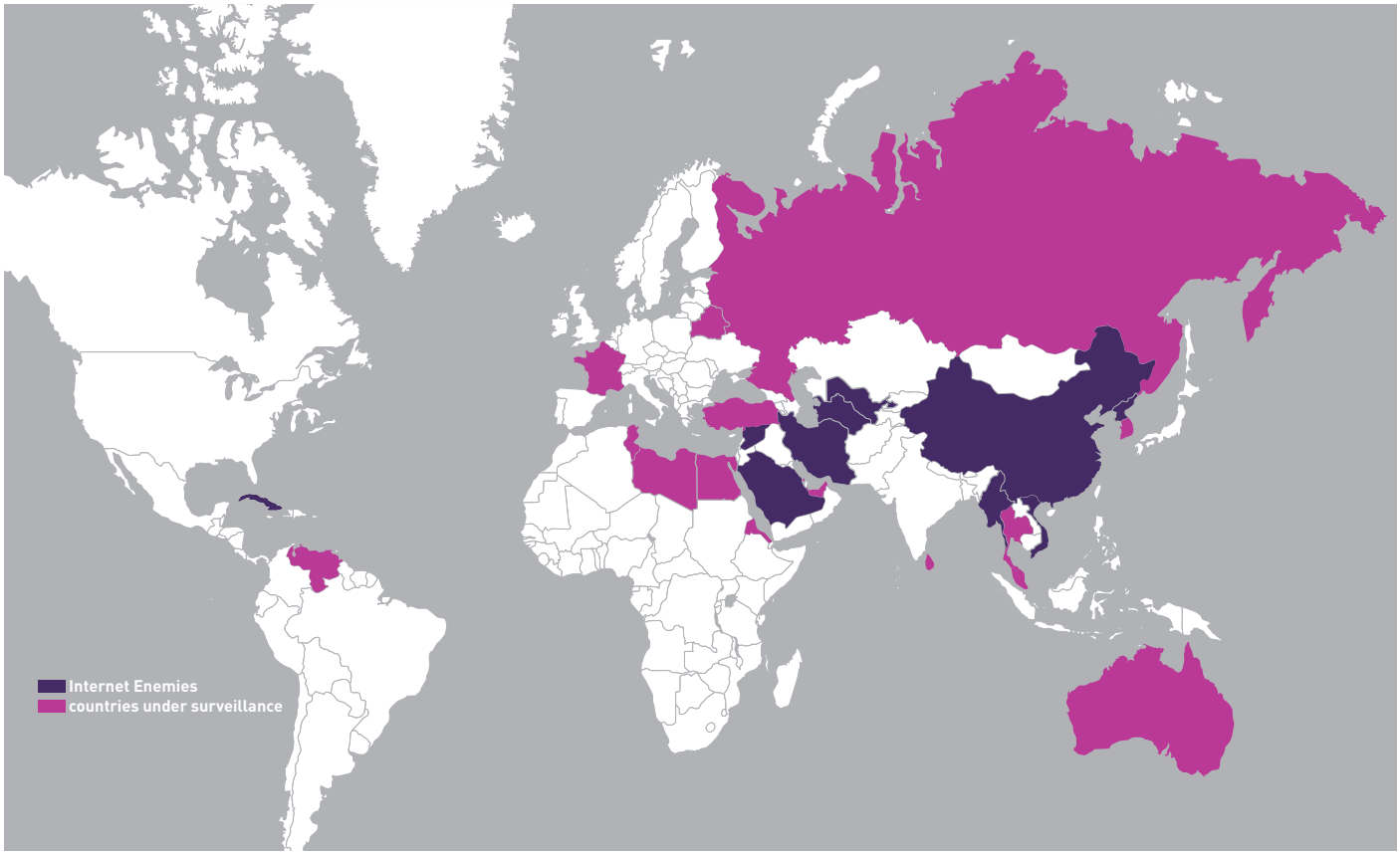
MARCH 2011

INTERNET ENEMIES

REPORTERS WITHOUT BORDERS
FOR PRESS FREEDOM

WORLD MAP OF CYBERCENSORSHIP



THE NEW MEDIA:

BETWEEN REVOLUTION AND REPRESSION, NET SOLIDARITY TAKES ON CENSORSHIP

ARAB SPRINGTIME: IS THE WEB REACHING NEW HEIGHTS?

The year 2010 firmly established the role of social networks and the Internet as mobilisation and news transmission tools. In 2010 alone, 250 million Internet users joined Facebook and by the end of the year, the social network had 600 million members. In September that year, 175 million people were Twitter users – 100 million more than in the previous year.

The Western media had praised the Internet and its "liberator" role during the 2009 Iranian revolution. According to The New York Times, the demonstrators "shot tweets" back at bullets. However, Twitter was then used mainly by the diaspora. "The Net Delusion," a theory advanced by Evgeny Morozov, an Internet expert, casts doubt on the Internet's role as a democratisation tool. Although the Internet is certainly used by dissidents, it is also used by the authorities to relay regime propaganda and enforce a police state.

The Internet remains above all a tool used for the better or the worse. In the most closed countries, it creates a space of freedom which would not otherwise exist. Its potential to disseminate news irritates dictators and eludes traditional censorship methods. Some regimes use it – mainly on Facebook and Twitter – to monitor dissidents and infiltrate their networks.

Nonetheless, the terms "Twitter Revolution" and "Facebook Revolution" have become watchwords with the events that rocked the Arab world in late 2010 and early 2011. The "online" movements were coupled with "offline" demonstrations, hastening the fall of dictators. The Tunisian and Egyptian uprisings turned out to be, first and foremost, human revolutions facilitated by the Internet and social networks.

Facebook and Twitter served as sound boxes, amplifying the demonstrators' frustrations and demands. They also made it possible for the rest of the world to follow the events as they unfolded, despite censorship. The role of cell phones also proved crucial. Citizen journalists kept file-sharing websites supplied with photos and videos, and fed images to streaming websites.

The Tunisian authorities had imposed a media blackout on what was going on in Sidi Bouzid. Since the so-called "traditional" media had failed to cover the protest movements that were rocking the country, at least at their beginning in December, their role as news sources and vectors was taken over by social networks such as Facebook and Twitter, and news websites like Nawaat.org. Facebook in particular acted as a platform on which Internet users posted comments, photos and videos. The Bambuser streaming site also had its moment of glory. Everyone was able to track the events as they happened. The online calls for demonstrations spread to other countries: Egypt, Libya, Yemen, Bahrain, Oman, Syria, Iraq, Morocco, and even China and Vietnam, etc.

CONTROL 2.0 GAINS STRENGTH

CENSORSHIP AND REPRESSION INTENSIFY

Authoritarian regimes' latest strategy is no longer to use pure and simple blocking as it is to use, but rather online tampering and propaganda. Naturally countries such as China, Saudi Arabia and Iran are still practicing strict filtering, which they tend to tighten during periods of unrest, notably with regard to micro-blogging sites and social networks. Meanwhile, their netizens keep on learning new ways to circumvent censorship. China in particular has reinforced its "Electronic Great Wall" and is tackling the anonymity of Internet and cell phone users. Uzbekistan,

Syria, Vietnam – to name but a few – have enhanced their censorship to stifle the echoes of the revolutions agitating the Arab world.

Currently, one out of every three Internet users is unable to access a free Internet. Net censorship is becoming the norm. Around 60 countries are implementing some form of Internet censorship, which entails either content filtering or netizen harassment. Others may well join their ranks in the months and years to come. For the first time, Bangladesh has blocked access to certain sites because of videos deemed offensive to the Prophet. Cambodia is censuring news sites.

Blogger and netizen arrests have continued and remained at the same level in 2010 as in 2009. As of this writing, 119 netizens are behind bars, as compared to 120 in 2009. Although 2010 saw the release of several popular bloggers such as Kareem Amer in Egypt a few days after serving his sentence, and Adnan Hadjizade and Emin Milli in Azerbaidjan, the authorities are finding new ways to hinder bloggers' and cyberdissidents' freedom of action. The number of false releases – such as that of Mongol cause activist Hada, in China – or forced disappearances, is growing, and so are house arrests. As for self-censorship, which is hard to quantify, it appears to have gained ground.

The world's biggest prisons for netizens remain: China (77 netizens), Vietnam (17) and Iran (11). A new wave of arrests in Vietnam preceded the January 2011 Communist Party Congress. The Chinese regime launched a series of arrests in February 2011 following online calls for demonstrations triggered by the Arab uprisings. The authorities feared that they would spread. For the first time in China, Twitter users were arrested for their posts on the social network.

AS OF THIS WRITING, 119 NETIZENS ARE BEHIND BARS

One such prisoner is no other than Liu Xiaobo – the winner of the 2011 Nobel Peace Prize, the only Nobel Peace Prize laureate currently in jail. The announcement of this news in December 2010 resulted in an unusually violent crackdown by the authorities: any reference to this award on micro-blogging sites is being censored and they are questioning or placing under house arrest hundreds of supporters and friends of the human rights activist and freedom defender.

In Iran, imprisoned netizens were sentenced to death for the first time. Blogger Hossein Derakshan, known as the "father of the Iranian blogosphere," received the most severe prison sentence: 19.5 years.

In this "Control 2.0" era, several tested methods are used simultaneously by the authorities to prevent dissidents from ruling the web and to maintain better control over the regime's disinformation.

BROADER RECOURSE TO PROPAGANDA AND MANIPULATION

First, the use of distributed denial-of-service (DDoS) cyberattacks has become commonplace, as has phishing, which involves stealing user passwords. One of the episodes which received the most media coverage is undoubtedly the pirating of Google's website and those of some 20 other companies in China in late 2009 and early 2010. Vietnam also uses cyberattacks to muzzle dissident opinions. Independent news websites based abroad and those which discussed bauxite mining were targeted in 2010. Burma not only attempted to immobilise several independent online media, but also tried to shift the blame for the bandwidth speed slowdown on hackers acting against the country's interests. Another weapon used by dissidents in Iran was the "Green Cyber Army," which attacked some government websites. The "Hackivists Anonymous" group paralysed the Tunisian president's and parliament's website in January 2011 as part of its "Operation: Tunisia."

In 2010, authoritarian regimes sought to control their country's Internet connection speeds by slowing down bandwidth during elections or periods of social unrest. Connection speed became the barometer of a country's political and social situation. Iran has become an expert in this technique, and used it just before and during every demonstration organised by the opposition. Ben Ali's and Mubarak's divested regimes also resorted to it. Often such disruptions are accompanied by jamming or shutting down cell phone networks in the areas concerned, such as Tahrir Square in Cairo.

Another Iranian strategy which proved successful in Belarus during the demonstrations over the re-election of President Lukashenko was redirecting users of opposition websites (or those critical of the regime) to pseudo-sites with similar, yet more pro-government, content.

In addition, every government seeking to control the net has vested itself with a cyberpolice force equal to its ambitions and which, particularly on social networks, closely monitors dissident activities. It has also deployed groups of "sponsored" bloggers paid to post online pro-regime comments, thereby eclipsing critical opinions. Russian brigade and "50-cent party" bloggers are experts at this. Initially, the authorities had used repression to counteract their opponents' use of the Internet, but now they are displaying their own content.

INTERNET DISRUPTIONS: A DRASTIC AND COSTLY MEASURE

Extreme measures which ultimately failed were taken in Egypt, and then in Libya, to try to put an end to protest movements against the incumbent leaders. In the evening of 27 January 2011, Egypt virtually cut off Internet access for five days, causing its economy a loss of at least USD 90 million, according to the Organisation for European Co-Operation and Development (OECD), which shows to what extent the Internet is an integral part of the global economy and essential to a country's economy. In Libya, the authorities first severed Internet access on 19 February, then maintained strong Internet disruptions after that and cut it off again on 3 March. It was not the first time that Internet access was totally suspended in a country. This occurred in 2005 in Nepal and in 2007 in Burma. However, such measures stir up strong reactions worldwide and further exacerbate demonstrators' resentment. It also induces the latter to resort to more creative ways to freely distribute information, despite the odds. Netizens have either resumed using earlier Internet methods (modem, fax, etc.) or have adopted the latest generation of technologies (phone-based tweet system set up by Google and Twitter).

CERTAIN REGIMES SOMETIMES INTENTIONALLY MAINTAIN INFRASTRUCTURAL PROBLEMS TO KEEP THEIR POPULATIONS FROM HAVING INTERNET ACCESS.

Burma learned its lessons from the 2007 Internet suspension and undertook a broad revamping of its national platform, to make certain that access providers would provide distinctly separate services to the population, the government and the military, thereby ensuring that the junta will be prepared, in the next crisis, to cut off Internet access to its citizens without being directly affected itself.

Certain regimes sometimes intentionally maintain infrastructural problems to keep their populations from having Internet access. The 2011 commissioning of the fibre optic undersea cable linking Cuba to Venezuela, which expanded bandwidth potential, therefore will eliminate one of the Cuban regime's excuses about access problems.

North Korea, on the other hand, launched its own pages on the online social networks in 2010, and is said to have initiated its first connections to the World Wide Web. The latter are apparently very limited, however, and are being run by the regime for propaganda purposes.

THE NEW VS. TRADITIONAL MEDIA: IS SYMBIOSIS AN OPTION?

There is truly no longer any reason for the long-lasting gap between the new and the traditional media. In the last few months, they have proven to be increasingly complementary. According to BBC Global News Direct Peter Horrocks, it is imperative for journalists to learn how to use social networks: "It is not an option." The new media have become key tools for journalists. At the same time, by flooding social networks with news and pictures, Arab revolutionaries were also seeking to ensure that the international media covered news events in order to put pressure on their governments and on the international community.

News staff now use Twitter and Facebook to find ideas for news stories, gather first-hand accounts and visuals, and to disseminate their own articles in order to expand their readership. The shelf life of an article no longer ends with the printing of a newspaper; it now has an extended life online.

According to a study conducted on print and web journalists by the Cision research company and George Washington University, 56% of the respondents responded that social media were "important or somewhat important" for researching and writing the stories they wrote. Blogs were still the main source for the respondents (89%). Micro-blogging was a source for 69% of the web journalists. However, these journalists remain cautious: 84% of them were aware of reliability problems with information gathered from the social media.

The instantaneous nature of social networks and streaming tools permit real-time coverage of critical events such as natural disasters (earthquake in Chili, floods in Pakistan), demonstrations (in Tunisia, Egypt, etc.), but makes media professionals' verification work tougher, yet essential. It is sometimes hard to separate the true from the false, which is why it is important to form a network of reliable contacts who can corroborate the "scoops" made by citizen journalists or ordinary netizens.

Any witness of a trivial or historical event becomes a chance informant. Journalists are no longer the only ones who filter information – their work is also being scrutinised by their readers.

Numerous unknown factors persist in the relations between the new and traditional media. Certain newspapers such as the Washington Post prohibit their journalists from offering their personal opinion on the Internet, out of fear that it might be interpreted as the newspaper's editorial policy. The New York Times and Reuters have issued internal guidelines for using social networks. They encourage their journalists to use them, but also make sure they are aware of the inherent risks involved. Reuters specifies that no scoops should be posted on social networks because the former are reserved mainly for press agency clients. Journalists are free to share their articles online, create an online network, invite comments from readers and post live tweets on the events they cover. However, they must obtain their supervisor's permission to open a professional account and they are required to maintain separate personal and professional accounts.

WIKILEAKS: INEVITABLE TRANSPARENCY

This collaboration between the new and traditional media is exemplified by changes in WikiLeaks' strategy. Initially focused on the massive release of unedited confidential documents, the website gradually developed partnerships with several international media leaders ranging from The New York Times to Le Monde, and The Guardian to Al-Jazeera. This strategy allowed it to combine the new media's assets (instantaneousness and a virtually unlimited publishing capacity) with those of the traditional media (information checking and contextualisation, thanks to journalists specialised in the issues covered). More than 120 journalists of diverse nationalities worked together to decipher the diplomatic cables released by WikiLeaks, and to remove the names of civilians and local informants from said documents in order not to put them at risk.

