

The Internet is catching on among Mozambicans but most people still use cybercafés to log on to it. The main towns have good Internet facilities and websites are not under threat of closure, censorship or monitoring. In fact the government is trying to expand Internet use and has set up a commission on computer technology policy under prime minister Pascoal Mocumbi.

The government does not politically harass Internet users or the rest of the media. However, the good record has been married by one serious episode – the murder on 22 November 2000 of Carlos Cardoso, publisher of the online newspaper *Metical*, which was only distributed by e-mail and fax.

He was killed driving home from his office through the centre of the capital, Maputo, by two gunmen who blocked the way and opened fire, killing him at once and seriously wounding his driver. Cardoso had been investigating the disappearance of 144 billion meticais (just over 7 million euros) from the Mozambique Commercial Bank (BCM). *Metical* had followed the scandal closely and expressed surprise at the lack of any enquiry. It had also mentioned the names of three powerful local businessmen, the Satar brothers and Vicente Ramaya.

On 28 February the following year, the interior minister announced the arrest of several suspects in the case and a few days later arrested Momade Abdul and Ayob Abdul Satar, as well as Vicente Ramaya, who had been the head of the BCM's Maputo office. At the end of May, six people had been charged in the case.

On the night of 1 September 2002, one of the six suspects, Anibal Antonio dos Santos Jr. ("Anibalzinho") escaped from Maputo's top security prison. The police gave no immediate explanation, but there had been recent public concern about the disorganised prison system. In August, Momade Abdul Satar, one of the alleged organisers of the killing, was put in solitary confinement after he was found to have a mobile phone.

On 3 September, three senior police officials working at the prison were arrested. The official version of Anibalzinho's escape was that he had walked out through the door of his cell. But this had three locks on it, to which only the police had keys. A few days later, eight more police officers were arrested.

The pro-government weekly *Domingo* called on 8 September for interior minister Almerino Manhenje to resign and at the end of the month, the independent weekly *Mediafax* accused him of being involved in the escape, saying he had direct control over the prison's security.

Two years after the murder, on 18 November, the trial of five of Cardoso's alleged killers began in a special courtroom inside Maputo prison (to guard against incidents) and the judge, Augusto Paulino, was given special protection. Journalists were allowed to attend the hearings.

The next day, one of the defendants, Manuel Fernandes, accused Nyimpine Chissano, son of President Joaquim Chissano, of having organised the murder. The president announced that justice had to be done and that the trial must continue even if his son's name had been mentioned. Another defendant, Momade Abdul Satar, said on 20 November that on Nyimpine Chissano's orders, he had paid Anibalzinho to kill Cardoso. On 25 November, the suspected triggerman, Rashid Cassamo, also accused the president's son of being the brains behind the murder.

The younger Chissano was summoned on 5 December and denied to the court he was involved. The six defendants were sentenced on 31 January 2003 to jail terms of between 23 and 28 years. The chief state prosecutor said Chissano's possible involvement in the murder was being investigated.

LINKS:

• www.infopol.gov.mz
Commission on Computer Technology Policy (in Portuguese)

• www.tropical.co.mz/~metical
The online daily *Metical* (in Portuguese, by subscription)

• www.mediacoop.odline.com
The independent weekly *Mediafax*

New Zealand

POPULATION: 3,808,000
INTERNET USERS: 1,908,000
PRIVATELY-OWNED ISPS: YES

The government has given itself legal authority to inspect computers and monitor private e-mail as part of a fight against crime and terrorism.

The government announced in March 2001 a plan to fight cybercrime that it said would also protect people's privacy better. But the country's Privacy Commissioner, Bruce Slane, immediately denounced it as allowing police to hack into private computers and look at people's e-mails armed with a simple search warrant. This was insufficient for something as serious as secret investigations and spying on citizens, he said. Associate minister of justice Paul Swain said police and intelligence agents needed such powers to fight crime and terrorism conducted through the Internet.

In July that year, the Green Party strongly denounced the bill and criticised the government's law and order committee for ignoring people's concerns about police spying on their private e-mail, especially as the police had not made a case for needing to do so.

In the wake of the 11 September attacks, the government announced measures to step up monitoring of private computers and Internet traffic. One, announced in December 2001, required all computer and Internet users to cooperate with police investigations and ISPs to work closely with police, the Government Communications Security Bureau (GCSB) and the Security Intelligence Service (SIS). In March 2002, the government allotted 1.5 million euros for phone-tapping and e-mail monitoring. Another law obliged phone companies and ISPs to install equipment to intercept their customers' calls.

In November 2002, the government moved to boost the powers of the police, the GCSB and the SIS to monitor e-mail. The Telecommunications (Interception Capability) Bill proposed that Internet operators be required to install equipment to monitor and intercept encrypted messages. The bill, drawn up after a report by the Law Reform Commission, provided for fines of up to 25,000 euros for failing to do so. Once again, civil liberties organisations, the Green Party (notably MP Keith Locke) and some Internet operators attacked the serious implications of the measure for

privacy of electronic communications. The bill had still not been passed in April 2003.

All these government efforts aimed to force Internet operators, especially ISPs, to monitor e-mail messages if need be. Such measures give the police and intelligence services powers that broadly escape scrutiny by the courts or parliament.

Using the Echelon electronic surveillance system

In June 2001, the media reported that New Zealand was part of the US Echelon spy-network to monitor electronic communications. New Zealand journalist Nicky Hager, an expert on Echelon, told the Japanese daily *Mainichi Shimbun* that the US National Security Council, the spy agency that runs Echelon, was used until the late 1980s to conduct US industrial espionage against Japan, watching the role the world's second biggest economy was playing in the South Pacific.

He said the GCSB spied on Japan until 1989 from its base in Wellington and helped analyse data about it from other Echelon network posts. In the early 1990s, the GCSB expanded and set up another base at Waihopai, near Blenheim. An advanced information-gathering system monitored the electronic traffic of Japanese embassies and consulates, including confidential information about trade negotiations, fishing, coal price talks, support for developing countries and immigration matters.

LINKS:

• www.internetnz.net.nz/index.html
The Internet Society of New Zealand

• www.gcsb.govt.nz
The Government Communications Security Bureau

• www.eff.org
The Electronic Frontier Foundation

• www.arena.org.nz/davesub.htm
Information about the anti-terrorism law

• www.privacy.org.nz/top.html
Site of the Privacy Commissioner

• www.nzherald.co.nz
The daily *New Zealand Herald*

North Korea

POPULATION: 22,428,000
INTERNET USERS: UNKNOWN
PRIVATELY-OWNED ISPS: NO

The Internet officially does not exist in the world's most isolated country, but a handful of privileged people are allowed to go online through the phone system or via satellite. The regime also uses the Internet for its own foreign communications and in early 2002 even set up a website (Arirang) to attract tourists.

China hosts the official DPRKorea Infobank site (in Korean, English, Japanese and Chinese), that describes the delights of the North Korea. A dozen other official sites, including the government's *Korean Central News Agency* (*KCNA*), are hosted in Japan or China. The *KCNA* site contains descriptions and articles about the "Dear Leader" Kim Jong-il and happy peasants and workers. There is no mention of the country's famine situation.

A North Korean scientific magazine, *The World of Science*, printed a diagram in 2000 showing a plan to instal filters between the Internet and the country's Intranet to control material passing between the two.

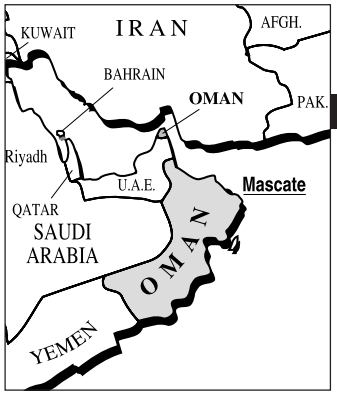
This ambiguous attitude to the Internet is denounced by human rights organisations using the Web to fight the repressive regime. One of the most active is the Citizens' Alliance for North Korean Human Rights, which is based in South Korea and heavily involved in helping those who manage to escape from the country via China or Russia. Its site contains many reports on the situation.

LINKS:

• www.nkhumanrights.or.kr
The Citizens' Alliance for North Korean Human Rights

• www.dprkorea.com
A government site to promote tourism

• www.kcna.co.jp
The government news agency *KCNA*



Oman

POPULATION: 2,622,000
INTERNET USERS: 120,000
PRIVATELY-OWNED ISPS: NO

Although it denies it, the government monitors the content of websites through its General Telecommunications Organisation (GTO), the country's sole ISP, founded in 1997. The GTO bars access to a large number of sites, especially foreign ones, that are considered morally offensive to Islam, so as to protect Omanis from supposed contamination by Western ideas. The government uses the Internet however to put out official information, mainly via the website of the official *Omani News Agency* (*ONA*).

LINKS:

• www.omanobserver.com
News site

• www.gulfissues.net
News about countries of the Gulf (in Arabic)

Pakistan

POPULATION: 141,971,000
INTERNET USERS: 500,000
PRIVATELY-OWNED ISPS: YES

The Internet is not yet widespread and is still mainly accessed through cybercafés. It does not seem to be especially censored. But the Daniel Pearl kidnapping and murder case showed how it could be used by extremists. The military regime has made every effort to block access to a US-based investigative journalism website.

With only a half a million Internet users, Pakistan is quite behind with new information technology. This is mainly because of the country's large size and low level of economic development, including only a few million private phone lines, mostly in big cities.

Gen. Pervez Musharraf's government appears to favour its growth, even though on the day he seized power, 12 October 1999, the army cut off all Internet connections for several hours, and in July 2002, the Pakistan Telecommunications Authority (PTA) tried to force cybercafés owners to record the names of their customers.

Gen. Musharraf says his government has invested more than 100 million euros in communications and sharply reduced the cost of connections and services since 1999. Pakistan has since launched a programme to boost digital technology, the Information Technology and Telecom Policy.

Slow and difficult development

This policy has led the government to cut Internet connection costs and invest in telecommunications infrastructure, while putting the Internet under the direct supervision of the PTA. The state's monopoly in the sector ended in December 2001 but big Internet operators such as AOL are reluctant to invest in a country where scant profits are to be made.

For the time being, Pakistanis are enthusiastically using cybercafés, which are everywhere in the cities. In Peshawar, a new one opens nearly every day.