The series of close to 400,000 confidential documents belonging to the U.S. Army concerning the war in Iraq which WikiLeaks released helped to expose the magnitude of the crimes which coalition forces and their Iraqi allies had committed against civilian populations since 2003. Reporters Without Borders denounced the pressure which U.S. and Iraqi authorities have placed on the website and asked these two governments to demonstrate transparency and to reconsider their document classification methods. Strong pressures are also being placed on WikiLeaks' collaborators. Founder Julien Assange has been repeatedly threatened. U.S. Army Private Bradley Manning, suspected of being one of WikiLeaks' sources, has been held in solitary confinement since his arrest in May 2010 and is facing life imprisonment. After being subjected to cyberattacks and being dropped by several host sites, WikiLeaks called upon its worldwide supporters on 5 December 2010 to create mirror websites. Reporters Without Borders decided to host one of them on its website. In December 2010 a number of media and websites – including Le Monde, El Pais and Al-Quds Al-Arabi in Morocco – were censored for having relayed the cables. Access to the website is notably blocked in China and in Thailand. The site is accessible in Pakistan, but some pages containing wires about Pakistan are blocked.

Reporters Without Borders wrote to the U.S. Attorney General to ask him not to prosecute Julian Assange and WikiLeaks' collaborators in view of the fact that the publishing by WikiLeaks and its five associated media of information – even classified – in an effort to inform the public is a activity promoting the right to information guaranteed by the First Amendment.

INTERNET: THE "I LOVE YOU – ME NEITHER" QUANDARY OF DEMOCRACIES

In a historic speech on January 2010, U.S. Secretary of State Hillary Clinton referred to online freedom of expression as the cornerstone of American diplomacy – a position that she reasserted in February 2011 in an address in which she reminded her audience that "On the spectrum of Internet freedom, we place ourselves on the side of openness." Nonetheless, the principles raised by

Hillary Clinton conflict with the treatment reserved for WikiLeaks. Several days prior to WikiLeaks' publication of the documents, the Pentagon had asked the media "not to facilitate the leak" of classified documents concerning the war in Iraq, claiming that it would endanger national security. American officials made some very harsh statements about the site's founder. Judicial action may still be taken against the website. According to Hillary Clinton, "the WikiLeaks incident began with an act of theft" of government documents. However she stated that "WikiLeaks does not challenge our commitment to Internet freedom."

Security trends tend to affect the web. Blackberry maker RIM is facing growing pressures from the Gulf States, as well as from Indonesia and India, who are trying to gain access to the content of its secured communications on the pretext of the fight against terrorism.

Apart from national security and cybersecurity, other problems are persuading democratic governments to relativise their commitment to a free Internet.

NONETHELESS, THE PRINCIPLES RAISED BY HILLARY CLINTON CONFLICT WITH THE TREATMENT RESERVED FOR WIKILEAKS

The Internet will be discussed during the next G20 meeting, not from the vantage point of freedom of expression, but of protecting intellectual property.

In the name of copyright protection, the French government adopted a law which makes it possible, after issuing warnings, to suspend the Internet connection of an individual suspected of illegally downloading copyrighted files online. This "graduated response" scheme, known as the "three strikes" and introduced by the Hadopi law, has inspired other countries, notably the United Kingdom with its Digital Economy Act. Spain's Sinde Law also provides measures for website blocking subject to a court order.

In addition, the French Parliament passed an internal security law ("Loppsi 2") which provides for an administrative filtering of the web – a dangerous principle – in the name of the fight against child pornography. The Australian filtering system, which has already been tested, has been put on hold, even though the government has not totally abandoned this project.

The highly controversial Hungarian media law could have some bad consequences on online media and bloggers because it can impose penalties and contains provisions which may jeopardise the full exercise of journalists' professions and the transmission of information.

Italy, on the other hand, attempted to regulate the posting of videos online by means of a March 2010 decree. Every website which regularly disseminates videos must now submit a "Statement of Activity" to the Italian Telecommunications Authority (AGCOM). This decree's scope of application was ultimately reduced to online television stations and no longer applies to traditional websites, blogs, search engines, or electronic versions of dailies, magazines and online betting.

The principle of Net neutrality seems to be increasingly at risk. In December 2010 in the United States, the Federal Communications Commission (FCC) adopted various measures concerning net neutrality which centred around two principles: that Internet service providers must ensure transparency regarding their Internet management and the prohibition of any discrimination in the manner "legal" contents are transmitted. However, such measures could leave the door open for the filtering of illegal websites and thereby signal the end of the unlimited Internet. Unlike President Obama, the Republican opposition opposes these measures and has challenged the legitimacy of the Commission's authority to rule on this issue. In France, on the pretext of potential traffic saturation, the Minister of Industry, Energy and the Digital Economy is calling for a regulation of Internet traffic and for abandoning the Net's absolute neutrality principle.

CORPORATE SOCIAL RESPONSIBILITY: MORE TIMELY THAN EVER

Google has kept its promises and has stopped censuring its search engine's results in China. Google.cn users are now being redirected to their Hong Kong-based website. Despite the boldness of this move and the cold reception it received from Chinese authorities, the company managed to get its Chinese operating licence renewed in the summer of 2010.

Microsoft and Yahoo! continue to practice self-censorship in China. However, Microsoft, after realising that the fight to prevent the pirating of its software in Russia was a pre-

text used by the authorities to justify the seizure of computers belonging to the media and to NGOs, took measures to supply the latter with pro bono licences. These three U.S. companies have signed the Code of Conduct of the Global Network Initiative, a coalition of NGOs, companies and investment funds seeking to promote good practices in countries which are censoring the Net.

For the first time in Egypt, companies such as Facebook, Twitter and Google have set aside their reticence and openly sided with protecting online freedom of expression. Facebook believes that "no one should be denied access to the Internet." Google and Twitter set up a system to enable telephone tweeting in order to bypass net blocking in the country. YouTube made its political news channel CitizenTube available to Egyptians who want to circulate their videos. Users do not run much risk on the site and should benefit in terms of image capabilities.

In the last few months, cell phones – particularly during the Arab Springtime – cell phone communications have been the focus of harsher controls. In countries such as Libya and Egypt, telephone carriers have been forced to occasionally suspend their services in some locations and to transmit SMS to the population. In early February 2011, Vodafone, Mobinil and Etisalat, pressured by the army, sent their Egyptian customers an SMS informing them of a demonstration in support of Hosni Mubarak being held that day. The headquarters of Western foreign companies apparently protested … after the fact.

These issues do not just concern companies in the new technologies and telecommunications sectors. PayPal's online payment service, based in the United States, decided to suspend WikiLeaks' account, claiming that its terms of use prohibit using its service "to encourage, promote, or facilitate any illegal activity." Visa and MasterCard made the same decision and suspended payments directed to the site until they have the results of internal investigations.

THE ENEMIES OF THE INTERNET 2011 LIST: NEW ADDITIONS AND REPEAT OFFENDERS

The most net-repressive countries which deserve the label "Enemies of the Internet" are, once again this year, Saudi Arabia, Burma, China, North Korea, Cuba, Iran, Uzbekistan, Syria, Turkmenistan and Vietnam. They often compound Internet repression with strict filtering, access problems, cyberdissident surveillance and online propaganda.

Tunisia and Egypt have been dropped from the "Enemies of the Internet" list and added to the "Countries under Surveillance" list The lifting of censorship in Tunisia and the collapse of Mubarak's regime in Egypt are encouraging signs for the future of online freedom of expression in these countries, a right which ranked high in demonstrators' demands. Nonetheless, vigilance will be needed until the censorship and surveillance apparatus has been dismantled. The authorities must demonstrate transparency in this regard.

Among the countries still "under surveillance": Australia is still considering implementing a dangerous mandatory filtering system. Bahrain is vacillating between intensifying filtering and releasing bloggers. In Belarus, elections have ushered in a new era of repression against the online media. South Korea is tightening censorship of North Korean propaganda and maintaining a repressive legislative arsenal. In the United Arab Emirates, filtering and surveillance are getting worse. In Eritrea, the police state is keeping its citizens away from the web and monitoring netizens. In Malaysia, bloggers – a more credible source of news than the traditional media – are under constant pressure. In Russia, the government is trying to shape the increasingly influential Russian net to suit its own purposes. Sri Lankan online journalists and media are still victims of violence. In Thailand, the spring 2010 crisis has had negative consequences for online freedom of speech. And in Turkey, thousands of websites are still blocked and legal procedures against online journalists continue unabated.

This year, several countries were added to the Countries under Surveillance list, including France, which enacted a law providing for the administrative filtering of the Net and the "graduated response" procedure as part of the authorities' idea of a "civilised" Internet. The year 2010 was difficult for several online media and their journalists who had to endure office break-ins, court summons, and pressure to identify their sources.

Venezuela was also placed "under surveillance." While there is still free access to the Internet in the country despite a climate of increasing tension between the leadership and the dissident media, censorship tools are now in place in the form of an Internet gag law and the

growing use of self-censorship. Discussion forums are in the authorities' line of fire.

Colonel Kadhafi's Libya also joins this list. Amidst the chaos, the regime has been trying to implement a nation-wide information blackout in an attempt to silence any news about the uprising and the way it was quashed.

This is by no means an exhaustive list of all attacks on online freedom of expression. In 2010, the Pakistan regime's attitude has raised much concern. A judge had ordered Facebook to be fully blocked after it posted videos considered disrespectful to the Prophet. The authorities reversed their decision, but promised to keep monitoring the web. Kazakhstan will need to be observed during the run-up to the presidential election.

As of this writing, protest movements continue to sweep through the Arab world and spread to other countries. They may give rise to new online mobilisations and to crackdowns by certain governments. In 2011, the Internet and new media are still experiencing shock waves from having been caught up in the momentum of all these political changes. The Internet has entered turbulent times in which its impact, power and frailties are likely to be magnified.

Lucie Morillon,
Responsible of the New Media Desk
Jean-François Julliard, General Secretary

BURMA

INTERNET ENEMY

Domain name: .mm
Population: 53 414 374
Internet-users: 300 000
Average charge for one hour's connection at a cybercafé: about 0,55 US$
Average monthly salary: about 27,32 US$
Number of imprisoned netizens: 2

Burma took drastic measures in 2010 to reorganise the country's Internet and to arm itself with the means, at the next sign of a crisis, to cut off its population's Web access without affecting official connections. Prior to the November 2010 elections – the first in twenty years – censors resorted to massive crackdowns, intimidation and cyberattacks to reduce the risk of any negative coverage. Tampering is now at its height.

WIDESPREAD NET CENSORSHIP IN BURMA

The regime is enforcing harsh and widespread Internet censorship. The Burmese firewall restricts users to an intranet purged of any anti-government content. Blocked websites include exiled Burmese media, proxies and other censorship circumvention tools, certain international media, and blogs and sites offering scholarships abroad.

In an interview granted to Rolling Stone magazine, American hacker and WikiLeaks member Jacob Applebaum, exposed the scope of the censorship by showing that only 118 of the country's 12,284 IP addresses are not blocked by the regime and have access to the World Wide Web. He also showed how vulnerable the network is the event of attacks.

Censors may also be counting on the complicity of Western companies. Some Burmese Internet service providers acquired censorship equipment and hardware from the Chinese subsidiary of the Franco-American company Alcatel-Lucent. On March 24, 2010, Reporters Without Borders and the Sherpa Association sent a letter to Alcatel-Lucent's management to ask for explanations, notably about the sale in Burma Lawful Interception Integrated hardware. The company denied this claim, insisting that it merely supplied telecom infrastructures within the framework of a Chinese-funded project.

Yet in an article appearing in the May 19-25, 2008 issue of the newspaper Myanmar Times, a spokesman for the state-controlled ISP Hanthawaddy confirmed that the Alcatel's Chinese subsidiary did indeed provide a website filtering and surveillance system.

OUTSTANDING BLOGGERS

Despite the regime's iron grip on the Internet, the number of bloggers keeps rising: there are now 1,500 of them, 500 of whom blog regularly. When Burmese bloggers based

abroad are included, this number totals 3,000. Every year, Reporters Without Borders and the Burma Media Association reward Burma's best bloggers. Thousands of Burmese netizens voted for their favourite blogs, and in late February 2010 in Chiang Mai, Thailand, a dozen of them received a prize for the best Burmese blogs. Myanmar E-Books (http://burmesebooks.wordpress.com) was voted the best general category blog. The prize for the best news blog went to The Power of Fraternity: (http://photayokeking.org).

In the months prior to the November 2010 elections, some bloggers stepped up to the plate by keeping their compatriots informed about the elections and the issues at stake. They occasionally disseminated news about the candidate contenders and the electoral laws – critical information rarely relayed by the traditional press, which is subject to stringent pre-run censorship.

Despite the slow connections and risks incurred, Burmese Internet users are still circumventing censorship, reading the foreign press, networking on Facebook or simply enjoying themselves online.

THREE NETIZENS ARE STILL LANGUISHING IN PRISON

Journalists who collaborate with the exiled Burmese media and bloggers are in the authorities' line of fire, particularly since the 2007 Saffron Revolution and the international outcry which followed the mass circulation of images of the ensuing crackdown. The authorities are making unabashed use of a particularly repressive law adopted in 1996, the Electronics Act, to regulate the Internet, TV and radio. This law notably prohibits the import, possession, and use of a modem without official permission, under penalty of a 15-year prison sentence for "undermining state security, national unity, culture, the national economy and law and order."

The Burmese military junta considers netizens enemies of the state. Three of them are in prison for having expressed themselves freely on the Web.

Zarganar, a blogger and comedian known as the "Burmese Chaplin," was arrested on 4 June 2008 after having testified to foreign media outlets – and notably to the BBC World Service – about the Burmese government's poor management practices and guilty silence over the loss of human lives and property caused by hurricane Nargis. He is serving a 35-year prison sentence for violating the Electronics Act.

On 10 November 2008, blogger Nay Phone Latt (http://www.nayphonelatt.net/), who owns three cybercafés in Rangoon, was given a jail sentence of 20 years and six months for having described on his blog how difficult it is for young Burmese people to express themselves freely, especially since the autumn 2007 demonstrations. According to Reporters Without Borders' sources, Nay Phone Latt was allowed to see his parents on 7 October 2010. The young blogger is said to have been deprived of his walking privileges for five months, and to have been confined to his cell. He is allegedly being held in a prison in south-eastern Burma, along with 10 other political prisoners.

From his prison, Nay Phone Latt – who has been denied the care his health problems require – has nonetheless managed to continue his fight for freedom of expression. Blogger Kaung Myat Hlaing ("Nat Soe"), who has already been given a two-year prison sentence, and is wrongfully accused of having participated in the April 2010 Water Festival bombings, was handed an additional 10-year sentence under the Electronics Act. This young man of 22 was interrogated for 10 days and deprived of food, water and sleep. He admitted being a member of the dissident group "Best Fertilizer." He is charged with having taken part in poster campaigns calling for the release of Daw Aung San Suu Kyi and of other political prisoners.

RECONFIGURING THE BURMESE INTERNET BEHIND A SMOKESCREEN

In October 2010, the Burmese junta-controlled Yatanarpon Teleport Company announced the launching of the country's "first national Web portal," a would-be Silicon Valley to be called "Yadanabon Cyber City."

In an exclusive report compiled by local sources entitled "National Web portal – Development or repression?" Reporters Without Borders and the Burma Media Association express concerns that the new Burmese Internet, billed by the government as a huge step forward, may actually be used to bolster the surveillance and repression already imposed on Burmese netizens, while reserving the benefits of faster and improved access for members of the regime.

The deployment of fibre-optic cables will not only allow Internet access but also Voice over Internet Protocol (VoIP) and Internet Protocol Television (IPTV) services because it will increase available bandwidth.

Burmese Internet users will be allocated to three Internet service providers, instead of the two they now have. One will be reserved for the Burmese defence ministry, one for the government and one for the public. Under this system, the government will be able to totally or partially block the population's access without affecting government or military connections. During the 2007 Safran Revolution, since all three "categories" were using the same providers, when the authorities disconnected the Internet to prevent civilians from sharing photos of the ensuing crackdown, members of the military and government were also cut off. What is more, he new architecture will allow the defence ministry to directly control Internet traffic at the point of entry into Burma.

The government and military will be likely to enjoy faster and better Internet performance than the average user, since ISPs will get an "equal share" of bandwidth in each of the three categories, even though the number of users will vary greatly from one ISP to the next. The cost of the new service, which will be passed on to the public, may also curb any growth in the Internet penetration rate, currently at about 2% in a country in which the average salary is 27 U.S. dollars and Internet cafés charge 54 cents per connection hour.

This national portal will supposedly offer an email service (Ymail) and a chat service (Ytalk) as alternatives to Gmail and Gtalk, making it even easier for the authorities to monitor users' online communications.

Lastly, undetectable Internet "sniffers" will be placed on the server reserved for the public to retrieve diverse confidential data. The military junta's ability to spy on netizens and dissidents, thereby restricting freedom of speech even further, will be greatly enhanced.

The Internet access difficulties experienced by local Internet users during recent key events attest to the new portal's timely arrival.

UNRELIABLE INTERNET CONNECTIONS IN THE RUN UP TO THE 7 NOVEMBER 2010: SLOWDOWNS, CYBERATTACKS AND TAMPERING

The elections initiated by the military junta had no credibility, mainly because of the Burmese and foreign media's lack of freedom. Despite the constraints, the Burmese media did their best and managed to offer the public a variety of news and analyses unmatched since the last elections in 1990. However, with all the preceding censorship, intimidations, detentions and expulsions of foreign journalists, stricter liberticidal laws and unreliable Internet connections, the conditions for a free election were far from present.

The military junta made it a requirement for political parties wishing to publish information or their programmes to first have them approved by the Press Scrutiny and Registration Board within 90 days after registering with the Election Commission. The regime announced on 17 March 2010 that the publishing of pamphlets, newspapers, books or other election-related printed material, now falls under the 1962 Printers and Publishers Registration Act, which provides for sentences of up to seven years in prison for disseminating information which is critical of the government or disturbs public "tranquillity."

A drastic slowdown in Internet connections was noted in early October, more than a month after the elections, indicating the authorities' resolve to tighten their control over information. "I can no longer connect to my Gmail account using proxies. Access to all websites based abroad has become terribly slow," a Rangoon-based journalist told Reporters Without Borders. According to Irrawaddy magazine, the capital's cybercafés had closed in advance of the elections.

This slowdown began after cyberattacks in the form of distributed denial of service (DDoS) affected several exiled Burmese media websites such as Irrawaddy and the Democratic Voice of Burma (DVB).

Just a few days prior to the legislative elections, the Burmese Internet network experienced a massive cyberattack. The attacks began around 25 October 2010 and gradually increased in number and severity, causing the country to be regularly disconnected from the Web for se-

veral days. They continued to occur until the elections were over, which made it extremely difficult for journalists and netizens to transmit videos and photos and to do their jobs.

The government shifted the blame to hackers whom they claimed launched the DdoS attacks on the country, but according to Burmese sources contacted by Reporters Without Borders, most of the attacks were allegedly launched by government agents to justify cutting off the Internet. The DDoS's were aimed at Internet service provider Myanmar Post and Telecommunications and constituted – according to the American IT security firm Arbor Networks – an onslaught "several hundred times" more than enough to overwhelm the country's terrestrial and satellite network. They reportedly reached 10 to 15 GB of data per second, a magnitude much greater than in the highly publicised 2007 attacks against Georgia and Estonia.

During the 2007 Safran Revolution, Burmese netizens had circulated news and videos on the authorities' bloody crackdown on monks and demonstrators. The regime subsequently cut off Internet access for several days. Connections are also slowed on key dates such as 8 August – the anniversary of the 1988 political uprising – and during the 2009 trial of dissident Daw Aung San Suu Kyi. After being released on 13 November 2010, the latter announced that she intends to set up a website to showcase her views and those of her political party, the National League for Democracy (NLD)

DAW AUNG SAN SUU KYI: FREE AND CONNECTED?

The well-known Burmese dissident and recipient of the Nobel Peace Prize, who was cut off from all means of communication during her years under house arrest, now has an Internet connection in her home via the state-run ISP, Yatanarpon Teleport. She has declared that she intends to make full use of the Internet and social networks, particularly the Twitter micro-blogging site, in order to more effectively reach Burmese youths in the country and abroad and to hold online discussions. This latter initiative may prove challenging to achieve right now due to the poor quality of the Internet infrastructure. As for the dissident's collaborators, they remain discreet about their role in developing the NLD's online network, as they are subject to a severe penalty under the Electronics Act.

Daw Aung San Suu Kyi is aware that her communications will be closely monitored and that the regime may decide at any time to suspend her Internet access. She has allegedly stated that she has nothing to hide.

CHINA

INTERNET ENEMY

Domain name : .cn
Population : 1 340 000 000
Number of Internet users : 457 000 000
Average charge for one hour's connection at a cybercafé : around 2 U.S. dollars
Average monthly salary : between 220 and 300 U.S. dollars
Number of imprisoned netizens : 77

The Chinese government, exasperated that dissident Liu Xiaobo was awarded the Nobel Peace Prize and concerned about spill-over effects from the Tunisian and Egyptian Revolutions, has drastically tightened its grip on the Web in order to transform it from a protest medium to a tool for political control. Any attempt to challenge the country's stability has been quashed by harsh repression. The regime is taking aim at social networks, particularly micro-blogging websites and online anonymity. New laws now regulate the Web, while Chinese Internet users continue to discuss banned topics and to mock censors.

CENSORSHIP TO ENSURE REGIME STABILITY

THE "GREAT FIREWALL": READY TO SPRING INTO ACTION

China has the world's most consummate censorship system. The Great Firewall combines URL filtering with the censoring of keywords considered "sensitive," ranging from "Tiananmen" to the "Dalai Lama" to "democracy" and "human rights." Censorship is institutionalised and managed by several ministries and administrations. In addition to filtering URLs, the authorities are monitoring the largest blog and micro-blogging platforms, from which they are removing numerous posts and comments. Assistance from foreign companies – mainly in the form of Yahoo ! and Microsoft self-censored search engines – is making their job that much easier. The regime has been known to use the pretext of fighting pornography or the crackdown against the "dissemination of false news" to justify the filtering.

The man who designed the Great Firewall, Fang Binxing, who is also President of the Beijing University of Posts and Telecommunications, defended his creation in early 2011, stating to the newspaper Global Times that censorship met an "urgent" need. Although he had opened a micro-blog account on sina.com, the account was closed a few days later after thousands of netizens left comments blaming him for the control measures he had made possible.

The main news sites, such as the Chinese state-controlled media, regularly receive oral and written directives from the Department of Propaganda specifying what topics can, or cannot, be covered and under what conditions. For example, the Department's directives of January 2011 imposed an information blackout on social and economic

problems and specifically on price increases, anti-government demonstrations and the real estate market, to "reassure" the Chinese people and defend the regime's concept of "fair growth."

TIGHTENING CENSORSHIP IN THE NAME OF NATIONAL SECURITY

On 29 April 2010, China adopted an amendment to the State Secrets Law which requires Internet and telecom companies to cooperate with the authorities on matters relating to national security. Such companies must now block the transmission of vaguely defined state secrets over their networks, keep connection logs and alert the competent authorities to any possible violations. They may also be forced to suppress certain contents.

This amendment thus seems to be yet another warning sent to netizens to induce them to practice more self-censorship, and an attempt to give the international community the illusion of legality, since companies are already cooperating with the authorities in matters concerning national security.

CENSORED REVOLUTIONS

The Tunisian and Egyptian revolutions and their potential domino effect are greatly troubling to Chinese leaders, who took prompt measures to restrict online discussions on such topics, in order to prevent the population from being influenced by them.

On 28 January 2011, three days after the Egyptian uprising began, China began censoring netizens' searches by blocking results linked to the keyword "Egypt" on the micro-blogging Twitter website and its Chinese equivalents, sina.com and sohu.com. In response to this keyword, users receive the following message: "Under existing laws, the result of your search cannot be communicated." On Twitter as well as on Facebook, both of which are blocked in China, the hashtag #jan25 referring to the Egyptian demonstrations of 25 January of 2011 quickly spread around the Web. The Chinese Communist Party seems to be more fearful than ever of political reforms, democratic demands and "breaches of public order." On 30 January 2011, news wires about Egypt issued by Xinhua, the official Chinese press agency, were reportedly also suppressed.

Censorship does not stop there. On 20 February, the authorities deployed security forces to Beijing and Shanghai following an online call for a "Jasmin Revolution" and arrested people suspected of organizing it. Since then, the term "Jasmin" has joined the Chinese Internet's long and ever-growing list of censored words, such as "Tunisia," "Egypt," and "democracy."

CENSORS ATTACK THE NOBEL PEACE PRIZE

The authorities' indignation over the awarding of the Nobel Peace Prize to intellectual dissident Liu Xiaobo has translated into harsher online censorship and acts of intimidation against supporters of this human rights activist.

The government reacted by doing everything it could to censure the topic on the Web in order to prevent Chinese citizens from becoming aware of the historical import of this event. Chinese media coverage of the awarding of the Nobel Peace Prize to the jailed dissident has been dominated by the Beijing authorities' hostile reaction. The national TV network and most of the newspapers – even the most liberal – did not even mention it, and for good reason: on 8 October 2010, when the laureate's name was announced, the newsrooms received a clear order from the Department of Propaganda that it was "forbidden to relay information" about the topic (不能跨范围转载). A few Chinese foreign-language media, including the English-language version of the nationalist newspaper Global Times, and the French and English editions of the People's Daily reported the government's reaction. The Youth Daily ran an article headlined "Chinese dissident Liu Xiaobo nominated: an insult to the Nobel Peace Prize." Foreign TV programmes are still being jammed whenever they broadcast any news about Liu Xiaobo.

Internet censorship has not abated. On some of the major news sites, Sina and Sohu in particular, no content can be accessed which directly mentions Liu Xiaobo. On the Baidu search engine, some results do refer to the awarding of the Nobel Peace Prize, but the corresponding media pages are usually blocked. The official network CCTV remained silent about Liu Xiaobo and opened its evening news programme of 8 October with a report about torrential rains falling on Hainan Island.

Some bloggers, such as the writer Han Han, have protested by posting empty messages to symbolise the impossibility of discussing what happened to Liu Xiaobo (http://www.rue89.com/node/170478). The chat forum 1984bbs,

used by many journalists, was closed by its administrators after the latter were pressured by police. Twenty-three retired Communist Party officials and intellectuals have been urging the country's highest authorities to carry out political reforms and to comply with Article 35 of the China's Constitution, which guarantees free speech and media freedom. This appeal was systematically removed from Chinese blogs and websites where it had been posted. Although within one hour of the announcement of the Nobel Prize award related online messages remained accessible for less than five minutes before being deleted.

It has also been impossible to send an SMS containing the characters found in "Liu Xiaobo" or "Nobel Prize." The micro-blogging website Weibo has also been censored. Yet on Twitter, which is blocked in China, thousands of enthusiastic messages from netizens have been posted since the announcement. Renowned artist Ai Weiwei stated that it was China's happiest day in the last sixty years.

Moreover, a short time before the Nobel Peace Prize was awarded, a bogus invitation to attend the 10 December 2010 ceremony in Oslo containing a very powerful "Trojan horse" computer virus circulated by e-mail. The computer security firm F-Secure stated that it was unable to identify the origin of these cyberattacks. Two weeks before the virus appeared, the Nobel Peace Prize recipient's website had been the target of an initial hacker attack.

THE HEIGHT OF CENSORSHIP: CENSORING THE DEBATE ON INTERNET CENSORSHIP

While censoring an article on censorship may seem to be business as usual in China, the Diyi Caijing Zhoukan case (第一财经周刊- cbnweek.com) proves yet again the extremes to which the Chinese propaganda apparatus will go to ensure that any discussion of Internet censorship in China is nipped in the bud.

On 24 November 2010, the authorities banned the reprinting or posting of an article by Shanghai business weekly Diyi Caijing Zhoukan, which was a behind-the-scenes look at Beijing's Bureau of Website Administrators (北京市的网管办), one of the entities responsible for online censorship. The report was quickly withdrawn from the website cbnweek.com. The article provides a detailed description of how the Beijing Bureau of Website Administrators, a government agency, controls online information and shuts down websites in order to stifle any debate about social and political issues.

In the last few months, the authorities launched a new offensive against the proxy servers used by Chinese Internet users to bypass the "Great Firewall." Access to Freegate and Ultrareach, two of the most popular proxies, was made very difficult for several days as from 27 August 2010. To counter this new wave of blockings, their developers reacted by making updated versions of their software available to netizens.

THE REGIME'S INTERNET CHARM OFFENSIVE

INTERNET WHITE PAPER

On 8 June 2010, the Chinese Council of State's Information Bureau published a "white paper" on the Internet, which reasserts the need for online censorship in China in the name of "respect for local laws" and "maintaining stability." Far from challenging the authorities' policy towards the Internet, or the upsurge in online censorship, it merely adds to the Beijing leadership's usual rhetoric. While the government's resolve to broaden the Chinese people's access to the Internet is commendable, it regretfully does not encompass access to the World Wide Web, but solely to the Chinese Web, complete with its sophisticated filtering system that blocks political, social or other news which the authorities deem undesirable.

IS A "NATIONAL" SEARCH ENGINE BEING DEVELOPED ?

In August 2010, the official Chinese press agency, Xinhua, and state-owned China Mobile – the largest Chinese telecommunications operator –signed an agreement to create a joint venture called the Search Engine New Media International Communications Co. Its purpose is to launch a search engine directly controlled by the state which would enable Chinese authorities to expand their control of the Internet by taking advantage of the mobile phone market boom.
In addition, the regime is encouraging state-owned companies such as CCTV or Xinhua to strengthen their online presence.

In the meantime, the "50-cent party," named after the Net surfers paid to post pro-government online comments in order to "influence public opinion," is still in operation.

A WINDOW OF OPPORTUNITY FOR ONLINE DIALOGUE BETWEEN INTERNET USERS AND THE AUTHORITIES?

Some local and regional officials are already using the Web to convey their messages and address criticisms. In September 2010, the website Zhitong Zhongnanhai, named after the government's headquarters in central Beijing, was launched as a way for Internet users to send their messages to the national leadership. One week after its launch, over 20,000 comments had already been posted for President Hu Jintao alone on subjects such as real estate price increases, corruption, pollution and violations of civil liberties.

However, this free-speech window has been subject to 26 rules ever since. Netizens may not, for example, post comments which could jeopardise the state's honour and interests, or disrupt social order by advocating for the right of association, demonstration, or assembly.

Any Internet user who sends a disagreeable comment faces penalties which can be as harsh as the permanent termination of his or her IP address. Aware that it is prohibited on this government website to send a message from an IP address located outside of China, Chinese netizens therefore cannot do so anonymously by using proxy servers which assign them a foreign IP address. Even in cybercafés, every user is systematically asked to present an ID.