Use of the Internet during the Pearl case

The Daniel Pearl murder showed how the Internet can exacerbate rising tensions in Pakistan. The Musharraf government supported the Taliban in Afghanistan until the 11 September attacks and has to cope with Islamic fundamentalists in Pakistan itself.

The Internet can also be used by these extremists to their advantage. The kidnapping of *Wall Street Journal* reporter Pearl on 23 January 2002 and his murder by a Pakistani fundamentalist group was an example. The kidnappers made great use of the Internet, logging on with their personal computers and in cybercafés to announce the kidnapping, put out political statements and generally publicise their crime.

The case could perhaps hamper growth of the Internet in Pakistan. The US government regularly complains about how Al-Qaeda militants use the Internet, often from Pakistan, to put out their messages, organise themselves and launch operations.

In January 2003, the Federal Investigative Agency (FIA) was put in charge of fighting cybercrime and cyber-terrorism and with US money and staff support, the government set up a system of surveillance of the Internet. Until then, Pakistan police had only three officers trained in combating cybercrime. The authorities have not said whether the FIA will monitor e-mail messages.

Military regime targets *South Asia Tribune*

The information ministry indicated in a special announcement on 2 November 2002 that newspapers reproducing articles from the Washington-based *South Asia Tribune* website (www.satribune.com) could be prosecuted under a new libel law that came into effect a month earlier and provides for up to three months in jail, a fine of about 50,000 rupees (850 euros) and an obligatory public apology by those found guilty.

The South Asia Tribune was founded in July 2002 by Shaheen Sebhai, a former senior editor of the daily *The News*, who has been exiled in the United States since March 2002. The website has reported several corruption and human rights scandals involving the government and gets about 100,000 visitors a month. Pakistani papers have also reprinted material from it. The information ministry announcement did not mention Sebhai or his website by name, simply referring to a Pakistani journalist it said had gone into voluntary exile and launched a campaign to defame the government and its officials.

Since he has been in exile, Sebhai has been targeted by the government. An army employee filed a complaint against him for a burglary supposedly committed in February 2001 and several of his friends were arrested and held several weeks in Islamabad in connection with it. Journalist colleagues have been threatened by intelligence agents for publicly defending him.

Attempts to control the Internet

The South Asia Tribune site reported in November 2002 that the PTA had in July that year ordered ISPs and cybercafé owners to keep a record of the names, connection times, numbers called and computer identities of their customers. Senior PTA official Col. Nayyar Hassan said the order to ISPs to keep this data for a month was justified by the rise in cybercrime. Cybercafé owners were required to keep such records for two weeks. *The South Asia Tribune* said the PTA had issued a reminder in August that the data should collected and kept. However, Col. Hassan himself admitted the order was being disregarded.

The Pakistan Telecommunication Company (PTCL) announced on 2 April 2003 that 400 new sites with "indecent" content had been added to an earlier list of 100 banned websites and asked Internet operators to block access to them. ISPs said the move would slow down Internet access. A senior PTCL official, Zahir Khan, said on 6 April that access to nearly 1,800 pornographic sites had been banned and that the PTCL was thinking of importing software to make it easier to do. Also targeted were "anti-Islamic" and "blasphemous" sites. The PTCL admitted the blocking would temporarily slow down Internet navigation but said it was necessary because of what it called the great threat to society from such sites. Mairajul Huda, a leader of the Islamist Jamaat-e-Islami party, welcomed the moves and said the electronic media had to be reformed to bring them into line with the country's culture and religion so young people would not be tempted by such evil.

Cyberwar between India and Pakistan

The Pakistani government set up a special interministerial committee in May 2003 to counter increasing attacks on government websites by Indian hackers who were making them inaccessible. Information technology minister Awais Ahmad Khan Leghari said that if the attackers were identified, the government would take the matter to the relevant international authorities to seek their punishment. The previous month, he had said the government was thinking of hiring its own hackers to fight the attacks. The daily paper The News said the government's working group on Internet security was responsible for protecting the country's cyber-security.

LINKS:

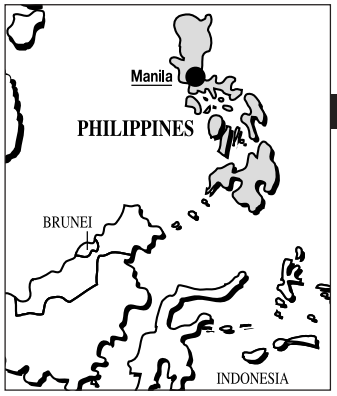
• www.satribune.com: The US-based *South Asia Tribune*

• www.paknet.com.pk: The country's main ISP

• www.oneworld.org/ppf: The Pakistan Press Foundation

• www.dawn.com: The major daily *Dawn*

www.dailytimes.com.pk: *The Daily Times*



Philippines

POPULATION: 77,130,000
INTERNET USERS: 2,000,000
PRIVATELY-OWNED ISPS: YES

Growth of the Internet has been helped by a general atmosphere of freedom of expression, but the fight against separatist organisations, officially called "terrorists," has been used to justify laws authorising surveillance of the Internet.

The Philippines is one of the few countries in the world that has laws covering 10 different sorts of cybercrime, divided into crimes involving data (interception, alteration and theft), the Internet (interference and sabotage), access (hacking and spreading viruses) and crimes planned with others (cyber-criminals, fraud and forgery).

But the government does not filter or block access to websites, which can be set up without any official procedures. However, non-government attempts have been made to control site content, especially pornography.

The national Catholic Bishops Conference (CBCP) launched its own ISP, cbcpnet.com, in April 2000, equipped with a firewall blocking access to pornographic sites, which it said would make it safe for children.

In June 2001, a bill (471) to protect students from the Internet was presented to Congress, requiring libraries in all schools and educational institutions to install filters to block access to obscene or violent sites.

Anti-terrorism and threats to privacy and security

Proposed new anti-terrorist measures, especially article 10 of House Bill 3802, drafted in the wake of the 11 September attacks would give the government a free hand to secretly tap any phone, cable or other means of transmitting any kind of written or oral messages, including conversations, discussions, news or data and to secretly record them. The measure clearly covers the Internet and e-mail messages.

The definition of terrorism in these measures is also sufficiently vague to allow it to be applied to all kinds of lawful critics of the government. The national constitution emphasises freedom of expression but the proposed laws, at a time when the

government is fighting Muslim separatists on Mindanao island, is a warning to groups that strongly oppose the government.

Some clauses of Bill 3802 seek to protect against abuses in its application, but human rights activists still fear these safeguards will be easily got round. In May 2002, a group led by Congresswoman Liza Maza called it the "mother of all repressive laws." Others see the anti-terrorist measures as restoration of former dictator Ferdinand Marcos' anti-subversion law, which he used to crack down on his opponents.

LINKS:

• www.cyberdyaryo.com/features/f2002_0513_02.htm
Article on the anti-terrorist measures

• www.cmfr.com.ph/index.html
About freedom of expression in the Philippines

• www.inq7.net
The newspaper *Philippine Daily Inquirer*

• web.amnesty.org/library/eng-phl/index
Amnesty International's archives on human rights in the Philippines

Russia

POPULATION: 144,664,000
INTERNET USERS: 6,000,000
PRIVATELY-OWNED ISPS: YES

The Internet has become very popular for putting out news, but dissidents' online freedom of expression has been undermined by anti-terrorist laws.

The lower house of the Russian parliament, the Duma, approved a law in late June 2002 at President Vladimir Putin's request to ban "all forms of extremist activity" on the Internet. The new law aroused fears among online freedom advocates of more power for the police. Putin's political opponents feared it would be used to target minority parties, which could be prosecuted and their websites shut down if they were accused by the authorities of encouraging or supporting extremism on the Internet.

"Russia does have extremists and nationalists, but their eradication is not this law's real purpose," said Sergei Kovalyov, a Union of Right Forces (SPS) member of the Duma."It allows online activity to be banned for no good reason." He was also concerned about the law's provision to allow punishment to be based on criminal legislation.

But the heaviest criticism was of the 11 categories of extremist activity, which drew on laws against terrorism, attempts to overthrow the government and inciting people to riot or racial hatred. The law also banned any activity or publication threatening the country's "security." Freedom of expression and human rights campaigners say this too-broad definition of extremism will threaten perfectly legitimate activity, such a websites that oppose the war in Chechnya.

The information ministry threatened in late October 2002 to shut down the website of the radio station *Ekho Moskvy* for broadcasting an interview with Chechen guerrillas holding several hundred people hostage in a Moscow theatre. The mass kidnapping gave the government a chance to propose an anti-terrorist law that allows the authorities to prosecute any journalist reporting on matters related to terrorism or the war in Chechnya. At the last minute, Putin vetoed the bill and asked parliament to revise it.

Access to Chechen news sites is systematically blocked. They included *chechen.ru*, cut off by the FSB (ex-KGB) on 5 November 2002. In early December, Dmitri

Chepchugov, head of the interior ministry's anti-cybercrime department, said all websites connected with Chechen rebels had been identified and that an undisclosed number had been shut down. Even though they were based abroad, foreign ISPs had barred access to them. Among them was kavkaztsenter site, based in Estonia, cut off in late April 2003 after pressure from the Russian authorities.

LINKS:

• www.gdf.ru
The Glasnost Defence Foundation

• rferl.org
Radio Free Europe / Radio Liberty

• www.prima-news.ru/eng
The human rights news agency *Prima News*

Saudi Arabia

POPULATION: 21,028,000
INTERNET USERS: 1,600,000
PRIVATELY-OWNED ISPS: YES

The government has only allowed general access to the Internet since 1999 because it had not until then installed effective censorship to monitor all connections made and block access to websites considered "immoral."

The firewall, which is housed in the King Abdulaziz City for Science and Technology in Jeddah, officially bars the way to pornographic sites but in fact censors all websites deemed to violate what the authorities call the social, cultural, political, economic and religious principles of the state. Opposition sites, such as that of the Movement for Islamic Reform in Arabia (MIRA), cannot be viewed, along with a large number of other sites of human rights groups or NGOs.

In early 2001, the authorities said they had blocked access to 200,000 sites. In April that year, they announced they would block 200,000 more whose content was considered "offensive to good morals." At the same time, the country's grand mufti called on Internet users to boycott Yahoo! on grounds that it was "promoting pornography."

There is no specific legislation dealing with the Internet, which is covered by the press law. This requires official authorisation to start up any kind of media outlet. The royal family also has the power to dismiss journalists and appoint the heads of newspapers or other media. There is no freedom of expression in Saudi Arabia for either the media or the Internet.

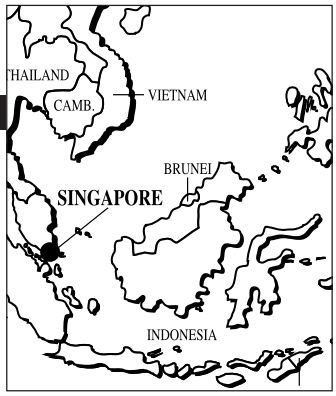
But getting round the restrictions seems increasingly popular. Internet users are going through proxy servers more and more to connect to banned sites and also to surf the Web anonymously.

LINKS:

• www.saudihr.org: Saudi Center for Human Rights Studies

• www.saudiinstitute.org: Saudi Institute for Development and Studies, which encourages the growth of civil society in the country

• www.gulfissues.net: News about countries of the Gulf (in Arabic)



Singapore

POPULATION: 4,108,000
INTERNET USERS: 2 247 000
PRIVATELY-OWNED ISPS: YES

The city-state is one of the most wired countries in Asia, but the government severely restricts Internet use by government opponents. The authorities are also trying to impose "responsible" use of the Internet.

The Internet has been a resounding success in Singapore ever since the country went online in 1995 and two-thirds of all households have a computer. More than two million people are online, up from 800,000 in 1999. The number of websites in the country's .sg domain has risen from 900 in 1996 to more than 17,000 today.

But the government does not like being criticised and, even though it denies doing so, quietly and effectively censors material. The Internet was placed in the late 1990s under the supervision of the Singapore Broadcasting Authority (SBA), which controls access to sites and requires them to obey rules for what it calls "responsible" use of the Internet.

It asks ISPs to bar access to sites containing material that "undermines public security, national defence, racial and religious harmony and public morality" and is thought to have blocked more than 100 sites deemed to be pornographic. Sites that do not comply with the SBA rules do not get an operating licence. They must also install filters on their servers.

Political and religious websites must register with the government's Media Development Authority, which also requires ISPs to block access to about 100 sites considered undesirable. Some Internet operators encourage customers to install filters, especially CyberPatrol and Smart Filter, on their computers, mainly to block pornographic sites.

The law was amended before parliamentary elections in 2001 to curb the activities of political websites. Government opponents, journalists and other critics are hampered by the internal security law, which allows the arrest of anyone undermining the very general notion of "state security," and by the heavy fines imposed in libel cases.

In July 2002, a government opponent, Zulfikar Mohamad Shariff, who has posted articles online, fled to Australia after police searched his house and threatened to arrest him. His computer was seized and he was accused of libelling the daughter-in-law of a government minister. He learned recently that if he returned to Singapore he would face charges of sedition and threatening racial harmony and could be jailed for two years.

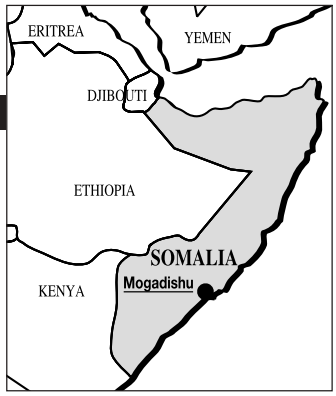
The government set up a "Cyber Wellness Task Force" in March 2003 to teach Singaporeans how to behave online. It aims to prevent the country's millions of users from sending "useless" e-mails and spam and not to look at pornographic sites or use false names in discussion forums. Its head, Michael Yap, is planning information campaigns, new websites and training workshops.

LINKS:

• www.thinkcentre.org
Southeast Asia's freedom of expression organisation, Think Centre

• www.jamesgomeznews.com
Site of James Gomez, an expert on freedom of expression in Singapore

• www.mda.gov.sg
The Media Development Authority, the government's Internet regulatory body



Somalia

POPULATION: 9,157,000
INTERNET USERS: N.A.
PRIVATELY-OWNED ISPS: YES

The country has been online only since 1999 and is very behind in new information technology. Just a few hundred people surf the Internet in the 40 or so call-shops and Web-bars in the capital, Mogadishu. One reason is that Somalia only has a total of 2,000 phone lines. The cost of calls fell in 2002 but is still very high for one of Africa's poorest countries.

A rare event in the history of the Internet happened in November 2001, when the country was completely disconnected for two months, after the sole ISP, Somalia Internet Company, and the main telecommunications firm, al-Barakaat, were forced to close. They had been accused by the US government of funding Al-Qaeda and were put on the US list of those supporting terrorism. In January 2002, a new ISP and telecommunications company, NetXchange, began operations, filling the gap left by the closed firms.

LINKS:

• http://allafrica.com/stories/200201230295.html
"Internet Returns to Mogadishu", in *AllAfrica.com*, January 23, 2002

South Africa

POPULATION, 43,792,000
INTERNET USERS: 3,100,000
PRIVATELY-OWNED ISPS: YES

The country started off as the spearhead of the Internet in Africa but in early June 2002, its parliament passed a controversial law to fight cyber-terrorism. The law's opponents also criticised the government for moving to take over assignment of the country's ".za" domain names.

The explosion of the Internet in South Africa delighted Internet fans all over Africa. The country has far and away the most connections. It has been online since the mid-1990s, with the big advantage that nearly all the continent's Internet traffic passes through its "backbones" (connection nodes enabling world-wide routing of messages). This gives South Africa a solid technological infrastructure to boost its own Internet growth.

The road to democratising the Internet began about two years ago and the fruits are now visible. ISPs are flourishing and competition is fierce. The government is keen to get all sectors of the population online as quickly as possible. This has not yet happened but the steady growth in the number of Internet users is very promising.

What kind of monitoring of what networks?

Two events however clouded the picture in June 2002 – passage of a law to combat cyber-terrorism and the government's move to take over attribution of ".za" domain names.

Parliament passed the Electronic Communications and Transactions Bill with the declared aim of protecting the country against cyber-terrorism. South Africa had earlier signed the first international convention against cyber-crime in Budapest on 23 November 2001, along with 30 or so other countries (the United States, Canada, Japan and members of the Council of Europe).

The new law was strongly criticised, especially by the Democratic Alliance party, which voted against it, and by Internet freedom organisations and private firms. The law allows telecommunications minister Ivy Matsepe-Casaburri to appoint

inspectors to monitor telecommunications networks and their content, which they are authorised to seize.

Private companies are worried about the government's interference with e-commerce, even though the minister told parliament she did not intend to monitor traffic. Apart from economic interests, privacy and freedom of expression campaigners fear a lack of openness by the inspectors and wonder which communications networks they will monitor and what kind of data they will seek access to.

Resistance over domain names

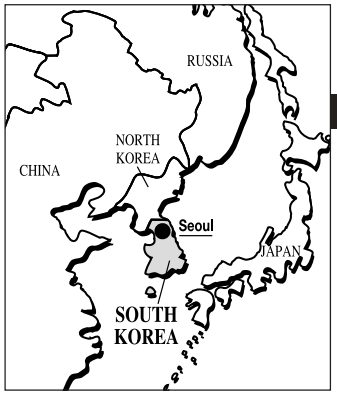
The government's decision to take over assignment of domain names has also sparked controversy. Until the measure allowing this was passed, it was done by a users' group called NameSpace ZA, run by Mike Lawrie. The government says this should not be done by just one person working in the private sector.

Lawrie says the move is plain nationalisation and is unacceptable because the degree of surveillance and control the government would have would threaten the independence of the Internet in the country. He has refused to comply with the new law and in June he switched some of his data and ISPs out of the country so as to protect them, he said, even if it meant being prosecuted.

LINKS:

• www.namespace.org.za
The Internet users' group Namespace ZA

• www.ispa.org.za
The South African ISP Association ISPA



South Korea

POPULATION: 47,069,000
INTERNET USERS: 26,270,000
PRIVATELY-OWNED ISPS: YES

The number of Internet users is soaring and the country has one of the world's biggest concentrations of high-speed connections, along with the US. But the government still censors sites it considers objectionable.

The country has fully realised the importance of the Internet in opening up and expanding the economy. In just three years, the number of people online rose from three million to 26 million, largely because of the growth of high-speed connections, whose quality is a big draw.

Black list of 120,000 sites

Despite being so widely used, the Internet is still regulated. South Korea was one of the first countries in the world, in 1995, to pass a law about the distribution and viewing of online material. The Information Communication Ethics Committee (ICEC) monitors the content of websites and forums very closely and can recommend that access to them be blocked.

The information and communication ministry called in July 2001 for access to be barred to 120,000 sites it considered offensive. These included sites featuring pornography, violence, information about computer hacking, spreading viruses, cybercrime and euthanasia. The government asked for filters against them to be installed on computers in cybercafés, schools and public libraries. ISPs faced prosecution if they did not install them too. The reason given was to protect young people from exposure to supposedly dangerous content.

This argument was rejected by Jinbonet, which campaigns for Internet freedom in South Korea. It was just one more attack on the Internet, it said, after the government was forced in 2000 to abandon an earlier proposal to introduce online censorship as a result of a public uproar. Jinbonet said the ministry had experts working on ways to block sites.

ICEC shut down the anti military service site non-serviam in May 2002 for two months, on grounds that military service was an obligation for all Korean men and

that anti-militarist campaigns had drawn many complaints. The decision was taken under article 53 of the 1995 law.

A month later, the country's constitutional court struck down article 53, along with article 16 providing for its application, after criticism by Jinbonet and the group Lawyers for a Democratic Society. In November, parliament amended Article 53, replacing the term "dangerous content" with "illegal content." But the powers of ICEC and the ministry to monitor and punish were upheld.

Political militant arrested

Kim Kang-pil, an activist of the far-left Democratic Labour Party, was arrested on 25 July 2002 for posting articles about North Korea on the party's website. He was held under article 7 of the national security law which severely punishes sympathisers of the North Korean regime. He was accused of committing "an act advantageous to the enemy" and sentenced to a year in prison and banned from voting for a year. After the trial, an anti Internet censorship group said it clearly showed the government was monitoring political and social websites and that there must be others reasons for the sentence. Kim was freed on 3 December after an appeals court had suspended his sentence.

Gay website banned

A federation of 15 gay rights associations filed a suit against the government in January 2002 for banning the country's first website for homosexuals, exzone.com. The group, the Lesbian and Gay Alliance Against Discrimination in Korea, pointed out that the national constitution did not permit the government to interfere with people's sexual orientation and that banning the site was a violation of the guarantee of freedom of expression, speech and the media.