Despite this risk, some critical comments do manage to slip through the Net's filter. "When will prices go down? The only thing that isn't going up is salaries!" "Comrade Hu, don't you think it interesting that I have left so many messages, yet they all have been harmonised? Can't you let us tell the truth?" one netizen asked. The government's website address is: http://cpc.people.com.cn/GB/191862/191865/index.html

CRUSADING AGAINST ONLINE AND CELL PHONE ANONYMITY

In February 2010, the Chinese Ministry of Technology had already announced that anyone wishing to create an Internet website should register with Internet regulators in person and present an ID.

In May 2011, Wang Chen, the Department of Propaganda's Assistant Director, quoted in an article published on 5 May by China Daily: "We are exploring an identity authentification system for users of online forums." Internet users are currently required to register before posting comments on these sites, but they can do so using a pseudonym. According to Wang, now that anonymous posting on key news and commercial websites is banned, the next step is to extend the system to online forums and chat rooms.

Cellular telephony is not exempt from this effort. Chinese authorities are tightening their grip on prepaid cell phone communications. A new regulation which entered into effect on 1 September 2010 now requires users of prepaid cell phones to provide detailed personal information by presenting their identity card when buying SIM cards. Anyone who already owns one has three years to register.

The newspaper Global Times claims that 800 million telephone numbers are already assigned to cell phones now used in China, of which 320 million were acquired anonymously. Card sellers, mostly in newsstands, will be responsible for collecting photocopies of the buyers' IDs and for recording their contact information in the centralised cell phone user name data collection system. The Ministry of Industry and Information Technologies (MIIT) justifies this initiative by claiming that it is part of the government's campaign against spams and fraud. In actuality, this new rule may potentially compromise the cell phone users' personal data protection, since it enhances the authorities' ability to monitor calls, SMSs, and data exchanges, thereby facilitating the identification of individuals who criticise or demonstrate against the government.

THE AUTHORITIES TAKE AIM AT MICRO-BLOGGING

In the summer of 2010, the authorities launched a new crackdown on online networking tools, especially micro-blog services. On 15 July 2010, several dozen micro-blog accounts were closed, among them those of blogger Yao Yuan and lawyer Pu Zhiqiang. Four of the leading Chinese micro-blogging platforms, Netease, Sina, Tencent and Sohu, were inaccessible for several hours or days, displaying notices that the site was down for maintenance.

Around the same time, censors implemented an additional control level. In August 2010, Chinese authorities ordered micro-blogging websites to hire a "self-discipline commissioner" to be responsible for censorship. According to the official press, the results of the first micro-blogger self-censorship test conducted in January 2010 in Hebei

province were deemed satisfactory enough to convince the authorities to extend its application in Beijing to eight micro-blogging platforms: Sina, Sohu, NetEase, Iphonixe, Hexun, Soufang, 139Mobile and Juyou9911. The latter hired such commissioners and asked them to monitor and censor anything which could threaten the country's security or the society's stability. They are focusing on content dealing with illegal activities, pornography and violence, as well as unsubstantiated rumours and politically sensitive issues. Each commissioner has been assigned a website whose content he or she is responsible for.

IMPACT OF THE GOOGLE CASE

STOPPING CENSORSHIP

The U.S. firm Google announced on 22 March 2010 its decision to put an end to censorship via the Chinese version of its search engine, google.cn. Now, when users click on the home page of google.cn, they are redirected to Google.com.hk, where they have access to uncensored content in simplified Chinese characters. This website was intermittently censored in late March 2010. Despite tenser relations with the Chinese authorities following this decision, the company did manage to get its operating license there renewed in July 2010. It will maintain its research and development activities in China, and keep on selling advertising spots on Google.com to Chinese companies.
Google may have set an example for others: the U.S. Internet company GoDaddy announced on 24 March 2010, during a U.S. congressional hearing, that it would stop offering its clients new Chinese domain names ending in the .cn suffix because of the radical controls measures being implemented by Chinese authorities.

ARE CHINESE AUTHORITIES DIRECTLY IMPLICATED IN HACKING ACTIVITIES?

Google's decision apparently was reached in the wake of cyberattacks launched from China against the Gmail accounts of several dozen human rights activists. Some twenty media and technology sector companies are said to have also been victims of these hacker attacks and of intellectual property infringement.

Cyberattacks were still going on in early 2010. The Foreign Correspondents' Club of China (FCCC) reported that the Yahoo! e-mail boxes of at least ten foreign journalists based in China and Taiwan were hacked. Independent news sites such as Boxun have been under constant attack.

In secret documents released by WikiLeaks, a "Chinese source" cited by U.S. diplomatic sources confirmed the Chinese government's involvement in the computer hacking of Google. These revelations have raised considerable concern about spying methods used on journalists and human rights activists working on China. The diplomatic cable cited by the New York Times specified: "The Google hacking was part of a coordinated campaign of computer sabotage carried out by government operatives, private security experts and internet outlaws recruited by the Chinese government."

WEB CENSORSHIP: A TRADE BARRIER?

Internet censorship is not just a human rights issue. It also negatively impacts trade and business through the lack of access to reliable information. Online censorship has also become a way to discriminate against foreign – particularly American – companies, and to afford Chinese companies preferential treatment, which led two experts of the European Centre for International Political Economy to label it, in The Wall Street Journal, "disguised protectionism."

The European Union entered the debate in 2010, as the censorship spread to mobile telephones – a sector in which European companies do considerable business. In May 2010, European Commission Vice President and Digital Agenda Commissioner Neelie Kroes called this censorship a "trade barrier" and said it is an issue that should be tackled within the World Trade Organization.

TIBET AND XINJIANG: SENSITIVE PROVINCES, SPECIAL TREATMENT

AT LEAST 50 TIBETANS SENTENCED FOR HAVING SENT NEWS ABROAD

The repression has never stopped since the March 2008 uprising in the Tibetan regions. Since then, at least 50 Tibetans have been arrested and some sentenced to lengthy prison terms for having sent information, photos

and videos abroad. The latest to be convicted, Dasher, was given a 10-year prison sentence on a charge of "separatism" in February 2010.

XINJIANG: RECONNECTED TO THE NET, BUT STILL PLAGUED BY PURGES

The arrests continue. Cut off from the world for nearly 10 months following the social unrest in July 2009, the Xinjiang Autonomous Region was then subjected to a discriminatory shut-down of Internet access, and was only reconnected to the Chinese Internet on 14 May 2010.

Meanwhile, Xinjiang's Internet users are subject to filtering by the Chinese Firewall, and the websites and blogs dealing with the Uyghur issue are still a favourite target for censors. Many of them are still blocked – including the sites of the Uyghur American Association (UAA) and the Uyghur Human Rights Project (UHRP) – because they refuse to toe the official Beijing Party line. Banned keywords include "Rebiya Kadeer" (the Uyghur human rights activist), "World Uyghur Congress", "Uyghur Human Rights Project" and "East Turkestan Independence."

Salkin website collaborator Gulmire Imin was sentenced to life behind bars in April 2010 for having "revealed" state secrets, for "organising a demonstration" and for "separatism."

On 21 July 2010, in Urumqi, three Uyghur webmasters, Dilshat Perhat, Nureli and Nijat Azat were tried in camera for having endangered state security and for the content of their publications, which the Chinese government deemed to be politically sensitive. They were sentenced, respectively, to five, three and ten years in prison.

LIU XIAOBO (刘晓波): THE WORLD'S ONLY NOBEL PEACE PRIZE RECIPIENT STILL BEHIND BARS

On October 8, the Nobel Peace Prize was awarded for the first time to a Chinese citizen residing in China, even though he has been serving an 11-year jail sentence in Jinzhou Prison (Liaoning Province). Very moved when he learned the news, intellectual and human rights activist Liu Xiaobo dedicated this prize to "the lost souls of 4 June" – the date of the Tiananmen Square massacre. Liu Xiaobo is one of the co-writers of Charter 08, which calls for more freedoms and an end to the one-party rule in China. His biography is available at: http://en.rsf.org/chine-liu-xiaobo-biography-28-10-2010,38704.html, and Charter 08 can be found at: http://www.nybooks.com/articles/archives/2009/jan/15/chinas-charter-08/

The pressures being placed on Liu Xiaobo's relatives and supporters, as well as on all defenders of freedom of expression, have not lessened in China since this announcement was made. Beijing tried to dissuade diplomats from attending the Nobel Prize award ceremony in Oslo on 10 December 2010 and prevented several human rights activists from leaving the country. Liu's wife, Liu Xia ( ), is under house arrest and her relatives are not permitted to leave China. The Nobel Committee awarded the prize to an "empty chair."

Am ever-growing number of Liu's supporters are being arrested. Since mid-October 2010, according to the independent Chinese PEN Centre, at least 40 human rights activists and journalists have been arrested or brought in for questioning throughout China for attempting to celebrate the news of Liu's award. Three of them were detained for at least eight days: Wang Lihong, Wu Gan and Zhao Changqing. Formerly imprisoned journalist Liu Jingsheng said that two police officers had been posted outside his home. Liu Xiaobo supporters without Beijing residence permits have been sent back to their home province.

Guo Xianliang, an Internet writer known by his pen name, "hermit of Tianshan Mountain" has been behind bars since 28 October after being arrested by the Guangzhou authorities for passing out flyers with pictures of Liu Xiaobo in the streets and parks of Canton. Human rights activist Liu Di, known by her pen name, "Stainless Steel Mouse", along with about 100 other people, were placed under house arrest and strict police surveillance.

A FEW RELEASES OFFSET BY NEW CONVICTIONS

The sentences of some "4 June dissidents" who had participated in the June 1989 Tiananmen Square demonstrations were shortened (http://www.duihuanews.org/). Cyberdissident Li Zhi, a former government official sentenced in December 2003 to an eight-year prison term for "subversive" use of the Internet, was released last Novem-

ber, nine months early. He is one of the netizens condemned on the basis of information originating from their e-mail accounts, which Yahoo! had provided to Chinese authorities.

Dissident Qin Yongmin was freed after serving his full 12-year prison sentence, but is still kept under close watch. Writer Guo Xianliang, who had been arrested in Canton for having passed out flyers supportive of Liu Xiaobo, was released on 26 November. His friends and family report that he was able to safely return to Kunming.

However, on 9 June 2010, the Sichuan Provincial High People's Court upheld the decision made against activist and environmentalist Tan Zuoren, who had been sentenced to a five-year prison term for "inciting subversion of state power" and to a three-year deprivation of his political rights. He had been arrested in March 2008, after urging Chinese netizens to travel to Sichuan Province to look into the situation of the earthquake victims' families.

For the first time, an ironic tweet earned a netizen one year of forced labour. On 15 November 2010, cybernaut Cheng Jianping was sentenced to serve a year in the Shibali River "re-education through work" labour camp for women in Zhengzhou, Henan Province, for "disturbing social order." Her lawyer, Lan Zhixue, appealed this administrative order, issued without any form of trial. Cheng Jianping was arrested on 28 October – on what would have been her wedding day – and charged with having retweeted, on 17 October 2010, a satirical message about anti-Japanese demonstrations taking place in China, using her pen name "Wang Yi" (@wangyi09) on the Twitter website. She has more than 5,000 netizen followers on this social network. The message suggested that young Chinese protesters should attack the Japanese pavilion at the Shanghai World Expo and mocked the excessive tension between the two countries.

ENDANGERED NETIZENS: CRIMINAL DETENTIONS AND MOCK RELEASES

CYBERDISSIDENTS DETAINED DESPITE BEING GRAVELY ILL

The incarceration of certain netizens can sometimes have a tragic outcome. Shortly after having finally been granted the medically motivated release he had repeatedly requested, cyberdissident Zhang Jianhong – better known by his pen name Li Hong – died on 31 December 2010 in a hospital in Ningbo of complications from a disease for which he had never been treated during his three years behind bars. Li Hong was the chief editor of Aiqinhai, a literary online magazine (http://www.aiqinhai.org/) closed by the authorities in 2006 for disseminating "content critical of the Chinese government." He also contributed to news websites Boxun and Epoch Times.

The lives of several other netizens are hanging in the balance. The Chinese authorities should have learned their lesson from this tragedy and immediately released all other netizens with health problems, particularly Huang Qi, Fan Yanqiong, Cheng Jianping, Hu Jia and Yang Tianshui.

Huang Qi, arrested in 2008, was sentenced to three years behind bars for having posted articles online about the consequences of the Sichuan Province earthquake. He is said to have stomach and chest tumours which are not being treated properly, and to have been tortured and deprived of sleep.

Cheng Jianping was sentenced on 15 November 2010 to a year of "re-education through work" in a labour camp for having relayed a comment on Twitter about tensions between China and Japan. She is suffering from tuberculous pleurisy, a chronic lung condition.

Netizen Fan Yanqiong, arrested in 2009, was given a two-year prison sentence in April 2010 for having reported online the case of a raped and murdered woman in Fujian Province. At the time of her trial, she had to use a wheelchair and an oxygen mask because she was suffering from high blood pressure, muscular atrophy and severe pains in all her limbs.

Blogger and human rights activist Hu Jia got a three-year prison sentence in 2008 for "inciting subversion of state power" after posting articles online and granting interviews to the foreign media. He has cirrhosis of the liver, but is not receiving the medications he needs.

FORCED DISAPPEARANCES?

Geng He, the wife of Chinese human rights activist and lawyer Gao Zhisheng, has never stopped demanding an explanation for the disappearance of her husband, one of the first "barefoot lawyers" who has been missing again since April 2010 .

Human rights activist and cyberdissident Govruud Huuchinhuu, a member of the Southern Mongolia Democratic Alliance (SMDA), has been reported missing since 27 January 2011, when she was released from the hospital in Tongliao, a city in the Inner Mongolia Autonomous Region of northern China, where she had received cancer treatments. Huuchinhuu had been under house arrest since November 2010 for using a website to call for a rally of Mongol dissidents to celebrate the anticipated release of Hada, a human rights activist and the SMDA's Chairman.

FALSE RELEASES?

Hada, a journalist and activist for the Mongal cause, is still being held by the Chinese authorities, even though he should have been freed on 10 December 2010 after serving his full sentence. When he was finally permitted to meet with his uncle, Haschuluu, in late January 2011, he looked undernourished and had had no news of his wife Xinna and his son Uiles. On 14 December, a Chinese official referred to only as "Jin," told people close to Hada that his wife and son were safe and enjoying the family's reunion in a "five-star luxury hotel." A testimony which Hada dictated to his wife from prison can be found at: www.smhric.org/Latest_A.htm.

Similarly, activist and netizen Zhao Lianhai allegedly has been released but still cannot be contacted. He was arrested in November 2009 and sentenced one year later to two and one-half years in prison for having set up an Internet news and mobilisation website ("Kidney Stone Babies") devoted to the scandal involving the milk powder contaminated by the Sanlu company in China. He had first announced that he wanted to protest the court's decision and had started a hunger strike, but he later said that he no longer wished to see his lawyers or to appeal.

ONLINE MOBILISATION STRONGER THAN EVER

WORD GAMES AND CARICATURES: NEW ANTI-CENSORSHIP WEAPONS

The Chinese are ardent word game players. The Chinese language is full of homophones and lends itself very easily to this exercise.

For several years, Web surfers have been making censors the butt of humorous and creative puns and word games. The fight against censorship is represented by a mythical creature called the Caonima a grass-mud horse), a homonym for a stinging personal insult. Internet users ridicule Chinese Communist Party (CCP) censorship by inventing false reports and songs about animal characters on the Caonima: http://www.youtube.com/watch?v=wKx1aenJK08&feature=player_embedded

More recently, the lizard Yake (yakexi in Chinese) appeared following a TV show on the Chinese New Year ceremonies in which Uyghur singers were supposed to praise the government, but they kept on repeating that the CCP Central Committee's policy was "good" (yakexi in Uyghur). Shocked by this propaganda in light of the utter instability in Xinjiang, some netizens invented a lizard character (xi in Mandarin) called Yake, who patrols the Internet. According to its authors, the lizard representing the Central Committee's policies had a glorious past in the Soviet Union, where its race is now dying out but is still thriving in countries like Cuba, North Korea and China. The lizard Yakexi, with his forked tongue, feeds on "river crabs" (hexie) a homonym of "to harmonise," President Hu Jintao's political leitmotif, and a government euphemism for censorship). Ironically it has been put to a new use by netizens.