A government committee on the protection of children, answering to the prime minister's office, had called the website pornographic and harmful to young people's morality. But a few months earlier, the committee had placed on the Internet the uncensored details of the sexual offences committed against children under 13 by about 60 named people, whose personal and professional details were also given.

High-speed connections help hackers

One result of the Internet's success and the ease of connection through high-speed access is that hackers are particularly active. A study in 2001 by consultants Predictive Systems said a third of all hacking done outside the United States originated in or passed through South Korea.

An example was the episode of a US spy-plane forced to land in China in May 2001, which triggered furious activity by US and Chinese hackers, with South Korea as the cyber-battlefield. More than 100 attacks were made on the websites of universities,

companies and research centres in South Korea, because the country has so many connections with both countries. The hackers on both sides wanted to conceal their identity so they hid behind South Korea rather than attack the "enemy" directly.

Election campaign online

The December 2002 presidential elections featured on an online battle between animated websites set up by young journalists close to reformist candidate Roh Moo-hyun and major newspapers such as the right-wing daily *Chosun Ilbo*. Roh's victory was helped by support from sites such as *OhmyNews*, which got 20 million visitors a day during the campaign. The site's founder, Oh Yeon-ho, said he had reproduced online the equivalent of the pro-democracy street-fighting in the 1980s. The site, based on a network of 23,000 "citizen-reporters" all over the country, had a scoop when it exposed a scandal involving the Hyundai industrial group.

LINKS:

• http://english.jinbo.net
Jinbonet and the Progressive Network Center

• www.mic.go.kr
Ministry of information and communication

• www.ohmynews.com
The independent online paper *OhmyNews*

Spain

POPULATION: 39,921,000
INTERNET USERS: 7,856,000
PRIVATELY-OWNED ISPS: YES

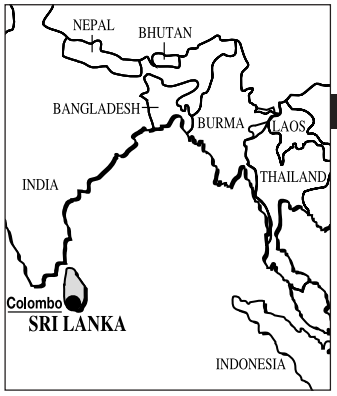
The lower house of the Spanish parliament passed the LSSICE "Internet law," to fight cybercrime and terrorism via the Internet, on 27 June 2002. Devised by the science and technology ministry, it obliges ISPs to retain traffic logs of their customers for at least a year. An opposition amendment bars police or intelligence officials from using such data without court permission.

But how such data retention will work in practice has not been spelled out and no official body has been given authority to shut down websites considered to have "undermined" a list of social values.

Freedom of expression is upheld in the Constitution, whose article 20 guarantees the right to "freely send or receive truthful information by any medium of communication" and whose article 18.3 protects confidentiality of postal, telegraphic and phone messages "except when there is a court order." This has led privacy campaigners and prominent lawyers to denounce the new law as unconstitutional.

LINKS:

• www.agenciaprotecciondatos.org
The national data protection agency



Sri Lanka

POPULATION: 19,104,000
INTERNET USERS: 200,000
PRIVATELY-OWNED ISPS: YES

Despite a variety of ISPs and the opening of more than 100 cybercafés in major cities, the relatively few Internet users mostly just send and receive e-mail.

Sri Lanka has no special Internet law and the telecommunications regulatory body licences ISPs. Editors and webmasters must register their sites with the Council for Information Technology (Cintec). The authorities can thus easily identify them. But so far no sites have been censored.

Though slow to develop elsewhere in the society, the Internet does play a part in the country's political life. The 20-year rebellion of the separatist Tamil Tigers has spilled over onto the Internet.

Dharmaratnam Sivaram, who runs the *Tamilnet* news site, was attacked by thugs at his office on 26 December 2001, six months after being accused by the pro-government media of being a Tamil Tiger spy. He needed six stitches in his head. *Tamilnet* is the main source of news on the Web about the political and military situation in the rebel areas.

The home of Senathirajah Jeyanandamoorthy, correspondent for the news website *Tamilnet* and the Tamil daily *Virakesari*, in the eastern town of Batticaloa, was attacked with grenades on the night of 7 January 2002. The attackers also tried to burn down the house. The journalist and his family managed to escape. The Eastern Journalists Association said he had received death threats, notably from Islamic extremist groups. Jeyanandamoorthy had written about Islamic extremists operating in the region. His articles about the Tamil Tigers also angered Sinhalese nationalists.

The Internet should expand in Sri Lanka now that a ceasefire has been signed (on 22 February 2002) between the army and the rebels, followed by peace talks in May.

LINKS:

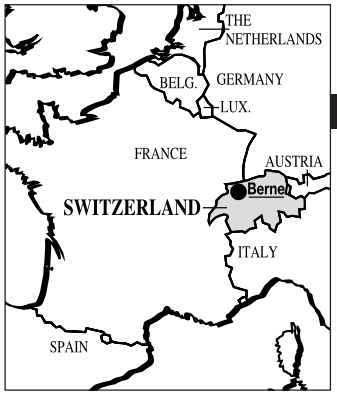
• www.theacademic.org
Independent news site

• www.tamilnet.com
The news site *Tamilnet*

• www.eelamweb.com
Tamil Tigers site

• www.cintec.lk
The Council for Information Technology

• www.slarmy.org
The Sri Lankan army



Switzerland

POPULATION: 7,170,000
INTERNET USERS: 2,375,000
PRIVATELY-OWNED ISPS: YES

Article 322-b of the Criminal Code, which came into force on 1 April 1998, provides for prosecution of anyone who, deliberately or carelessly, allows the posting of illegal material. This is the system of responsibility by association that also applies to the written media. So if the author cannot be found or cannot be tried in a Swiss court, a website's content can be blamed on the publisher, the site's host and even the ISP.

The federal law on monitoring postal and telecommunications traffic that came into effect on 1 January 2002 requires ISPs to retain customers' connection records for six months and to hand them over to the monitoring authorities, by court order and if possible in real time.

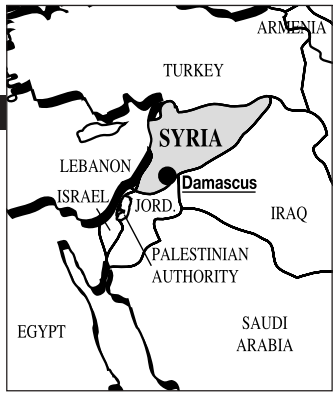
The federal police, in a written statement in spring 2000, said a site's host had a duty to check the legality of material in case there was a legal complaint. The police can also ask an ISP to block access to a site and ask a host to either block or erase one, all at their own expense and without compensation. The exact extent of these monitoring obligations has so far only been discussed and no court has yet had a case testing these rules.

LINKS:

• www.edsb.ch
Federal Data Protection Commissioner

• www.juriscom.net
Information technology law site

• www.siug.ch
Swiss Internet User Group



Syria

POPULATION: 16,610,000
INTERNET USERS: 60,000
PRIVATELY-OWNED ISPS: NO

Syria is one of the countries most tightly monitoring the Internet. Access is restricted to government bodies and a number of hand-picked companies. The rest of the population can only go online at a few closely-watched government-run cybercafés or at clandestine centres.

The government's Syrian Telecommunications Establishment controls all access to the Internet, blocking "offensive" content such as pornography and pro-Israeli material. E-mail is monitored too and people can be sent to prison for sending unauthorised messages to foreigners. When a person wants an Internet connection at home, state technicians install the phone line and the access package and choose the customer's password themselves.

LINKS:

• www.teshreen.com
The Arabic-language government daily *Teshreen*, with link to the English-language government paper *Syria Times*

• www.arabnews.com
News about Arab countries

Thailand

POPULATION: 63,584,000
INTERNET USERS: 4,800,000
PRIVATELY-OWNED ISPS: YES

The Internet is supervised by the National Information Technology Committee (NITC), the National Electronics and Computer Technology Center (NECTEC), the Telephone Organisation of Thailand (TOT) and the Communications Authority of Thailand (CAT). The rise of such bodies has hindered Internet growth more than encouraged it. The CAT by law has a minimum 32 per cent share in all privately-owned ISPs.

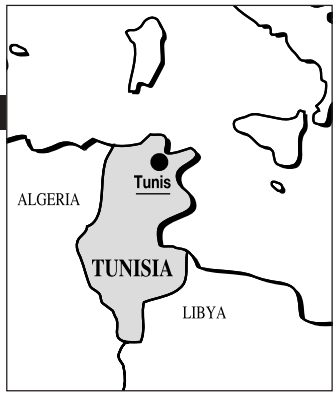
The media, most of which have websites, do not complain about censorship, even though relations between the independent media and populist prime minister Thaksin Shinawatra are tense. But the NITC said in July 2001 it would hunt down "unsuitable content" on the Internet. It ordered ISPs to retain connection data about their customers for at least three months, so that undesirable websites could be spotted and blocked and those who logged on to them could be prosecuted. The police and technical and legal experts work closely with the NITC to monitor cybercafés as well as the Internet to identify target sites.

Information and communication technology minister Surapong Suebwonglee said on 19 December he had asked the country's Internet operators, including a score of ISPs, to block access to "obscene" or "subversive" websites. The daily paper *The Nation* said he had defined "subversive" as endangering national security and the monarchy. The minister said he wanted the Internet in Thailand to be "a pleasant place."

LINKS:

• www.cat.or.th/eng
The Communications Authority of Thailand

• www.nationmultimedia.com
The Nation media group



Tunisia

POPULATION: 9,562,000
INTERNET USERS: 500,000
PRIVATELY-OWNED ISPS: YES
CYBER-DISSIDENTS IN PRISON: 1

The government says it favours rapid and democratic growth of the Internet. But in practice, state security police keep it under very tight control. Sites are censored, e-mail intercepted, cybercafés monitored and users arrested and arbitrarily imprisoned. One cyber-dissident was arrested in 2002 and sent to jail for two years.

The country has been online since the mid-1990s and the Internet is more widespread than in the rest of North Africa because the government promotes it as a major economic tool. It is administered by the Tunisian Internet Agency (ATI), which is part of the telecommunications ministry.

Phone lines are good and the government has encouraged ISPs, of which there are six state-owned and six privately-owned. The authorities have set up 300 cybercafés ("publinets") throughout the country and says all universities and secondary schools and universities are on the Internet.

Press freedom does not exist in Tunisia, so people have taken wholesale to the Internet to take part in it there. This is what journalist Sihem Bensedrine did when she could not get permission to publish a newspaper and instead set up an online magazine, *Kalima*. But President Zine el-Abidine ben Ali and his powerful police apparatus are determined to stamp out all cyber-dissidence.

The Tunisian government runs one of the world's most extensive Internet censorship operations. The only ISPs allowed to serve the general public are those owned by the president's associates, including his daughter. The ATI ensures that the market is tightly controlled by the authorities. ISPs must sign a contract saying they will only allow customers to use the Internet for "scientific, technological and commercial purposes strictly to do with their area of activity."

Cyberspace in Tunisia has been regulated since 2001 by the press law, which provides for censorship. Access to some news websites, such as *Kalima* and

TUNeZINE, but also those of NGOs and foreign media carrying criticism of the government, is routinely blocked.

The powers of the "cyber-police"

The managers of the publinets have the right to check what sites their customers are looking at and can force them to disconnect at any time. There is plenty of evidence that cybercafés are closely watched by the police. Plainclothes officers regularly collect details of Internet activity from the machines to check who has been looking at what sites.

Control of telecommunications, including the Internet, was stepped up further in 2002 and a full-scale corps of cyber-police went into operation to track down "subversive" websites to be blocked, intercept e-mail or attempts to reach sites containing "political or critical" material, hunt for and neutralise "proxy" servers used to get round directly-blocked access to sites, and track down and arrest "over-active" Internet users – the cyber-dissidents.

About 20 young men were arrested at their homes in the southern town of Zarzis on 5 February 2003. In April, seven of them, including a minor, were in prison in Tunis for "delinquency, theft and obtaining material to make explosives" as a result of consulting "terrorist" websites. Their lawyer, who visited them in jail, said they had been tortured.

The daily paper *La Presse* reported on 22 April 2003 that the government had stopped issuing permits to open privately-owned cybercafés and had said access to the Internet would be limited to the government-controlled publinets.

"Ettounsi" sent to prison for two years

Zouhair Yahyaoui was arrested by plainclothes police on 4 June 2002 in Tunis, at a computer centre where he worked. He was taken to his home, where they searched his bedroom and seized his computer equipment.

During interrogation, he was tortured with three sessions of being made to hang by his arms with feet off the ground. As a result of this, he gave them the password to his website, which allowed the authorities to block access to it.

Yahyaoui, who used the pseudonym "Ettounsi" ("The Tunisian" in Arabic), founded the website *TUNeZINE* in July 2001 to put out news about the fight for democracy and freedom in the country and to publicise opposition material. He wrote many columns and essays and was the first to publish an open letter that his uncle, Judge Mokhtar Yahyaoui, had sent to President Ben Ali denouncing the Tunisian judiciary's lack of independence. The judge's own website, almizen.com, which his nephew also ran, was destroyed.

TUNeZINE was censored by the authorities right from the start. But its fans each week received a list of "proxy" servers through which they could access it.

He was sentenced by an appeals court on 10 July 2002 to a year in prison for "putting out false news to give the impression there had been a criminal attack on persons or property" (article 306-3 of the penal code) and another year for "theft by the fraudulent use of a communications link," meaning an Internet connection at a cybercafé where he worked (article 84 of the communications code). He was jailed in very harsh conditions and staged two hunger-strikes in early 2003 to protest against his imprisonment.

LINKS:

• www.kalima-tunisie.com
Online news magazine *Kalima*

• www.tunezine.com
Online news magazine *TUNeZINE*

• www.maghreb-ddh.org
Human rights in North Africa

Turkey

POPULATION: 67,632,000
INTERNET USERS: 4,900,000
PRIVATELY-OWNED ISPS: YES

The government cracks down on the Internet as it does on the rest of the media, censoring and prosecuting journalists who dare to criticise the state and its institutions.

The Internet is growing fast in Turkey, with an estimated 700,000 people connected from their homes. Other users go online from cybercafés which are opening everywhere, especially in big towns and cities. The state-owned Turkish Telekom, through its subsidiary TTnet, has cornered most of the market, but privately-owned operators are growing without much difficulty.

However, before starting out, owners of cybercafés must promise in writing to block all access to sites that promote separatism, Islamic fundamentalism or pornography, and also get permission to open from the police, who have an "electronic brigade" that strengthens surveillance of the Internet and electronic communications. The Ankara police have a special Internet division, as do the country's regions.

No national laws refer specifically to the Internet, but the May 2002 law on the National Broadcasting Council (RTÜK) imposed severe restrictions on freedom of expression on the Internet, with webpages requiring approval by the authorities before being posted. Courts tend to treat Internet cases under the country's very repressive media laws.

On 6 December 2001, an Istanbul court ordered closure of *ideapolitika.com*, the website of the political and cultural quarterly *Idea Politika*, which was being sued. The judge used the press law as a reference. However, the verdict was not applied, since the site is run from France. The magazine's former editor, Erol Ozkoray, was due to appear before the press court on 11 July 2003 for publishing an article on 11 September 2001 called "What's the use of the army?" on the website. He is accused of insulting the army and faces three years in prison.

On 12 March 2002, Coskun Ak, coordinator of interactivity at the firm Superonline, was sentenced to three years and four months in prison for "insulting and making fun of the state, the armed forces, the police and the judiciary." He had left on the

firm's website in May 1999 an item about human rights violations in southeastern Turkey, which had been posted on the site's forum by a participant. The sentence was commuted to a fine. He was acquitted on 24 April 2003 by the Istanbul assize court, which said there was insufficient evidence he was responsible for the item, which it said contained "serious insults to state institutions."

LINKS:

• www.ideapolitika.com
The magazine *Idea Politika*

• www.cyber-rights.org
The organisation Cyber-Rights & Cyber-Liberties

• www.europa.eu.int
The European Union

Turkmenistan

POPULATION: 4,835,000
INTERNET USERS: 8,000
PRIVATELY-OWNED ISPS: NO

President Separmurad Nyazov's regime has total control of the media, including the Internet, which barely exists in the country. The state-owned Turkmen Telecom is the only ISP permitted. The website of the Prague-based *Radio Free Europe/Radio Liberty*, which is funded by the US Congress, is one of the rare sources of independent news.

LINKS:

• www.rferl.org/bd/tu
The Turkmen service of *Radio Free Europe / Radio Liberty*

• www.eurasianet.org
The news site *Eurasianet*

Ukraine

POPULATION: 49,112,000
INTERNET USERS: 600,000
PRIVATELY-OWNED ISPS: YES

Although not yet very widespread, the Internet has proved a boon to investigative journalists whose online publications are the only places they can publish uncensored material. But these websites are under constant pressure from the authorities.

Ukraine is rather behind where the Internet is concerned. The price of computers and especially the cost of connections is too high for most people. Continuing delay in privatising UkrNet, the government telecommunications firm, is also an obstacle to the introduction of competition and thus much lower prices.

But bold journalists in this country under the iron hand of President Leonid Kuchma have been using the Internet since the late 1990s to put out independent news. This has come at a big price, as shown by the murder of journalist Georgy Gongadze.

Progress in the Gongadze murder enquiry

Ukrainskaya Pravda was founded in spring 2000 as the first opposition newspaper published only online. Its incisive articles soon made it popular with Ukrainians. "It's a way to be a free journalist that's otherwise impossible in Ukraine," said Gongadze, its founder and editor. In the months before he vanished, he several times reported he had been threatened. In July 2000, he even complained to the country's prosecutor-general, Mihailo Potebenko, about "deliberate intimidation" to frighten him and stop him working.

On 2 November that year, his headless corpse was found near Tarashcha, 140 km from Kiev. Revelations that top government officials were probably involved jolted Kuchma's regime. But the authorities vigorously blocked a search for the truth. The prosecutor-general's office and the interior ministry opposed any serious attempt to investigate Gongadze's disappearance and murder.

But investigations started making progress in 2002. On 19 July, the prosecutor-general ordered a new analysis of tape recordings implicating Kuchma and agreed to a new autopsy on Gongadze's body with the help of European experts.

On 5 August, a new prosecutor-general, Svyatoslav Piskun, granted Reporters Without Borders secretary-general Robert Ménard the right to legally represent the civil parties in the case. On 3 September, Piskun admitted the law had been broken during the enquiry, formally recognised the body as Gongadze's and that he had been decapitated.
On 10 September, Piskun said the public prosecutor in Tarashcha, where the body had been found, had been charged with forging the initial statement about the body and with not having tried to identify the body immediately. The Tarashcha police investigator, Sergy Belinsky, was also charged with forgery.

On the second anniversary of Gongadze's disappearance, on 16 September, Reporters Without Borders asked for permission to re-examine, with an independent expert of its choice, all the forensic tests done so far as well as related documents. It also asked the prosecutor-general's office to question four men who reportedly followed Gongadze in the weeks before he vanished.

The same day, Gongadze's widow Myroslava, with the help of the Damocles Network and the Institute of Mass Information, filed a complaint with the European Court of Human Rights, accusing the prosecutor's office of obstructing investigations. In October, Reporters Without Borders secretary-general Ménard and a French pathologist went through all the results of the previous forensic analyses.

An independent autopsy, at the request of Gongadze's mother and arranged by Reporters Without Borders, was done in January 2003 and formally identified the body as that of Gongadze. The investigation, which should now focus on former interior ministry officials, has not produced any further results.

Monitoring increases

In January 2001, an Internet department was set up in the State Information Committee with the aim of "monitoring false news about Ukraine."

On 28 February, a government decree put the State Centre for Information Security under the secret police, the SBU, which thus gained control over the Internet.

On 1 June, an NGO was set up to administer websites using the national domain name ".ua". Among its founders, apart from the SBU, were several ISPs previously in charge of running the domain but which had yielded control to the new body. The NGO proposed a law on 12 November to step up monitoring of the Internet under the guise of fighting terrorism, organised crime and pornography.

On 26 June, investigative journalist Oleg Yeltsov was summoned for questioning by the SBU and accused of "violating state secrets" by posting on the website Ukraina Kriminalna (Criminal Ukraine) an article describing the lifestyle of former secret police chief Leonid Derkach and his son, a member of Ukraine's oligarchy. Yeltsov's apartment was searched while he was away being questioned.