The Chinese Internet's latest "harmonised" animals are featured in an animated video produced by Wang Bo, which shows an innocent rabbit population oppressed by a government of aggressive tigers. The year 2010 was the "Year of the Tiger," while 2011 is that of the Rabbit, according to the Chinese calendar. In this film, baby rabbits are dying and in atrocious pain after drinking some Sanlu milk, a reference to the 2008 melamine scandal which had caused the death of several infants and poisoned several hundred thousand others. The Li Gang case is also featured.

In all, Chinese bloggers and netizens have created a dozen creatures representing Internet censors.

A NECESSARY BATTLE WHICH IS NOT WITHOUT RISK

While there have been many examples of successful online mobilisations, tragic cases of tortured bloggers and journalists are still far too frequent.

"You will be punished in kind," as member of the Guobao (public security squad) told Liu Shasha, a young Beijing

blogger who was in jail in July 2010. While being interviewed by a French journalist, she described the conditions of her detention and the barbaric tortures that she had to endure. What was this young woman's crime? She had urged people on the Twitter network to place funeral wreaths in front of the building which houses the Chinese research engine firm Sohu, after it reportedly eliminated hundreds of free speech activist blogs.

DENOUNCING CORRUPTION: NETIZENS' TROJAN HORSE

The Li Gang case has caused a massive outcry in the Chinese blogosphere, where the impunity enjoyed by Chinese officials is extremely unpopular. In October 2010, one young man, Li Qiming, caused a mortal road accident on the Baoding campus of Hebei University (in Hebei Province, near Beijing) while driving intoxicated. Right after hitting two young women head on, one of whom later died, the young man allegedly said, while leaving the scene, "Go ahead and try to sue me, my father is Li Gang."

The story spread like wildfire on the Internet, as did the statement, "my father is Li Gang," which has become a catchphrase for shirking responsibility while breaking the law. By using a "human flesh research engine," some cybernauts managed to identify Li Gang as the deputy police chief of Baoding's Beishi district. His son, Li Qiming, was arrested on 24 October 2010. The case was referred to the country's highest courts, which were troubled by the intense public indignation aroused by this case. A video of Li Gang was broadcast on the national TV station in which he tearfully asked to be forgiven for his son's behaviour.

"HE WHO HAS NOT CLIMBED THE GREAT WALL IS NOT A TRUE MAN" – CHINESE PROVERB

The Great Wall of censorship continues to rise higher and higher around the Middle Kingdom's readers, listeners, TV viewers and cybernauts. Yet defenders of free expression are managing to circumvent it, or scale it. As these "true men" join forces in pursuing this effort, they will win. It is up to governments, corporations and Internet users in democratic countries to give them their unwavering support, for the Chinese government seems disinclined to change its positions on the issue. In his 19 February 2011 speech to leaders of Chinese provinces, Hu Jintao spoke of intensifying the regime's management and control of the Internet in his country. He notably specified the need to "increase the government's level of control over the virtual society and to perfect mechanisms for channelling online public opinion."

CUBA

INTERNET ENEMY

Domain name: .cu
Population: 11,451,652
Internet users: about 1,604,000
Average cost of a one-hour cybercafé connection: about 1.5 U.S. dollars for the national network – 5 to 7 U.S. dollars for the international network.
Average monthly salary: 20 U.S. dollars
Number of imprisoned netizens: 0

The Cuban regime, more wary of bloggers than traditional dissidents, decided to expand its online presence to combat them. Now that Venezuelan fibre optic cable is available on the island, the authorities have what they need to improve connection speeds and lower costs. There are fewer and fewer excuses for maintaining censorship or keeping the population away from the Web. Are we witnessing signs of a Web Springtime, now that the journalists persecuted during the Black Springtime of March 2003 have all been released from prison?

FIBRE OPTIC CABLE IN CUBA: UNPRECEDENTED POTENTIAL FOR GROWTH?

According to the authorities, nearly 10% of Cuba's population is connected to the Internet. That does not necessarily mean that they have access to the World Wide Web. Two parallel networks co-exist on the island: the international network and a closely monitored Cuban intranet consisting only of an encyclopaedia, e-mail addresses ending in ".cu" used by universities and government officials – a sort of "Cuban Wikipedia" – and a few government news websites such as Granma.

Outside of hotels, only a few privileged individuals have a special permit to access the international network. Yet even the latter does not escape censorship, which is mainly directed against dissident publications on foreign websites, but has been relaxed to some extent since early February 2011.

The regime does not have the means to set up a systematic filtering system, but it counts on several factors to restrict Internet access: the exorbitant cost of connections – about 1.50 U.S. dollars per hour from the points of access to the state-controlled intranet, 7 U.S. dollars per hour from a hotel to access the international network (even though the average monthly salary is 20 U.S. dollars), and lastly infrastructural problems, particularly slow connections. These obstacles explain why the number of Internet users and the time spent online remain limited. Most cybernauts try to just read their e-mails and answer them. They do not have the time to navigate the Internet or surf websites.

For years, the regime has been blaming the American embargo for the lack of a good Web connection on the island, claiming that it prevents the country from acces-

sing international networks. That problem is about to be solved, thanks to the ALBA-1 fibre optic undersea cable which has been linking Cuba to Venezuela since February 2011, thereby increasing 3000-fold Cuba's capacity to connect to the rest of the world. It is scheduled to be put into service in July 2011.

Until then, international network connections will continue to be made via satellite, at immoderate costs. Theoretically, fibre optic cable should lead to lower Internet access prices and improve connection speeds.

It is unlikely, however, that Internet access will be democratised and made available to the general population.

The authorities are cautious when commenting on this new development. In February 2011, Cuba's Vice-Minister of Information and Communications, José Luis Perdomo, pointed out that cable "is not a 'magic wand,'" and that granting Cubans access to the Internet will require a substantial investment in its infrastructures. He also said that there is "no political obstacle" to offering such access. For the time being, this access to the Web will remain reserved for "social use" by institutions, universities and certain categories such as doctors and journalists. He stated: "Our priority is to continue the creation of collective access centres in addition to strengthening the connections in scientific, university and medical research centres."

RESOURCEFULNESS

A genuine black market has been prospering in Cuba in which offers are made to buy or "rent" passwords and codes used by the few individuals and companies whom the incumbent party has cleared for Internet access. Navigating the Net costs 50 U.S. dollars per month and receiving/sending one e-mail message costs 1 U.S. dollar in some "hacker centres." Illegal users find it safer to connect only at night.

Some international network connections can be accessed from foreign or private residences.

Certain dissidents tweet by sending SMS via foreign-based accounts, while others insert foreign SIM cards into their cell phones to access the Net. While netizens will stop at nothing to pass on information, it can come at a high cost.

Freelance bloggers do not have direct access to their websites, which are not hosted on the island. They are have to rely on friends abroad to publish their articles and posts. They do that by following a well-tested procedure: they prepare their content in advance, copy it onto a USB flash drive, and send it by e-mail from a hotel or other location, because dissidents are more and more frequently denied entry into tourist hotels. USB flash drives, which are also being passed from hand-to-hand, are the new vectors for freedom of speech in Cuba – the local "samzidats."

DEMONISING BLOGGERS AND SOCIAL NETWORKS: A DIGITAL COLD WAR?

In 2009, the regime became wary of the growing popularity of certain bloggers, notably Yoani Sanchez. The latter has been repeatedly assaulted, interrogated and targeted by genuine slander campaigns, while other bloggers, such as Luis Felipe Rojas, have been arrested several times.

Cuban dissident and cyberjournalist Guillermo Fariñas Hernández ("El Coco"), winner of the 2010 Sakharov Prize for Freedom of Thought awarded by the European Parliament, was arrested three times in less than 48 hours in January 2011. His only wrongdoing is that he has been militating in favour of the right to inform and to circulate news freely.

The legal arsenal used against online opposition to the regime remains particularly harsh and dissuasive. Cuban netizens risk punishment of up to twenty years in prison for posting an article deemed "counter-revolutionary" on an Internet website hosted abroad, and five years for illegally connecting to the international network.

The problem is becoming increasingly urgent as the authorities fear the social networks' mobilisation power even more after witnessing Tunisian and Egyptian examples of it. Some U.S. diplomatic cables published by WikiLeaks in December 2010 revealed that the Cuban regime is more afraid of bloggers than of "traditional" dissidents.

In a 15 April 2009 telegramme, dissidents were described as forming "a movement as old and out of touch from the lives of ordinary Cubans as the regime itself." A cable dated 20 December 2009 stressed, to the contrary, that bloggers are "a much more serious threat" to the Cuban government.

The United States views the reporting by Cuban netizens of their arrests and mistreatment as an invaluable political tool, because the latter represent "a group which frustrates and scares the Cuban government like no other." "The bloggers' mushrooming international popularity and their ability to stay one tech-step ahead of the authorities are causing serious headaches for the regime." The U.S. diplomat concluded: "We believe that it is the younger generation of 'non-traditional dissidents' that is likely to have a greater long-term impact on post-Castro Cuba."

Another telegramme noted that "Younger individuals, including bloggers (…) are much better than traditional dissidents at taking 'rebellious' stands with greater popular appeal" – an assessment that Cuban leaders seem to share. Since February 2011, a one-hour or so video has been circulating on the Internet (vimeo.com/19402730) in which an unidentified Cuban expert explains in detail how the American enemy is funding Cuban cyberdissidence.

Using as an example blogger Yoani Sanchez (www.desdecuba.com/generaciony), he asserts that "she is organising a virtual network of mercenaries who are not traditional counter-revolutionaries." The expert urges that these new forces be neutralised, stressing that "being a blogger is not bad. They have their bloggers and we have ours. We're going to fight to see which of the two turns out to be stronger."

GOVERNMENT REPRISAL: OCCUPY THE FIELD

The authorities are now striving to expand their presence on the Web: an official Cuban bloggers association was formed in 2009. The number of "pro-government" bloggers is said to be constantly rising, and may be as high as several hundred. In February 2011, the Reuters press agency reported that Cuba had some 1,000 "official bloggers."

Any possible links between the Havana government and hackers who target Cuban websites and blogs hosted abroad, among others, are under heavy scrutiny.

Since the regime's strategy is to "drown" dissident bloggers in a flood of pro-government bloggers, the government no longer needs to keep such a tight rein on the former, and can afford to make some concessions.

Since 9 February, forty-some opposition blogs and Internet pages, among them Yoani Sanchez's Generación Y, are accessible again from the island for those who can connect to the international network. According to this blogger's statements to the foreign press, Cuba may owe this breath of fresh air to the 14th Informática - International Convention and Fair, held in Havana from 7 to 11 February. What remains to be seen is whether this deblocking will last.

The authorities' negative track record with regard to censorship accounts for dissidents' doubts that the Internet will ever be accessible throughout the island. According to Yoani Sanchez, "the cable optic fibres are already engraved with the name of their owner and its ideology. This undersea connection seems destined more to control us than to link us to the world."

However, with this cable, "it will be more difficult to convince us that we cannot have YouTube, Facebook or Gmail," she pointed out, specifying that "no one will prevent us from using this cable to do something very different from the plans of those who bought it."

For the middle or long-term, some people are banking on Chinese-type progress: Web growth for economic reasons, with more access for the population, while maintaining political control. A glimmer of hope remains: Cuba has announced that it wishes to switch from a Windows to a Linux operating system. This initiative may enhance the technical expertise of Cuban IT specialists, who will then be in a better position to circumvent censorship.

IRAN

INTERNET ENEMY

Domain name: .ir
Population: 76,923,300
Number of Internet users: 28, 200,000
Average cost of a one-hour cybercafé connection: USD 3 to 4
Average monthly salary: about 560 dollars
Number of imprisoned netizens: 11

Iran has intensified online crackdowns and surveillance again this year, particularly in periods of unrest and demonstrations, during which the authorities have resorted to causing Internet slowdowns and disconnections, or jamming telephone lines. The regime has also continued to demonise the new media, accusing them of serving foreign interests. Several netizens have been sentenced to death.

TOUGHENING AND BROADENING INTERNET CENSORSHIP

In January 2011, the authorities finished setting up the first Iranian cyberpolice to strengthen their control of the Internet. On 20 May 2010, Ebrahim Jabari, an Islamic Revolutionary Guard Corps (IRGC) commander, officially confirmed the creation of an Iranian "Cyber Army" which has already cracked down on online networks deemed "destructive," and arrested hundreds of netizens.

Internet service providers were already leasing bandwidth to the Telecommunications Company of Iran (TCI), controlled by the Revolutionary Guards, who are responsible for ordering the blocking of websites. Although the authorities boast that they have blocked hundreds of thousands of websites, it is certain that thousands of them and millions of associated pages are now inaccessible in Iran. Under Ahmadinejad's administration, the censorship of news sites covering politics and human rights has been considerably tightened.

Filtering software developed in Iran is used in these blocking efforts. Censorship criteria are formulated by the Committee in Charge of Determining Unauthorised Websites (CCDUW). In January 2010, the authorities had issued a "list of Internet offences" drawn up by a "committee of experts" which was already implementing a genuine Net filtering system. This "list" is an inventory of banned websites. Targeted are contents "contrary to the morals of society," "to religious values" and "to security and social peace," "hostile towards government officials and institutions" or which "facilitate the commission of a crime," including circumventing censorship or bypassing filtering systems. It is forbidden "to sell filter circumvention software" in the country. This list supplements the law enacted by the Iranian Parliament over a year ago which imposes sanctions of up to several years in prison. At least two netizens have been arrested for using censorship-circumventing software.

The "committee of experts" includes members from several government branches and the judicial wing, represen-

tatives of the Ministry of Communications and Information Technology, the Ministry of Culture and Islamic Guidance, the Ministry of National Security and Teheran's Public Prosecutor.

Iran's censors combine URL blocking with keyword filtering to ensure optimal censorship and act promptly in the event of breaking news. The Reuters press agency and Yahoo ! websites have allegedly been censored since the Tunisia and Egypt uprisings. Google is also said to be partially blocked and some links to foreign news sites supposedly have been replaced by official sources.

A system for censoring conservative sites has been set up which reveals internal divisions in the leadership. In October 2010, several news portals were blocked, including those of the three influential Grand Ayatollahs – Ayatollahs Saanei (http://saanei.org/), Bayat Zanjani (http://bayatzanjani.net/) and Dastgheib (http://www.dastgheib.ir/) – inaccessible since 3 October 2010.

In February 2010, the Gmail messaging service was suspended. According to the authorities, a national messaging service will soon be launched. Several websites such as Radio Zamaneh and Twitter have been the target of cyberattacks. Blog platforms like www.blogfa.com are not totally blocked, but those run by individuals are. Participative photo- or video-exchange websites are among those targeted by censors: Flickr.com, Photobucket.com and YouTube.com are blocked.

THE REGIME'S PROPAGANDA AND TAMPERING AGAINST INTERNET AND SOCIAL NETWORKS

Iran's government seems to be launching a real war against social networks which has been intensifying since the latter's presumed role in the disputed re-election of Mahmoud Ahmadinejad. The authorities are shamelessly advancing the theory that it was a plot.

In September 2010, a state-owned Iranian TV station declared that Facebook and Twitter were the country's hidden enemies used by Western secret services to recruit new members and collect information. Facebook and Twitter are accused of being implicated in a "psychological and propaganda war." At the end of 2008, the Revolutionary Guards announced their plan to create 10,000 blogs to support Iran's paramilitary militia, the basij, and to promote the regime's ideology. Several websites and blogs were created to disseminate propaganda and infiltrate social networks, which they used mainly to spread messages to incite hatred.