On 16 July, SBU chief Volodymir Radchenko told a press conference in Kiev that the SBU wanted all Internet users to register with the authorities. He said this was so a directory could be produced for users.

On 23 August, President Kuchma signed a decree about openness of telecommunications in Ukraine that gave the government a month to spell out steps to improve state regulation of the flow of information.

On 25 September, access to the website of the opposition newspaper *Antenna* in Cherkassy was blocked. The previous day, the local militia had visited the paper's offices and offered "protection" for the website.

In December 2001, journalists of the online newspaper Forum were called in by the SBU and accused of revealing state secrets on the website on 15 June that year in an article reporting the results of an inspection of the state reserves office. Legal aid from the Institute of Mass Information enabled the journalists to escape prosecution.

On 21 February 2002, the editors of the online political newspaper *Obkom* filed a complaint against the national tax authority the day after its officials went the paper's offices to search them even though they only had a warrant to search a bank on the floor below. Despite editor Sergy Sukhobok's protests and presentation of various legal documents allowing the site to operate, the officials seized computer equipment and some of the archives. Although the tax authority said later the search had been done "by accident," the computers were never returned.

LINKS:

• http://en.imi.org.ua
The freedom of expression body The Institute of Mass Information

• www.antenna.com.ua
The opposition paper *Antenna*

• www2.pravda.com.ua/en
The online opposition paper *Ukrainskaia Pravda*

United Arab Emirates

POPULATION: 2,654,000
INTERNETS USERS: 1,175,600
PRIVATELY-OWNED ISPS: NO

The January 2002 opening of Dubai Media City, a media and new technology free-zone, has not really changed the situation where the government officially bars access only to pornographic websites but in practice to many more.

The country is the keenest in the Gulf region about the Internet but that has not made it the most tolerant. Yet no specific Internet law has been passed and the only relevant legislation, the 1996 Telecommunications Law, is quite liberal because it guarantees freedom of expression in all media.

And since January 2002, the UAE has become a kind of regional Silicon Valley, with the opening of the Dubai Media City free-zone of media, computer and new technology firms, including the Arab satellite TV station *Middle East Broadcasting Centre* (*MBC*), which used to be based in London. About 30 businesses in all, mostly foreign, are expected to set up shop there.

But this gives a false impression of opening up. A single ISP, the state-owned telecommunications firm Etisalat, has a monopoly on Internet connections and services. Internet access is filtered, the authorities say, to weed out "pornography." But this firewall also blocks a very large number of other sites.

Self-censorship is routine for fear of punishment. People avoid mentioning in e-mail topics such as religion, morality, friendly countries or members of the ruling families.

LINKS:

• www.emirates.net.ae
Emirates Internet & Multimedia

• www.etisalat.co.ae
The government ISP Etisalat

• www.dubainews.com
News site

• www.dpc.org.ae
Dubai Press Club

• www.gulfissues.net
News about countries of the Gulf (in Arabic)

United Kingdom

POPULATION: 59,542,000
INTERNET USERS: 24,000,000
PRIVATELY-OWNED ISPS: YES

The government pushed through measures to monitor the Internet in the wake of the 11 September attacks. The Terrorism Act passed in December 2001 extended the period of obligatory traffic log data retention by ISPs to at least a year. The home office (interior ministry) also said it would monitor online financial transactions and private e-mail messages. The new law said police no longer had to get prior court permission to act, but simply approval from the home secretary or a senior ministry official. This caused a big row and some ISPs said they might move their servers out of the country.

In June 2002, home secretary David Blunkett proposed amending a controversial law passed in June 2000, the "RIP Act" (Regulation of Investigatory Powers Act), that allowed monitoring of all Internet activity by the secret services as a means to fight cybercrime. Blunkett now proposed to allow local authorities (tax and social security offices and municipal services, for example) to access details of people's Internet activity, including e-mail they sent and received. This caused such uproar in the media and among civil liberties groups that the government dropped the measure two weeks later.

The independent Information Commissioner, Elizabeth France (responsible for seeing that the government, official bodies and the secret services respected citizens' rights to data privacy), savaged the proposal in an August 2002 report. She said data retention and the proposed amendment of the RIP Act would seriously undermine basic freedoms and reduce guarantees of privacy and that some aspects of the proposed law would be illegal.

LINKS:

- www.hmso.gov.uk: Government information site
- www.cyber-rights.org: Cyber-Rights & Cyber-Liberties
- www.ispa.org.uk: ISP Association UK

United States

POPULATION: 285,926,000
INTERNET USERS: 155,000,000
PRIVATELY-OWNED ISPS: YES

The United States was where the Internet started but it was also where electronic surveillance of it began. The 11 September attacks have only strengthened the government's determination to monitor the flow of information on the Internet.

More than half of all Americans are online and most have high-speed connections. The Internet is a vital means of communication in the United States. However, the 11 September 2001 attacks and the terrorists' presumed use of it to contact each other in preparing that operation abruptly changed the government's attitude to the Internet.

Just a few hours after the attacks, FBI agents went to the head offices of the country's main ISPs, including Hotmail, AOL and Earthlink, to get details of possible e-mail messages between the terrorists. The online magazine *Wired* said FBI agents also tried to install the Carnivore surveillance system (since renamed DCS 1000) on the ISPs. It said they turned up at ISP offices with the software and offered to pay for installation and operation. They reportedly demanded and obtained material from certain e-mail accounts, most of whose names included the word "Allah." All major US-based ISPs are thought to have complied fully with the FBI demands.

Easing the rules

Carnivore, designed by the FBI, can record and store all messages sent or received by an ISP's customers, using word filters that make no distinction between different kinds of messages, thus exceeding the bounds of normal surveillance. US civil liberties campaigners fought Carnivore, which had never been used before without a court order. However, the Combating Terrorism Act, passed urgently by the Senate on 13 September, after 30 minutes of debate just two days after the attacks, allowed intelligence services to use it without having to seek such approval. A prosecutor can now order electronic surveillance of someone for 48 hours without getting a judge's permission.

Monitoring Internet data was legalised on 24 October 2001 when the US House of Representatives overwhelmingly passed the "USA Patriot Act" (Provide Appropriate Tools Required to Intercept and Obstruct Terrorism). It confirmed the authority already given to the FBI to install Carnivore on an ISP's equipment to monitor e-mail messages and store records of Internet activity by people suspected of being in contact with a foreign power. This requires only the permission of a special secret court. The Act also expands the kind of information a prosecutor can ask for from an ISP without a judge's permission and invites ISPs to freely hand over to the authorities data unrelated to content, such as records of websites visited.

A new step was taken on 20 November 2002 with Senate approval of the Homeland Security Act, which set up a super-ministry with the job of preventing terrorist attacks. It will eventually have a staff of 170,000 drawn from 22 government departments and bodies. Section 225 of the law allows ISPs to disclose the content of their customers' messages at the request of federal or local officials if, "in good faith" they think this will prevent death or serious injury. The Electronic Frontier Foundation (EFF) says this means ISPs will be doing the work of a court. It deplores the fact that disclosure will be on the basis of "good faith" rather than "reasonable belief" as before and says the threats cited can be very general.

Section 225 also allows police to record without permission any message sent or received by a "protected computer" (one used in interstate commerce or communications) which is under attack. It also increases to 20 years the penalty for computer crimes that cause serious injury and life imprisonment if they result in death.

Encryption in the dock

Many US officials have also criticised encryption, which allows Internet users to keep their messages and activity confidential by encoding it with software. Encryption, mainly used by companies to exchange sensitive economic data, has never been banned in the United States. But its export is restricted under the Wassenaar Arrangement, which required inspection of material that could be used for both civil and military purposes. The 11 September attacks have revived the debate between supporters and opponents of encryption.

The director of the FBI said in March 2001 that terrorists were using encryption. On 13 September that year, Republican Sen. Judd Gregg proposed a blanket ban on encryption software whose makers had not handed over the decoding key to the government.

The authorities noted that plans to hijack 11 US airliners had been found on the laptop computer of the man behind the first attack on the World Trade Center in 1993 and that the FBI had needed 10 months to decode the files, most of which were encrypted with the Pretty Good Privacy (PGP) software. PGP's inventor, David Zimmerman, who nearly went to jail in the 1980s for widely distributing his programme, recently defended it in an interview in *Futur(e)s* magazine. He said the US

Congress, courts and media had discussed the issue for the past decade and concluded society had more to gain than lose from powerful encryption. PGP was saving lives all over the world, he said, and was used by human rights organisations everywhere, especially in countries ruled by dictatorships.

Encryption software has under attack from the FBI's Magic Lantern programme, an e-mail that can secretly record the keystrokes of an Internet user, so the FBI can see the passwords and codes employed by encryption users. After press reports about it, the FBI denied having such a programme but admitted it was working on one.

Against censorship, but in favour of monitoring

As well as seeking to monitor the flow of online information to check what is being said and exchanged, the authorities are also trying to use the Internet to put out US propaganda in their war against terrorism.

The New York Times reported on 19 February this year that the Defense Department's Office of Strategic Influence (OSI) had proposed planting disinformation in the foreign media, mainly through websites set up and secretly run by the OSI and through e-mails sent to journalists or media offices. The revelation caused an outcry and White House spokesman Ari Fleischer quickly said President Bush knew nothing about the project and had ordered the OSI closed down because, said defense secretary Donald Rumsfeld, the Pentagon "does not lie to the American people" or to "foreign audiences."

The Bush administration could also use the Internet to break the information monopoly under some dictatorships. Two members of the US House of Representatives proposed a law on 2 October 2002 to fight censorship worldwide. The Global Internet Freedom Act would set up a federal Office of Global Internet Freedom to counter jamming and censorship of the Internet by authoritarian regimes and persecution of those who use it. The office would be part of the International Broadcasting Bureau, which runs several radio stations that already combat censorship, such as *Radio Free Europe* and *Radio Free Asia*. It would have a $50 million budget for 2003 and 2004.

But what is censorship? The Global Internet Freedom Act would have the US take no steps against government censorship aimed at protecting minors. A legal battle pitting several civil liberties groups and public libraries against the Bush administration over the Children's Internet Protection Act is growing. The US supreme court said on 12 November 2002 it would rule on the Act, passed in 2000 and obliging all libraries receiving federal funds for Internet facilities to install anti-pornography filters on their computers.

The Act's opponents say it violates the first amendment to the US constitution concerning freedom of expression and also blocks access to other websites as well as pornographic ones. In May 2002, a federal court in Philadelphia said forcing public

libraries to install filters was indeed censoring freedom of expression protected by the constitution. The federal government has appealed to the supreme court, saying the filter software was the best available to prevent taxpayers' having to subsidise the spread of obscene websites and material unsuitable for children. Ten per cent of the 143 million Internet users in the US go online at public libraries, 80 per cent of which have received federal funds to set up Internet facilities.

An Orwellian future?

In early November 2002, the US media reported that the Pentagon had set up an Information Awareness Office to develop technology to trawl Internet navigation records to spot activity such as credit card purchases and airline reservations that might indicate a potential terrorist. The head of this $200 million a year project, John Poindexter, says software will pick out travel in dangerous parts of the world, suspicious e-mail and dubious money transfers. The data will be regularly gathered by intelligence services with the permission of governments and companies.

Opponents of the project call it "Orwellian" and several civil liberties organisations say personal information unrelated to terrorism and which is none of the government's business would also be obtained. Marc Rotenberg, head of the Electronic Privacy Information Center (EPIC), says the authorities would have data in their hands hitherto only obtainable by court order as part of criminal investigations. He deplores the lack of a body to monitor the collection of such information.

Poindexter was sentenced to six months in prison in 1990 for lying to the US Congress in the Iran-Contras scandal but the conviction was quashed on grounds that his legal rights were not respected.

LINKS:

• www.aclu.org
American Civil Liberties Union

• www.cdt.org
The Center for Democracy and Technology

• www.dfn.org
The Digital Freedom Network

• www.eff.org
The Electronic Frontier Foundation

• www.epic.org
The Electronic Privacy Information Center

• www.peacefire.org
Peacefire

• www.rcfp.org
The Reporters Committee for Freedom of the Press

Basic documents :

• USA Patriot Act
www.eff.org/Privacy/Surveillance/Terrorism_militias/hr3162.php

• Homeland Security Act
www.whitehouse.gov/deptofhomeland/bill/index.html

• Global Internet Freedom Act
www.theorator.com/bills108/hr48.html

• Information Awareness Office
www.darpa.mil/iao

• Children's Internet Protection Act
www.ifea.net/cipa.html

About Carnivore

• www.fbi.gov/hq/lab/carnivore/carnivore2.htm

• www.epic.org/privacy/carnivore

• www.wired.com
News for specialists

Uzbekistan

POPULATION: 25,257,000
INTERNET USERS: 275 000
PRIVATELY-OWNED ISPS: YES

The number of Internet users doubled between 2001 and the end of 2002, but the high cost of connection excludes most people from the Internet and the few who can afford it suspect the government spies on their messages. Several cybercafés have sprung up in the capital, Tashkent, but the US organisation Internews says customers have to promise in writing not to send "political or religious" e-mails. So self-censorship is routine in a country where no independent media are allowed.

There are several ISPs, two of them privately-owned. The authorities ended the monopoly of the state-owned ISP, Uzpak, in October 2002.

OpenNet Initiative (ONI), which catalogues censored sites, says the authorities systematically block access to opposition sites such as the Birlik party and the banned Islamic party Hizb ut-Tahrir. News sites that carry critical articles about President Islam Karimov are sometimes censored.

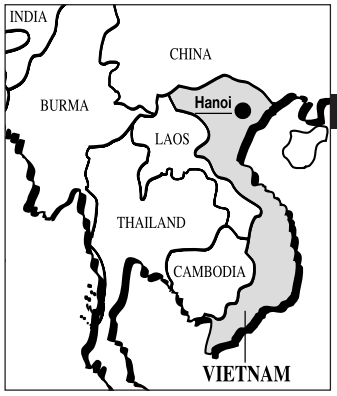
In February 2003, a freedom of information law, which restricts news put out by all media, including the Internet, came into force. Its article 4 says freedom to inform the public can be restricted to "protect the moral values of society, national security and the country's spiritual, cultural and scientific potential." This vague definition leaves plenty of room for interpretation and thus censorship. The same is true of other articles, which give pretexts such as "preserving cultural and historical values," "preventing psychological influence over and manipulation of public awareness" and preserving "social stability."

LINKS:

• www.rferl.org/bd/uz/index.html
The Uzbek service of *Radio Free Europe / Radio Liberty*

• www.eurasianet.org
The news site *Eurasianet*

• www.birlik.net/engl.html
The censored site of Birlik, the opposition Popular Movement of Uzbekistan



Vietnam

POPULATION: 79,175,000
INTERNET USERS: 1,500,000
PRIVATELY-OWNED ISPS: YES
INTERNET USERS AND CYBER-DISSIDENTS IN PRISON: 5

The Internet is not very widespread and remains under the control of the ruling Communist Party. Cyber-dissidents are arrested, politically and culturally "incorrect" websites are blocked and personal e-mail is monitored. The government seems to be closely following China's example.

When the younger-generation Nong Duc Manh took over the Communist Party leadership in April 2001, hopes were raised for greater media freedom and growth of the Internet. But this has not happened and Vietnam remains one of the world's most repressive countries where the Internet is concerned. One of the main blocks to its growth is the high cost of communications. However, more and more people in universities are logging on and cybercafés are springing up everywhere.

The biggest of the five public or part publicly-owned ISPs, Vietnam Data Communications (VDC), catering to nearly a third of all Internet users, is controlled by the posts and telecommunications ministry (DGPT). The government blocks access to websites it considers politically and morally "dangerous," including foreign news sites and those of human rights organisations set up by Vietnamese abroad. VDC monitors what sites its customers visit.

Opposition groups say the government even regularly hacks into "undesirable" sites. The Hoahao spiritual movement, for example, says the Vietnamese embassy in Singapore sends viruses by e-mail to the movement's followers and to political opponents abroad.

But the government also uses the Internet for propaganda purposes. The proceedings of the 9th Communist Party Congress in April 2001 were reported in several languages on the website of the official *Vietnam News Agency* (*VNA*). Internet access points were set up around the country so the population could follow the congress. The party also advertises its doctrines on its own website, which opened in 2001.

The prime minister announced in August 2001 that the government would allow new

ISPs to operate, including privately-owned ones. But this has not yet happened. The government has forbidden use of the Internet for political opposition, for actions against national sovereignty and security and violations of morality or the law.

Deputy culture and information minister Nguyen Khac Hai ordered police on 8 January 2002 to seize and destroy any publication not authorised by the government. The *BBC* reported that photocopies of printouts from the dissident news website *Dialogue* were among the targets.

On 5 August 2002, the DGPT asked the authorities in the country's 61 provinces to step up monitoring and inspection of cybercafés. The government called for punishment of those making "harmful use" of the Internet. Two days later, the culture and information ministry suspended the website *TTVNonline.com* because it did not have proper authorisation to operate and was putting out news that violated the press law and "twisted the truth."

The ministry refused to say what this news was, but official sources said the target was the site's discussion group, where topics such as territory ceded to China in December 1999, political reforms and corruption in the Communist Party were being discussed. The website was voted by the specialist press in 2001 as the best one for young people.

On 16 August 2002, Phan An Sa, deputy chief inspector at the culture and information ministry, called for access to subversive and pornographic material on the Internet to be blocked. He listed five kinds of Internet use he said was harmful to national security, including exchanges of anti-government material and use of the Internet to defraud people. He added that the authorities should fine young people and train them better how to use the Internet. Most Vietnamese users are aged between 14 and 24.

In early 2003, Phan announced new laws would be passed to monitor Internet content more closely. Sites run from Vietnam would have to have a licence and inform the authorities whenever they changed the content of the site. He said Internet operators, especially ISPs and cybercafé owners, should be responsible for their customers' messages. He told a foreign journalist in January 2003 that just as restaurant owners had to ensure their food contained nothing harmful, cybercafé owners were not allowed to serve poison to their young customers.

The government newspaper *Thoi bao Kinh te Vietnam* (Vietnam Economic Times) said on 26 June that the government planned to set up a national monitoring system to ensure that cybercafé users did not see "politically or morally dangerous" websites. It said the culture and information ministry had reported "very many" violations of the law about spreading subversive material and publishing state secrets. Prime Minister Phan Van Khai ordered police on 24 June to inspect the country's 4,000 cybercafés.

Five cyber-dissidents arrested in 13 months

Le Chi Quang, a 31-year-old computer teacher and law graduate, was arrested on 21 February 2002 in a Hanoi cybercafé and charged with sending "dangerous" information abroad. Police seized computer equipment and papers from his home and he was sent to the B-14 prison camp near Hanoi. He was arrested after posting on the Internet a very detailed article he wrote called "Beware of the empire to the north," about the circumstances of the government's signing of border agreements with China in 1999. The article was very widely distributed among Vietnamese abroad.

He was sentenced to four years in prison on 8 November and three years of house arrest after that for "opposing the government of the socialist republic of Vietnam" under article 88 of the criminal code banning the distribution of anti-government material.

During his three-hour trial, the rights of the defence were flouted and the foreign media were not allowed to attend. Only his parents were allowed to be present. His mother said he admitted posting the article but rejected the government's accusation and that the family would appeal against the sentence. He appeared to be physically very week and his face was swollen. Friends said he had kidney problems and that the prison authorities had refused him treatment. Nearly 100 people, including dissidents, demonstrated outside the courthouse and police arrested one of them.

Police searched the house in Ho Chi Minh City of Tran Khue, a literature teacher and founder of an anti-corruption group, on 8 March 2002 and confiscated his computer, printer, camera, mobile phones and papers. Two days later, he was put under house arrest. He had earlier posted on the Internet a letter he had written to Chinese President Jiang Zemin on the eve of an official visit to Vietnam demanding that he revise some clauses of the border agreements. In August 2001, Tran Khue had been arrested and escorted home when he was found near the border with China investigating the situation there.

Members of the special P4-A25 police unit went to the Hanoi home of Dr. Pham Hong Son, the local representative of a foreign pharmaceutical company, on 25 March and took him in for questioning about his translation of articles on the website of the US embassy in Vietnam. Shortly afterwards, eight members of the police unit searched his home and took away computer material and personal papers. He returned to the police the next day to get them back but was turned away. A day later, he posted online an open letter protesting against the illegal search and confiscation of his property. Two days after that, on 29 March, his family reported he had vanished. His mother was not allowed to visit him in prison until 15 April.