Through the agency of its Cyber Army, the government itself repeatedly initiated politically motivated cyberattacks on various opposition or news sites such as Jaras, Kalameh, Balatarin.com, etc. In the morning of 14 February 2010, a day of demonstrations, Fararu.com and the site sahamnews.org, which have close ties to opposition leader Mehdi Karoubi, were hacked, as was the supposedly secure Voice of America (VOA) website. Hackers claiming to be members of the Cyber Army managed to post messages on the page in Farsi, calling for an end "to U.S. meddling in the Muslim world" and labelling the media as a "spying tool for the United States."

The regime is also spying on cyberdissidents and attempting to infiltrate social networks, blocking various profiles on Facebook. On 18 December 2009, the Iranian Cyber Army succeeded in hacking Twitter. The website displayed the following message: "This site has been hacked by the Iranian Cyber Army": iranian.cyber.army@gmail.com". In January 2010, the Chinese search engine Baidu was also the target of cyberattacks, probably to counter the Chinese netizens' support of the Iranian people. Lastly, the regime launched a call for online collaboration and denunciation with the website Gerdab ("vortex"), spearheaded by the Organised Crime Surveillance Centre.

Ever since its creation in March 2009, the Organised Crime Surveillance Centre, established by the Revolutionary Guards, has played an active role in tracking down and arresting netizens. In March 2009, the Centre officially announced the dismantling of a "malevolent" online network and the arrests of several moderators of incriminated websites. A few days later, "confessions" of those arrested, together with their photos, were posted online, notably by the Gerdab website. The accused were allegedly forced to admit to the existence of websites which were critical of Islam and Iran's incumbent government, and to their intention of "corrupting" Iranian youth by publicising pornographic sites. They also had to confess to participating in a plot supported by the Americans and the Israelis.

Some of the regime's opponents have created their own "Green Cyber Army," which sometimes adopts the regi-

me's methods. For example, some activists have attacked the Basij militia's website, moghavemat.ir, as well as sites created by individuals or Iranian agencies close to the government, such as Farsnews. In 2010, this Green Cyber Army also posted photos of people suspected of being government agents.

SLOWING DOWN THE NETWORK AND CENSURING SMS

Under normal circumstances, bandwidth speed is slow. By order of the Ministry of Communications and Internet Technology, households and cybercafés are prohibited from having high-speed access, which is limited to speeds of 520 kb/s. Individual connection speed is slow in Iran and limited to 128 kb/s. This technical obstacle limits Internet users' ability to upload and download photos and videos. According to the International Telecommunication Union (ITU), Iran's Internet penetration rate is the sixth highest in the region. However, its slow connections place the country 15th in a regional ranking of countries with Internet access. Worse still, according to Speedtest.net, Iran placed 176th (in terms of connection speed) in a 185-country survey.

In periods of social unrest, speed is intentionally made even slower. Following Mahmoud Ahmadinejad's disputed re-election, the regime intentionally jammed all means of communication. Two days prior to the presidential polls, the authorities had already cut the SMS network and slowed down Internet speed. In June and July 2010, they systematically shut down mobile telephone networks in the centre of Iran's major cities during the demonstrations, and decreased Internet network even more.

As of 10 February, after several calls had been posted on the Internet for a demonstration to coincide with the Islamic Revolution's anniversary on 14 February, bandwidth speed was slowed down sharply in several of the country's major cities. As they have done with the approach of every opposition event or potential demonstration, the authorities intensified censorship of all media likely to relay the call for demonstrations on Monday 14 February 2011. Independent news websites, or those deemed to have close ties to the opposition, such as Jaras, Kalameh, or Balatarin – one of the opposition movement's online bastions – and Gooya.com, one of the most popular news portals, have been blocked. Two news websites, www.fararu.com and sahamnews.org (the latter having close ties to opposition leader Mehdi Karoubi), were made inaccessible for several hours after being attacked by hackers. Access to Gmail, Google Reader and Yahoo ! was made more difficult in several regions of the country. The term Bahman, which corresponds to the 11th month of the Iranian calendar, was added to the blacklist of filtered keywords. Bloggers were ordered to withdraw any photos of the demonstrations from their websites. Cell phones and SMS's were also jammed. The same scenario reoccurred during the demonstrations on 20 February.

ANTI-NETIZEN REPRESSION IS ESCALATING: RECORD PENALTIES, THE WORLD'S YOUNGEST IMPRISONED BLOGGER AND DEATH SENTENCES

Authorities rely on Iran's Press Law, Penal Code and the Cyber Crime Act of 2009 to prosecute Internet users. Article 18 of the latter provides for prison terms of up to two years and a fine for anyone found guilty of "disseminating false information likely to agitate public opinion." By virtue of Articles 500 and 514 of the Penal Code, "anyone who somehow insults the founder of the Islamic Republic of Iran, Khomeini, or the Supreme Leader of the country should be sentenced to imprisonment from six months to two years" (Art. 514) and "anyone who undertakes any form of propaganda against the state will be sentenced to between three months and one year in prison" (Art. 500).

Again this year, netizens – and especially the regime's opponents and advocates for women's rights – have been the target of countless arrests, summons and threats on the part of the authorities. The government has created numerous VPNs (virtual private networks) in order to gather information on dissidents. Seven netizens are still behind bars in the country.

On 16 February 2011, in response to recent demonstrations, Mohammad Hussein Khoshvaght, webmaster of www.fararu.com, and Gholam Ali Dehgan, webmaster of www.aftabnews.ir, were arrested by officials of the Ministry of Intelligence and National Security, and later released.

On 22 September 2010, Noushin Ahmadi Khorasani, Editor-in-Chief of the Feminist School website, (http://www.feministschool.com/), was summoned and interrogated by

the Fifth Chamber of the Tehran Revolutionary Court located inside Evin prison, before being released on bail. On 8 June 2010, blogger, journalist and women's rights activist Jila Bani Yaghoob was sentenced by the 26th Chamber of the Tehran Revolutionary Court to one year in prison and a 30-year ban on working as a journalist because of her opinions. Various "feminist" websites have been blocked, including www.we-change.org, www.roozmaregiha2.blogfa.com and www.pargas1.blogfa.com.

Hossein Derakhshan, an Irano-Canadian blogger, was given the harshest prison term ever meted out to a netizen in Iran: 19 and one-half years in prison, a five-year ban on engaging in political and media-related activities, and a fine of about 42,280 U.S. dollars. The netizen appealed his sentence, but is still waiting for a new trial. This excessive sentence was followed, in January 2010, by the conviction of blogger Navid Khanjani, a young student, who received a 12-year prison term. The Revolutionary Guards arrested netizen and human rights activist Hossien Ronaghi Maleki on 13 December 2010 during an "operation to dismantle a counter-revolutionary network." He was charged with developing and using anti-filtering software, and of assisting and hosting websites and blogs actively involved in defending human rights. This netizen, now gravely ill and deprived of medical care, was sentenced to 15 years behind bars.

The Iranian regime is now using the pornography pretext to definitively muzzle dissident voices and tighten its iron grip on information in the country. Second only to China in the number of people it has executed, Iran sentenced to death two Internet website administrators in December 2010, Saeed Malekpour and Vahid Asghari, for "agitating against the regime" and "insulting the sanctity of Islam." The verdicts were sent to the Supreme Court for confirmation. Close to 70 people have already been executed in Iran since early 2011.

It has intensified repression by sentencing to death – for the first time this year – individuals with dual nationalities, while the international community is forced to stand by, being unable to intervene.

Saeed Malekpour, a 35-year-old web designer, is a Canadian national. He has lived in Canada since 2004. In 2008, he was arrested in Iran while visiting his dying father and sentenced to death for having created pornographic websites. The cybernaut allegedly created a programme enabling the user to upload photos, but which was used without his knowledge to post pornographic images. Vahid Asghari has also been held since 2008. Like many prisoners, he was kept in solitary for seven months and tortured to make him admit that he had organised a pornographic network which blasphemed Islam. The two netizens were actually managing several news and opposition websites.

This year, Iranian authorities have unfortunately outdone themselves by incarcerating Navid Mohebbi, who was 18 at the time – the world's youngest blogger behind bars. This netizen, editor of the blog called "The writings of Navid Mohebbi" (http://navidmohebbi3.blogfa.com/) and women's rights activist in Iran, was arrested in his home on 18 September 2010 by eight Ministry of Intelligence agents. Beaten at the time of his arrest, he has been held in a cell with regular inmates ever since. The authorities accused the blogger of "activities contrary to national security" and "insulting the Islam Republic's founder and current leader" by means of "foreign media." He was also charged with being a member of the "One Million Signatures movement to petition for changes in laws that discriminate against women." The Revolutionary Court in the city of Amoi (in northern Iran) had sentenced him to three years in prison, but he was freed on parole on 25 December 2010.

REACTIONS OF THE INTERNATIONAL COMMUNITY

The European Union recently recalled that the sanctions against Iran cannot be limited to penalising nuclear proliferation, but must also target against human rights violations. Scottish Conservative Struan Stevenson recently called for the EU "to impose tougher sanctions on the clerical regime for its flagrant human rights violations."

U.S. Secretary of State Hillary Clinton recently praised "the courage of the Iranian people," who refuse to abandon their right to free speech.

Despite all the risks, the Iranian blogosphere remains one of the most active in the world. It can count on the attention and support of bloggers around the globe, who, even in the middle of the 2009 protests, were relaying photos of the repression and launching support groups on Twitter via hashtag #CN4Iran. Iranian cybernauts do not fear censorship and have learned to use such circumvention tools as the Farsi versions of UltraReach, FreeGate and Nassim – software developed by the Global Internet Freedom

Consortium in the United States and originally intended for Chinese netizens.

The recent events in Egypt and Tunisia have revitalised Internet mobilisation in Iran, but also to closer scrutiny on the part of censors. The Iranian Internet is once again navigating a turbulent period.

NORTH KOREA

INTERNET ENEMY

Domain name: .kp
Population: 22,665,345
Internet users: data not available
Average cost of a one-hour cybercafé connection: about 8 U.S. dollars
Average monthly salary: 17 dollars
Number of imprisoned netizens: 0

While Kim Jong Il has been diligently keeping his people away from the rest of the world, Internet access has been reserved for a small circle of the elite. Recently, the country made its entry into the social networks, bringing its virulent propaganda war onto the Web. North Korea's alleged first direct connections to the World Wide Web were first observed when the "Dear Leader" was preparing his succession.

INTERNET: AN ILLUSIONARY HUNTING GROUND FOR THE COUNTRY'S ELITE

North Korea is literally cut off from the world, and the Internet is no exception. The World Wide Web is only accessible to a small minority: a few of the regime's senior officials and some foreign diplomats, assured only (at least until the end of 2010) via a satellite link to foreign-based servers.

The great majority of the population is kept away from the Web and is restricted to using an intranet which provides an e-mail inbox, a few news sites relaying the regime's propaganda and a browser which gives users access to web pages with links to the databases of the country's three largest libraries: the Grand People's Study House, Kim Il-Sung University and Kim Chaek University of Technology. This intranet system is accessible only to academics, businessmen and high-ranking officials who have received special clearance. In the last few months, hand-picked information obtained from the World Wide Web was made available on the intranet. Some universities now use open-source software derived from the Web.

The capital's rare cybercafés are considered mainly as entertainment venues offering access to computers and games.

On the other hand, when foreigners are invited to North Korea, the regime pulls out all the stops. On the occasion of the 65th anniversary of the founding of the Workers' Party of Korea in October 2010, some 80 foreign journalists invited to cover the military parade were granted full Internet access from Hotel Koryo, where they were staying. This parade marked the official introduction of Kim Jong Il's son, Kim Jong Un, as the country's designated successor and his ascension to the Party's Central Committee and to the Central Military Commission.

During these celebrations, in October 2010, North Korea is said to have made its first full connection to the Worldwide Web from its own territory, as explained by Martyn Williams of IDG News Services.

FIRST DIRECT CONNECTIONS TO THE WORLD WIDE WEB FROM NORTH KOREA?

Traditionally, North Korea has been connecting its websites to the rest of the world via its foreign-based servers, but that is now changing.

Some sites using the domain name ".kp" are said to be gradually entering into service. The servers managing these domain names will now operate within the Star JV Network, a joint venture between the North Korean government and the Thai company Loxley Pacific. Six new second-level domains have apparently been recorded in addition to com.kp and edu.kp. These are: net.kp, gov.kp, org.kp, rep.kp, tra.kp and co.kp.
These include:

- Naenara: www.naenara.com.kp, a multilingual platform run by the Pyongyang-based Korean Computer Centre

- The Cultural Relations Committee, in collaboration with foreign countries: www.friend.com.kp

In addition, over 1,000 IP addresses assigned to North Korea in 2007 by the Internet Corporation for Assigned Names and Numbers (ICANN), but not previously used, are now in service, which suggests that servers have been set up in the country, making it possible to access the international network from North Korea: a first for the country.

The reasons for this turnabout are still not clear. Could it be an attempt to regain direct control, for ideological and practical reasons, over websites previously hosted abroad? At any rate, just as the country is supposedly making its direct entry on the World Wide Web, the regime is making an entrance on the social networks and simultaneously launching a particularly aggressive propaganda war.

THE PROPAGANDA WAR IS ALSO BEING WAGED ONLINE

The strained relations between the two Koreas have found a soundboard in the media and on the Web. South Korea resumed its radio propaganda broadcasts after one of its ships was torpedoed – an incident for which it blamed North Korea. The latter decided to retaliate, mainly on the Internet.

The regime decided to take advantage of social networks by creating accounts on Twitter (11,662 subscribers to date) and YouTube (for which the total views for all videos combined is currently 816,334) under the user name "Uriminzokkiri," which means "our nation" in Korean. An account by that name had been deleted by Facebook in August 2010, but a new and similar group emerged shortly thereafter with close to 500 members. The Internet website www.uriminzokkiri.com is run by the Committee for the Peaceful Reunification of Korea, a propaganda agency based in Pyongyang. It is the closest thing to North Korea's official website. These sites and accounts have been the target of cyberattacks in the last few months.

In 2010, North Korea "took its propaganda war against South Korea and the United States to a new frontier: YouTube and Twitter," to repeat Choe Sang-Hun's statement in The New York Times.

The propaganda circulating on these sites is meant to be particularly virulent against South Korea and the United States. In one video clip posted on the YouTube account (lien), U.S. Secretary of State Hillary Clinton is called a "minister in a skirt," Secretary of Defense Robert Gates a "war maniac" and former South Korean minister of defence Kim Tae-young a "servile dog" that likes to be patted by its "American master".

South Korean authorities are equally guilty of preventing their citizens from gaining access to the North's websites. (read the chapter on South Korea)

SMUGGLING NEWS

The cell telephone service provided by Egyptian company Orascom, which mainly serves Pyongyang and a few cities in the South, has been extended to some other cities, most of them along the border. It does not permit Internet access or international calls and remains too expensive for most North Koreans, even though the number of cell phones in circulation within the country has supposedly increased. Foreigners and Koreans are assigned two different types of numbers and it is impossible to make calls between them. The authorities can monitor these calls and are doing so. Security police are tracking anyone who attempts to use telecommunications as a means to defeat the government's control.

News smuggling is practiced in border areas. The limited information entering the country passes through the Chinese border in the form of clandestine CDs and DVDs. There is a thriving black market in those areas. Telephones from China can be used to make calls by capturing signals on the border. The recent introduction of 3G telephones in China may also improve Internet access in these border regions.

Among other alternative news websites is Dailynk, run by North Korean refugees based in South Korea. Independent radio stations broadcasting from South Korea to North Korea, Free North Korea Radio, Radio Free Chosun, Open Radio for North Korea and North Korea Reform Radio, mainly gather their news by calling upon stringers based along the Chinese border.