The family were told he had been arrested for translating and posting online an article from the US embassy website called "What is democracy?" He has also written many articles himself, such as "Promoting democracy: a key part of the new world order" and "Sovereignty and human rights: the search for reconciliation," which have

appeared on pro-democracy online forums Danchu.net and Ykien.net. On 29 April, he was reportedly at the B-14 prison camp. His wife Ha Thuy Vu and their two sons were forced to leave their home after harassment and threats. In July, the interior ministry said the cyber-dissident would stay in prison.

Police searched the house of journalist Nguyen Vu Binh on 25 September, seized his personal belongings and took him to the B14 prison camp. He wrote for the magazine section of the Communist Party newspaper *Tap Chi Cong San* but was dismissed in January 2001 for trying to set up an independent political party. Since then, he has written articles criticising the government.

He had been briefly arrested on 19 July for sending a written report to a human rights conference in Washington DC. He was freed the next day but put under house arrest and closely watched by police, who he had to report to every day. In August, along with 20 other writers and dissidents, he signed a petition to the government calling for reform of the judiciary and creation of an independent anti-corruption squad. The authorities have not said why he was arrested this time, but it may have been for posting online in August a critical article he wrote about the sensitive topic of border agreements signed with China.

Cyber-dissident Nguyen Khac Toan was jailed for 12 years on 20 December by a "people's court" in Hanoi for "spying" after e-mailing material to allegedly "reactionary"Vietnamese human rights organisations abroad. His rights to a fair trial were ignored and the hearing, which lasted only a few hours, was held in secret, in violation of article 131 of the national constitution and without even family members present. He was only allowed to see his lawyer twice, a few days before the trial, but was not able to talk to him in private. Toan, a former army officer, was arrested on 8 January in a Hanoi cybercafé and was being held in the B14 prison not far from Hanoi.

Dr Nguyen Dan Que, editor of the underground magazine *Tuong Lai* (The Future) and author of many articles posted on the Internet, was arrested at his home in Ho Chi Minh City on 17 March 2003. A few hours later, police returned to the house and seized his computer, mobile phone and many personal papers. His arrest was thought to be linked with a statement he put online criticising the lack of press freedom in the country. He was responding to remarks made by a foreign ministry spokesman on 12 March that freedom of information was guaranteed.

He has already spent nearly 20 years of his life in jail and is being held at the main prison in Ho Chi Minh City. He studied medicine at Saigon University and was arrested in 1978 and held without trial for 10 years. He was arrested again in 1990 after campaigning for democracy and sentenced to 25 years imprisonment, including 20 at hard labour. He was freed in an amnesty in 1998, but was still frequently interrogated and his home repeatedly searched. He was also publicly and regularly vilified by the Ho Chi Minh City state security department.

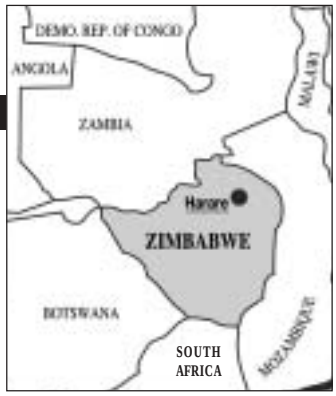
LINKS:

• www.vnpt.com.vn
Ministry of posts and telecommunications

• web.amnesty.org/library/eng-vnm/index
Amnesty International news about Vietnam

• www.vnn.vn
Government information site

• www.rfa.org/service/index.html?service=vie
Radio Free Asia



Zimbabwe

POPULATION: 12,852,000
INTERNET USERS: 500,000
PRIVATELY-OWNED ISPS: YES

Zimbabwe is one of the most-connected countries in Africa, but in 2000 the government passed a law to monitor e-mail. The open warfare waged by President Robert Mugabe against the independent media and locally-based foreign correspondents led in 2002 to passage of a press law that seriously threatens freedom of expression. It was used to prosecute a journalist who had an article posted on the website of the British daily *The Guardian* that the government objected to.

More and more Zimbabweans are logging on to the Internet, especially in the dozens of cybercafés that have opened in the capital, Harare, and major towns. But soon they may not be able to look at websites that contain criticism of President Robert Mugabe's iron rule.

The government pushed through the Posts and Telecommunications Act in November 2000 which regulated online activity by allowing the security services to monitor phone calls and e-mail. The law obliges ISPs and other operators belonging to the Computer Society of Zimbabwe to supply information to the authorities on request and give police and intelligence officials access to their equipment.

Censorship and intimidation of journalists sharply increased in 2001 and early 2002 for those who dared criticise President Mugabe and reporters from the independent media were frequently arrested and foreign correspondents deported.

At the end of 2001 and during 2002, the government banned most foreign (mainly British) publications but their articles could still be read on their websites. This was the government's argument in prosecuting Andrew Meldrum, local correspondent for the British daily *The Guardian*, the weekly *The Economist* and *Radio France International* (*RFI*), in June 2002.

It was the first trial of a journalist under the 2002 Access to Information and Protection of Privacy Act. Meldrum was accused of "abuse of journalistic privileges" and "publishing falsehoods."

He had reported in *The Guardian* an item carried by the independent Zimbabwean paper *The Daily News* that said activists of the ruling ZANU-PF party had beheaded a woman in a village in the northwest of the country. A few days later, *The Daily News* admitted that the incident had not been confirmed and apologised to the ZANU-PF. Two of the paper's journalists, Lloyd Mudiwa and Colin Chiwanza, were arrested on 30 April and Meldrum was picked up the following day.

Since *The Guardian* newspaper is banned in Zimbabwe, the government accused it of publishing the article in the country through its website. A Harare court cleared Meldrum of all charges on 15 July.

LINKS:

• www.csz.org.zw
The Computer Society of Zimbabwe

• www.dailynews.co.zw
The newspaper *The Daily News*

Is the United Nations against freedom of expression

BY CLAUDE MOISY
TRUSTEE, REPORTERS WITHOUT BORDERS

Can it be that the United Nations, guardian of the Universal Declaration of Human Rights, is giving a hand to the enemies of freedom of expression and the free flow of information?

The World Summit on the Information Society, jointly organised in Geneva this December by the UN, will officially aim to narrow the "digital divide" between rich and poor nations. But during the past two years of preparations, many countries that crack down on freedom of expression have been taking advantage of this goal to suggest rules that would allow them to curb the free flow of information on the Internet.

Some of their proposals hark back to the "New World Information and Communication Order" that nearly destroyed UNESCO about 20 years ago. It is not unfair to say that the idea behind the new elitist approach is that freedom of information is not so much an individual right as a collective one best exercised by governments.

The grave danger today is that the chaotic way the Internet has expanded gives governments sometimes legitimate excuses to try to restore some order to it. For some, that means preventing it being used by terrorists, organised crime, money-laundering and paedophiles. Others do not want commercial and personal copyright to be rendered meaningless by the free exchange of original material the new technology makes possible. And some want to ensure growth of the Internet does not increase the domination of one language and culture.

Democracies may be inclined to adopt Internet surveillance systems that respect basic individual rights and the free flow of information. But we know only too well how consistently authoritarian regimes abuse legitimate measures so as to gain complete control of news and free expression. The recent annual reports of Reporters Without Borders and other such organisations show that regimes that refuse to allow the traditional media to be independent are the first to try to block free access to the Internet.

Preparatory intergovernmental conferences for the Geneva summit have revealed some alarming attitudes in the shape of proposals about freedom of information for the Declaration of Principles and the Action Plan the summit is due to adopt. Some call for recognition that the Internet can be used for ends that are incompatible with international stability and security and

that can harm a country's unity, infrastructure and economy. This is perhaps not entirely false, but it can be used to justify all kinds of censorship by paranoid regimes. Just like at the time of the New World Information Order, people are again talking about readjusting the balance of news and respecting national sovereignty in putting out stories.

Just as worrying is a proposal about supposed new ways of looking at human rights, basic freedoms, economic progress and social justice. This is like the old chestnut of China's demand for local conditions to be taken into account where human rights are concerned. In other words, every government should be allowed to decide what is good for the people.

National and international media, especially those online, have every reason to distrust another new attitude, likewise being presented as an advance in human rights. This is the "right to communicate," as a basic human right that cannot be restricted to media organisations. At first sight, it seems to support freedom of expression. But what it actually means is that media outlets will violate human rights if they refuse to allow anyone to express their views in a newspaper, on radio or TV or on a website, even if those rights have not been challenged. Giving "a right of reply" already involve technical problems. Recognising such a "right to communicate" would make it impossible to operate the media.

Many press freedom groups, including Reporters Without Borders, have given the organisers of the Geneva summit a set of demands they intend to press strongly. They state the principle that new technology provides a means of communication that, like others, does not need to have special laws passed about it. The groups say the media should have the same rights

and freedoms on the Internet and on international satellite networks as the traditional media have. They demand that the summit's Declaration of Principles stresses that, where freedom of information is concerned, Article 19 of the Universal Declaration of Human Rights is paramount and applies to all the new technology as it does to the old.

Several more preparatory meetings are to be held before the December summit. But the governments that are harshest towards the media have so far shown they are not interested in discussing such matters with "civil society," even though UNESCO, which is part of the summit, has shown sympathy for the position of the press freedom organisations.

These groups are well aware that their concerns are only one aspect of the summit, whose main aim is to put new information technology at the service of the most undeveloped parts of the world so people there can have a chance of a better life. But they object to this laudable goal being exploited by the enemies of press freedom to get the United Nations to rubber-stamp new obstacles to independent news.

The fears of those who defend freedom have been revived by the spectacle in recent times of the UN Commission on Human Rights (some of whose members are among the world's worst rights abusers) which refuses to condemn the situation in countries such as China and Cuba. Also, the second session of the Information Society Summit is to be held in 2005 in Tunisia, whose president has long been on the Reporters Without Borders worldwide list of predators of press freedom and has already staged trials of Internet users and thrown them in prison.

CLAUDE MOISY
TRUSTEE, REPORTERS WITHOUT BORDERS

CONTENTS

REPORTERS WITHOUT BORDERS

International secretariat

5, rue Geoffroy-Marie 75009 Paris, France

Tél. : 33 . 1 . 44 . 83 . 84 . 84

Fax : 33. 1. 45 . 23 . 11. 51

Web :

www.rsf.org

Notes

Notes

Notes

Notes

Notes

Notes

Notes

Notes