Nonetheless, the authorities announced in early 2010 that they intended to intensify their crackdown on “defectors” while tightening their control over border-based means of communication, focusing on the Chinese cell phones used in North Korea. The regime boasted that it has the means “to crush reactionary forces” and that it has already provided an example in January 2010, by executing a worker accused of having used an “illegal” Chinese cell phone. It is allegedly now using signal triangulation to localise and arrest offenders. Koreans who use such telephones are being careful to limit their calls to avoid being caught.

In this context, the first tentative connections from the country to the World Wide Web should not be viewed as a revolution or the first step towards generalised access by North Koreans to this open window on the outside world. This would be too dangerous for the regime.

Do these connections signal a new trend initiated by the regime’s heir apparent, who is said to be very familiar with the latest computer technologies? Or a desire, consistent with the country’s recent industrial modernisation, to partially open the Web to North Korean business?

In any case, the authorities remain resolved to maintain strict control over the population at all costs. This means controlling the Net and, above all, keeping most of the population away from the Web. The aim of North Korea’s new presence on the Web thus seems to be more to disseminate official news from the country than to allow any news unauthorised by the regime from entering it.

SAUDI ARABIA

INTERNET ENEMY

Domain name .sa
Population: plus de 25 millions…
Internet users: 11.2 million (according to correspondent, as of Sept. 2010) - 41%
Average monthly salary: $ 1233
Number of imprisoned netizens: 2

Unrelenting censorship still plagues the Net – the only space in the country where some form of freedom of expression has managed to thrive in the last few years. Some still-mobilised cyberdissidents, who were caught by the authorities exercising their right to voice critical opinions, paid a stiff price.

STRICT FILTERING AND DENUNCIATIONS

An strictly enforced filtering system targets any content which authorities deem to be pornographic or "morally reprehensible." Websites which discuss religious or human rights issues or the opposition viewpoints are also blocked. Far from concealing their actions, the authorities openly attest to their censorship practices and claim to have blocked some 400,000 sites.

Prohibited websites now include the Arab Network for Human Rights Information (ANHRI), (www.anhri.net/saudi/spdhr) and the sites www.gulfissues.net,www.saudiinstitute.org, www.arabianews.org, www.aljazeara.org and www.saudiaffairs.net.

The latest censorship targets are the pages about Saudi Arabia on the Arabic-language version of Wikileaks and the Elaph website (www.elaph.com), an online political news magazine. The latter had recently published an article entitled "Gulf after WikiLeaks storm: Riyadh speaks while all are silent." The article discussed the turmoil in political circles after WikiLeaks published cables revealing that Saudi diplomats had urged the United States to attack Iranian nuclear reactors.

Two websites were blocked in early 2011 in reaction to the Tunisian and Egyptian revolutions. Both sites, dawlaty.info and www.saudireform.com, were calling for political change in the country.

Participating websites are subject to particularly harsh censorship. The site newarabia.org, a political discussion forum, is blocked in Saudi Arabia. The blogger.com platform, totally blocked at first, is now the subject of a targeted censorship of its content – proof that authorities are no longer able to prevent blogger input. Censors took aim at the micro-blogging website Twitter for the first time in August 2009, blocking the pages of two human rights activists, Khaled al-Nasser and Walid Abdelkhair. Facebook pages on human rights were also rendered inaccessible. The government-controlled Internet Services Unit has even ventured to explain the principles behind its filtering policy on its website, www.isu.net.sa/saudi-internet/

contenet-filtring/filtring.htm. It provides a form which citizens can use to request that a website be blocked or unblocked. According to Saudi authorities, this procedure has been rather successful. The Telecommunications and Information Technologies Agency claims that the blocking requests target from 700 to 1,000 sites daily, averaging some 300,000 "citizen-denounced" sites per year. A representative of that same agency estimates that 93% of the filtered sites are pornographic in nature. The rest: websites which disseminate information "contrary to kingdom values." One of the agency's officials acknowledges, however, that 55% of users are concerned about the blockings and that three-quarters of them feel that the current filtering policy is too harsh.

BLACKBERRYS UNDER PRESSURE

BlackBerry phones are popular in the Gulf and in Saudi Arabia, where they enable users to circumvent censorship. However, as a result of pressures from authorities threatening to block the BlackBerrys' instant messaging service, RIM, the BlackBerry manufacturing company, allegedly agreed, in August 2010, to install a server in Saudi Arabia. Supposedly, the aim was not to share the keys to its encryption with Saudi authorities, which would enable them to set up real-time surveillance, but to give them the opportunity of having court-ordered access to certain messages after the fact. In view of the Saudi court system's independent status, the country's smartphone users have reasons to be worried.

CYBERCAFÉS UNDER SURVEILLANCE

Draconian restrictions were imposed on cybercafés as of April 2009. They are now required to install hidden cameras, provide a list of customers and websites consulted, prohibit the use of prepaid cards or non-authorised Internet satellite links, to close at midnight and to refuse to admit minors.

Their owners risk prison terms if their premises are used to disseminate information contrary to "kingdom values" as set out in the 2008 law on the use of technology. This law also provides ten-year prison sentences for Internet website managers who promote terrorism, and five years for those who disseminate pornographic information or violate the country's religious and social values.

ANTI-FREEDOM LEGISLATION INTENSIFIES

New regulations on Internet publications aimed at strengthening Net censorship and discouraging Internet users from creating a website or blog were announced on 1 January 2011 by the Minister of Culture and Information, Abdul Aziz Khoja.

According to Article 7 of this text, online media, the Internet websites of the so-called "traditional" media, and platforms circulating audio or video material and offering online ads must, in order to operate, obtain an Internet licence, valid for three years, from the Ministry of Culture and Information. In order to get it, the applicant must be at least 20 years of age, be a Saudi national and hold a diploma equivalent to the baccalaureate. He or she also must produce "certificates of good conduct."

The media must also indicate the name of their hosting service, which gives the government the option of forcing the service to eliminate the site or its content. All forms, blogs or personal Internet sites, distribution lists, electronic archives or "chat rooms" will henceforth have to be registered. Bloggers may identify themselves "if they wish to." The obvious intent is to chip away at their anonymity. The Ministry was supposed to first approve the editor appointed for all electronic newspapers. However, in view of the wave of protests triggered by this provision, the Minister of Information promised, on 6 January, to drop it. All that is required now is for a "simple declaration" of the editor's identity to be filed with the Ministry.

Under Article 17, any violation of these provisions is punishable by fines and a partial or total, temporary or permanent, blocking of the website. Fines may be as high as 100,000 Saudi riyals (20,000 euros), which constitutes an indirect form of economic censorship, given that many sites cannot afford to pay such a sum. The Ministry reserves the right to expand the scope of these measures.

INCARCERATED CYBERDISSIDENTS

Any bloggers who dare to discuss sensitive subjects are subject to censor reprisals. Two of them were arrested in 2010. Sheikh Mekhlef bin Dahham al-Shammari, a writer, social reformer and human rights activist known for his outspoken defence of women's rights and his efforts to

reconcile Shiites and Sunnis, has been behind bars since 15 June 2010 and is said to be in poor health. He stands accused, quite fancifully, of "annoying others." His arrest was linked to his criticisms of political and religious leaders, posted primarily on the new sites www.saudiyoon.com and www.rasid.com.

Mohammed Abdallah Al-Abdulkarim, a law professor and activist known for his efforts to defend political and civic rights, was arrested on 5 December 2010 in Riyadh. Following King Abdullah bin Abdulaziz Al Saud's medically motivated trip to the United States, Mohammed Al-Abdulkarim posted, on 23 November 2010, on the website http://royaah.net/, an article mentioning differences within the royal family – specifically disputes over King Abdullah's succession and their consequences for Saudi Arabia's political future. In this post, he mentioned not only the King's state of health, but also the power struggle between the 86-year-old sovereign's potential successors.

There is still no news of Syrian blogger Raafat Al-Ghanim, a resident of Saudi Arabia who was arrested in July 2009. He openly criticised the Syrian and Saudi social and political situations on both countries' online forums.

FACEBOOK: A TOOL FOR MOBILISATION OR SOCIALISATION?

In November 2010, Facebook was blocked for several hours for having violated Saudi Arabia's moral values, which raised caused a stir on the Web. Was this an isolated incident or a test paving the way for even harsher censorship? The authorities have little tolerance for online mobilisations, especially since the Tunisian revolution.

Not only are Saudi netizens resisting censorship by learning how to circumvent it, but they are also capable of conducting online mobilisation campaigns, notably on Facebook.

In 2010, a woman launched a Facebook group to protest against the ban prohibiting women from working in lingerie shops. She succeeded in winning 10,000 supporters: http://www.facebook.com/pages/hmlt-kfayt-ahraj-dd-by-alrjal-llmlabs-aldakhlyt-alnsayyt/119561098100718.

The Net has been providing Saudi women – who now represent more than half of the country's bloggers and internet users – with an unprecedented space in which to express themselves. There, they can discuss topics which they are forbidden to mention in public, such as health. Saudi Arabia's tight control over these new technologies also indicates the depth of their resolve to maintain the social order.

Online mobilisations are also being launched in support of human rights activists. News about Mohammed Abdallah Al-Abdulkarim's arrest was initially circulated on his Facebook page before being reposted on a large number of Internet websites. Numerous Saudi human rights organisations publicly denounced it. Several Facebook pages, including "We are all Mohammed Abdulkarim" and "Free Dr. Abdulkarim" http://www.facebook.com/FreeDrAlabdullkarim), as well as a hashtag (#FreeDrAbdulkarim) on Twitter, were created to demand his immediate release. His case aroused heated discussions between netizens siding with him and those who sided with the regime. A memorable debate broke out on Twitter between Abdulrahman Alenad, a member of the Consultative Assembly of Saudi Arabia (Shura) and Dr. Abdulkarim's lawyer, Waleed Abulkhair, when the former ordered the latter to keep quiet.

SYRIA

ENNEMIS D'INTERNET

Domain name: .sy
Population: 22,198,110
Internet users: 3,935,000
Average cost for a one-hour cybercafé connection: from 1 to 2 U.S. dollars
Average monthly salary: 200dollars
Number of imprisoned netizens: 3

Syria's lack of infrastructure is still impeding Web growth. The new online media law has tightened censorship which, from late 2010 until now, has sought to discourage messages concerning the regime's fall in Tunisia. As a symbol of netizen repression, the case of Tal al-Mallouhi – the youngest blogger in the world behind bars – is mobilising the blogosphere beyond Syria's borders.

CONTROLLED GROWTH OF THE INTERNET

Although internet access has expanded considerably in the last decade, the infrastructure has shown little improvement, resulting in bottleneck problems, connection slowdowns and frequent outages. The very slow connection speed remains a key obstacle to Internet use. Most cybernauts are restricted to a speed of 56Kb, which severely limits downloads and makes it arduous to navigate the Web. In peak periods the speed is even slower. ADSL and 3G connections are still expensive. Nonetheless, the 3G network controlled by the Syriatel mobile telephone company – owned by Rami Makhlouf, a cousin of the president – is experiencing strong growth.

Syrian Telecom has announced a plan to expand ADSL access within the country. A new 10-Gb broadband portal is said to have replaced the former international backbone portal. Yet in actuality, the technical improvement promised by the authorities has been slow to materialise. Some interpret this as a deliberate plan to keep the population off the Web.

Internet control is carried out by two government agencies, the Syrian Telecommunications Establishment (STE) and the Syrian Information Organisation (SIO), which control bandwidth. The STE and SIO use Thundercache software to maintain a centralised control over the Web. The programme provides online website monitoring and filtering by spotting key "banned" words.

The Syrian government, which had long been minimising its Web presence, has completely reversed course, mainly due to Bachar al-Assad's influence. Websites promoting propaganda or official positions are proliferating, such as those of the Syrian News Agency (SANA), Syria News, Al-Gamal, Sada Suria and Sham Press, not to mention Presidentassad.net – all praising the Head of State. The President and the First Lady, Asma al-Assad, already had pages on Facebook even before the social network was

unblocked again in the country, in February 2011. However, the President and First Lady Asma al-Assad, already had their own Facebook pages. In January 2011, the Presidential Palace's press service, finding it necessary to clarify the situation, explained that these were neither official pages nor official communication channels, but merely the result of individual initiatives by the president and the First Lady.

SPECIFIC CONTENT FILTERING

In December 2010, Syrian Minister of Telecommunications and Technology, Imad Sabouni, stated during a seminar held by Latakia University that censorship was not a solution and that it was more important to raise Internet users' awareness, while stressing the need for caution on social networks which can harm private lives. He also pointed out that Internet-blocking systems exist in all countries.

Nonetheless, censorship never abated in 2010. To date, 240 websites are blocked. The contents affected involved political criticism, religious matters, sites deemed "obscene," sites discussing the Kurd minority, and those based in Israel. Other sites targeted are those of the opposition parties, certain Lebanese newspapers and independent news sites. The website www.onemideast.org, launched in May 2010, was rendered inaccessible in the country. It provides Syrians and Israelis with a public forum on which they can discuss obstacles to peace between their two countries. Contributors from both countries have posted a list of the top twenty impediments.

The Syrian government justifies its actions by claiming that its aim is to prevent "denominational unrest" and any attempt at infiltration on the part of Israel.

Traditionally, censors have been particularly wary of social networks and blog platforms. Potential dissidents must be prevented, at any cost, from forming groups and recruiting additional members through the net media. Blogspot and Maktoob are blocked. YouTube has been inaccessible since August 2007, after videos were circulated which denounced the crackdown on the Kurd minority. Wikipedia's Arabic version was blocked from May 2008 to February 2009. Amazon and Skype are also censored.

TUNISIAN REVOLUTION IN THE CENSORS' LINE OF SIGHT

In an interview granted to the The Wall Street Journal on 31 January 2010, Bachar al-Assad declared that "real reform is about knowing how to open up the society and how to start dialogue," explaining that decades of political and economic stagnation, leaders with no ideology, foreign interventions and wars have generated the agitation in the streets of Tunisia and Egypt.

At the same time, while the traditional Syrian media scarcely mentioned the fall of President Ben Ali's regime in compliance with orders from the authorities, the latter have tightened Web censorship, fearing that the Internet and social networks might promote social unrest.

For example, on 26 January 2011, the authorities blocked access to Nimbuzz and eBuddy – programmes which enable surfers to use chat functions, like those on Facebook, from a mobile telephone.

Several Syrian websites have also been preventing netizens from leaving comments on the popular uprising in Tunisia, such as Syria News, a pro-government website, while others have left a few very moderate or vague comments, removing the more explicit comments.

In February 2011, there was a wave of blogger arrests in connection with the Tunisian and Egyptian revolutions. In the morning of 20 February 2011, blogger Ahmad Hadifa, known by the blog name of Ahmad Abu Al-Kheir, was arrested in Baniyas by military security officials and released four days later. Hadifa, 28, a journalism student at the Falsam Al-Islam institute in Damascus, had used his blog, ahmadblogs.net, to request support for the bloggers recently arrested in Syria and for the political prisoners incarcerated in Golan (a region occupied by Israel since 1967 and annexed since 1961). He had also posted demands for Syrian authorities and updates on the last few weeks of uprisings in Tunisia and Egypt, and provided advice on how to circumvent Internet censorship.

In addition, a cybernaut was arrested for posting on YouTube a video of the 17 February 2011 demonstration in the Harika district of Damascus. During that protest, a young man was beaten by police. The video shows several hundred people shouting anti-police slogans, and Said Sammour, the Ministry of the Interior, addressing the crowd.

However, the authorities reversed their tactics in February 2011, when they began to realise how ineffective their censorship system was. While popular revolts were at their height in the Arab world – undoubtedly having been stirred up by social networks – in February 2011, Syrian authorities decided to unblock access to Facebook and Twitter. This was a way for them to make concessions without jeopardising their position. Facebook was already very popular in the country, and netizens were using censorship circumvention tools to gain access to it.

JAILED FOR EXPRESSING THEMSELVES FREELY ON THE INTERNET

Syria continues to incarcerate netizens so as to make examples of them and to persuade others to practice self-censorship. To date, at least three cyberdissidents are behind bars.

On 6 May 2008, Syrian government security agents arrested writer and cyberdissident Habib Saleh. He was sentenced to three years in prison on 15 March 2009, by virtue of Article 285 of the Syrian Penal Code for “weakening national sentiment” after disseminating on the Internet of political articles calling for governmental reform, democracy and freedom of opinion. This is the third time that he has been tried under Bachar al-Assad’s regime.

Kamal Cheikhou ben Hussein a Kurd blogger and student at Damascus University’s Faculty of Literature and Human Sciences, was arrested on 23 June 2010 while attempting to enter Lebanon with his brother’s passport. There has been no news of him since then. Syrian authorities have forbidden this author of numerous publications on the All4syria website to leave the country. On 16 February 2011, he began a hunger strike to protest against his detention conditions in Adra prison. Held since 23 June 2010 under charges of “publishing information that could compromise the nation’s honour,” his trial is scheduled to begin on 7 March.

Journalist and writer Ali Al-Abdallah is still behind bars. Incarcerated since 17 December 2007 for having signed the Damascus Declaration, he was expected to be released on 16 June 2010, after serving a two-and-one-half year prison term, but the Syrian authorities decided to charge him with "spreading false information with the aim of harming the state” (Article 286 of the Syrian Penal Code) and "intending to harm Syria’s relations with a another state” (Article 276 of the Penal Code). These new charges followed the publication on the Internet, on 23 August 2008 – while he was in prison – of an article in which the journalist criticised Iran’s Wilayat al-Faqih doctrine (which gives the country’s clerics absolute power over political affairs). The Syrian Third Military Court in Damascus issued new counts of indictment against him which the Court of Appeals upheld on 1 December 2010. Ali Al-Abdallah now faces a possible new prison term. This new development is all the more troubling in that it shows how dangerous it is for journalists to criticise not only the regime, but also its allies.

The Tal al-Mallouhi case[1] has caused great concern not only in Syria, but around the globe. This 19 year-old student – the youngest female blogger to be in custody anywhere in the world – was arrested by Syrian intelligence officers in late December 2009. Her computer and her personal effects were also seized. The fate of Palestinians was the main topic she discussed on her blog. After being detained in an unknown location for eleven months, she appeared before the Supreme State Security Court on 10 November 2010 and 17 January 2011. She was sentenced on 14 February 2010 to five years in prison for “divulging information to a foreign state,” namely the United States. Her sentence, typical of the brutality of the Syrian regime’s repression, is designed to intimidate Syrian bloggers by making Tal Al-Mallouhi a scapegoat.

Lastly, there has been no news of three other bloggers since their arrest: Firaz Akram Mahmoud, arbitrarily arrested in a cybercafé in Homs on 5 February 2011, Ahmed Ben Farhan Al-Alawi, arrested by security agents on 26 October 2010 and Ahmed Ben Abdelhalim Aboush, held since 20 July 2010. The latter had been incarcerated for six years until he was released under a presidential pardon on 2 November 2005.

INTERNET USERS ARE BEING WATCHED

Since 2007, the authorities have been requiring website owners to retain personal data of the authors of articles and comments posted online.

Police raids on cybercafés are commonplace. Officers

suggest to netizens caught doing "excessive surfing" that they "have a cup of coffee with them" – their expression for taking them in "for questioning." Website managers must keep visitors' personal data and a list of visited sites, and alert the authorities if they notice any illegal activities. Cybernauts even have to provide the name of their mothers and fathers.

Activist Suhair Atassi, leader of the "Jamal Atassi Forum" on Facebook, who has been calling for political reforms, civil rights guarantees and an end to the State of Emergency Law, has been subjected to multiple pressures and threats on the part of the authorities. Nonetheless, she has refused to dissolve her group.

NEW LAW TARGETS ONLINE FREEDOM OF EXPRESSION

An Internet communications bill formulated by Syrian Prime Minister Mohammad Naji Otri, was approved by the cabinet in November 2010. Parliament is expected to vote on this bill soon.

The aim of this bill is clearly to further restrict the circulation of information on the Internet.[2] Two provisions are particularly disturbing. The first would allow the authorities to try journalists before criminal courts and impose harsh jail sentences. The second would allow any "judicial auxiliary" – an intentionally broad term – to conduct investigations on journalists suspected of committing "crimes" as defined by law, and to decide whether or not they should be arrested.

Ayman Abdel-Nourm, head of the All4syria.org website, which is blocked in Syria, told AFP that he thought this bill was "very harsh," as it would notably allow "police to be dispatched to editorial offices to arrest journalists and seize their computers."

The new bill is a reaction to the growth of new media in Syria over the last few years, which is deemed to be a threat to the regime. A dozen radio stations, as well as privately owned newspapers and magazines, have recently been created, headed by a new generation of journalists. One of them, Forward Magazine, also has a digital version featuring blogs and tweets on political and social topics. Some online journalists feel that they can express themselves more freely on the Web than on a paper version. This bill may convince them otherwise.

EMERGENCE OF ONLINE PRESSURE GROUPS

Many Internet users have mastered censorship circumvention tools. When the authorities start blocking the proxies most often used, others are created.

Facebook was blocked when the Syrians began making friends with Israelis, yet the social network, which is very popular in the country, hosts hundreds of groups with hundreds – if not thousands – of members devoted to tourism, business, sports, technology and entertainment.

Online pressure groups have formed to express their economic or social demands. One online campaign opposing a bill on amending the existing personal statute law seems to have played a crucial role in the government's decision to abandon it, especially since privately owned radio stations had broadcasted online posts objecting to the legalisation of marriage for girls as young as 13.

Netizens from around the world mobilised on behalf of Tal al-Mallouhi. Egyptian bloggers massively rallied around her case.[3] International attention was probably also a contributing factor to her appearance before a court in November 2010, after she had been held in an unknown location for nearly eleven months.

In September 2010, a video showing teachers hitting their young students circulated around the Web after having been posted on Facebook. The Syrian cybernauts' anger spread to the rest of the population, forcing the Syrian Minister of Education to ask the teachers involved to resign and to reassign them to office jobs.

A Facebook group was launched at the end of January 2011 to call for a peaceful Damascus sit-in "in front of the Egyptian embassy to express our condolences for Egyptian victims." Syrian police dispersed a group of some fifty young people who had gathered on 29 January, carrying candles. Many Syrians left comments on Facebook such as "One day, I will have the courage to become Tunisian."

WILL INTERNET FREEDOM FOSTER INNOVATION?

In June 2010, a delegation of representatives of U.S. high-tech companies – among them Microsoft, Dell and Cisco Systems – led by the State Department, met the Syrian President, officially to open a new market for U.S. technology exports and to promote freedom of expression online. American leaders seem to be banking on a more open form of the Internet in Syria and are dangling the prospect of millions of dollars of investments, insisting that U.S. companies cannot do business in such a closed environment and that a free Internet fosters innovation.

Although a few hopes had flourished with the growth of online media and their effort to push back the limits of censorship, the adoption of the law clearly shows that the authorities are continuing to do everything possible to block the Internet in order to prevent any discontent online from spreading offline. These early 2011 uprisings by Arab civil societies are bound to convince the regimes that they should maintain their current Internet strategy. Despite the fact that the Syrian government acts as though it were ready to give the international community guarantees that it will end its diplomatic isolation and attract foreign investors, it is ultimately unwilling to give up its control of the Web.

TURKMENISTAN 

INTERNET ENEMY

Domain name: .tm
Population: 5,342,342
Number of Internet users: 127,000
Average cost of a one-hour cybercafé connection: about 1 U.S. dollar
Average monthly salary: about 200 U.S. dollars
Number of imprisoned netizens: 0

The Turkmen government has curbed the very recent Internet growth and continues to practice widespread censorship. Its monopolistic takeover of the cell telephone market has allowed it to enhance its control over communications. The international community seems more determined to make concessions than to exert any real pressure on this country, in view of its vast energy and strategic potential.

PROHIBITIVE COSTS OF INTERNET ACCESS

Although President Gurbanguly Berdimuhamedow finally allowed Turkmen to access the Web in 2008, many technical and financial barriers still remain. Internet access is possible, but its generalised use is not encouraged.

Apart from the few businesses and foreign embassies which can access the Worldwide Web, the few other Internet users can only access an ultra-censored version of the Internet nicknamed "the Turkmenet." Very strict filtering is focusing on opposition Turkmen-language publications, targeting primarily local users and potential dissidents, mainly for linguistic reasons. Opposition websites such as XpoHo.tm and Gundogar, and regional news sites covering Central Asia such as ferghana.ru and eurasianet, are blocked. YouTube and LiveJournal were rendered inaccessible late in 2009 to prevent Turkmen from blogging or sending videos abroad. Facebook and Twitter are also blocked.

However, Turkmen can view most generalist NGO websites. The same applies to Russian and Turkmen media websites that contain no articles critical of Turkmenistan, because of the significant commercial ties between the two countries.

In view of the climate of terror prevailing in the country, Turkmen netizens do not discuss political or societal subjects online. They consult their e-mail boxes and exchange messages with their friends via Skype or cell phone instant messaging services. A few Turkmen social networks were created about two years ago. The Teswirlar.com forum and the blog platform Talyplar.com are highly popular among the country's netizens and the diaspora. They receive hundreds of visitors every day.

One notable improvement is the fact that Turkmen citizens are now allowed to have personal computers, even if the latter's purchase price automatically puts them out of reach for all but the elite. The setting up of WiFi connections affords users more flexibility and allows them to

avoid having to communicate their personal information, as they need to do when ordering a subscription or in a cybercafé. The authorities keep these establishments under very close surveillance. On the other hand, netizens no longer have to tell the manager which websites they want to consult, as was previously the case...

Most Turkmen connect from cybercafés, since the regime imposes prohibitive rates for Internet access. An unlimited monthly Internet subscription at a speed of 64 Kbit/sec costs $213.16. The cost for ADSL is almost $7,000, even though the average monthly salary is about $200! For those who choose unlimited access, the cost will be $25 for 1 MB.

Bandwidth speed is often very slow. Some users who have private connections complain that they can only use the Internet a short time during the day. At night, the speed is somewhat faster. Some of them go to the offices of international organisations to get access to the World Wide Web.

CELL PHONES UNDER PRESSURE

In December 2010, a shortage of cell phone SIM cards once again caused long waiting lines in Ashgabat, according to the Chronicles of Turkmenistan website, published by the NGO Turkmen Initiative of Human Rights. Long lines also formed in front of the Altyn Asyr brand shops.

This "shortage" coincided with the departure from Turkmenistan of the Russian telecommunications company MTS, leaving some two million Mobile TeleSystem subscribers without access. The licence granted to MTS-Turkmenistan was suspended, effective on 21 December 2010, by the Ministry of Communications. The only competitor of the state-owned company and market leader Altyn Asyr was thus eliminated. Altyn Asyr, which until then only had a few hundred thousand subscribers, now enjoys a monopoly status, which assures the government an even stronger control of cell phones in terms of censorship and surveillance. Unlike MTS, Altyn Asyr blocks access to independent and opposition websites.

A RETURN TO REPRESSION?

On 30 September, President Berdimuhamedow gave a belligerent speech before National Security Ministry officials, calling on them to fight against those who "defame our secular and democratic law-based state and try to destroy the unity and solidarity of our society."

The website of the Turkmen Initiative for Human Rights (TIHR) was hacked in early October 2010 and had to change its host site. These attacks followed an interview which the NGO's director, Farid Tukhbatullin, granted on 28 September 2010 to the satellite TV station K+. Broadcast in Central Asia, it was therefore accessible to the Turkmen population. Farid Tukhbatullin, who is exiled in Vienna, addressed the human rights situation in Turkmenistan. The authorities were apparently displeased with his comments.

In the last few months, several dissidents have been forbidden to leave the country, including human rights activist Umida Dzhumabaeva, one of the most recent examples, in July 2010. The authorities reproach her for her activities and relations with other dissidents. She was accused, totally without proof, of having delivered information to opposition websites.

IS THE INTERNATIONAL COMMUNITY PREPARED TO OFFER ANY CONCESSIONS?

Turkmenistan's capital, Ashgabat, plays a key role in supporting NATO within the framework of the war in Afghanistan, mainly by authorising it to access Turkmen air space, which the U.S. views as a strategic asset. Despite this, U.S. Assistant Secretary of State Robert Blake, while visiting the country in February 2011, conveyed a warning to Central Asian countries which practice harsh censorship: "It is important for leaders of countries where the companies are controlled to listen to the lessons of Tunisia and Egypt."
This position contrasts with that of French diplomacy. According to a cable leaded by WikiLeaks and published in the newspaper Le Monde, "The French Embassy refrains from speaking out on the issues of religious freedom or human rights so as not to compromise (contracts with the Group) Bouygues," which enjoys a privileged status in the country.

As for the European Union, it is about to enter into a Partnership and Cooperation Agreement (PCA) with Turkmenistan, which would include a monitoring clause concer-

ning the human rights situation and calls for the country's democratisation, under penalty of suspension. The European Parliament's Foreign Affairs Committee took a position in January 2011 in favour of signing this political and economic agreement.

UZBEKISTAN

INTERNET ENEMY

Domain name: .uz
Population: 27.8 millions
Internet users: 6.626 million
Average cost for a one-hour cybercafé connection: 800 soums per hour ($0.35)
Average monthly salary: $289
Number of imprisoned netizens: 0

Despite the European Union's decision in late 2009 to lift the sanctions against Uzbekistan, the regime has not loosened its grasp on the Net – quite to the contrary. This police state is still routinely preventing the dissemination of information online and all efforts to initiate a civil society – virtual or any other kind.

BETTER ACCESS TO THE INTERNET?

Internet access costs are gradually decreasing, thereby providing more opportunities for the population to surf the Web. Consequently the number of Internet users is rising by 2 to 3% every three months. There is still a long way to go before the Internet will be accessible to everyone, but at least access costs are no longer an insurmountable barrier.

Netizens primarily visit entertainment sites. The most popular news website is Gazeta.uz. Uzbek netizens seem to prefer Russian-language social networks to blogs. Odnoklassniki.ru ("Classmates") and My World (my.mail.ru) have higher traffic rates than Facebook and Twitter.

BIG BROTHER IS ABOUT TO FINE-TUNE ITS CENSORSHIP

The Centre for Monitoring Mass Communications (CMMC) closely monitors the content of Internet websites and audiovisual media. Reporting to the Uzbek Agency for Communications and Information (UzASCI), it is responsible for blocking the IP addresses of the sites or articles which it deems undesirable.

Among the blocked sites are the Ferghana.ru news agency website and that of Nezavissimaya Gazeta (www.ng.ru). The regional news site Centrasia.ru is partially blocked, but most of the pages can still be read. When attempting to access prohibited articles, Internet users are redirected to the home page. The Central Asian News Service site, www.ca-news.org, is also partially blocked. The Uzbek-language BBC is constantly blocked, as is the Russian version intermittently. Social networks such as LiveJournal, MySpace, Facebook, Twitter, Blogger, Flickr and the most popular blog platform in Uzbekistan, kloop.kg, are made inaccessible from time to time.

Sensitive subjects include criticisms of the government, information on the actual state of the economy, human rights and the social situation. It is not advisable to discuss the private business of the Karimov family or their daughters' personal lives, the forced labour of children in

cotton fields, or emergency situations. It is much too risky to mention petrol supply problems, inflation, the population's impoverishment, and social unrest. Any reference to the Andijan massacre is simply removed. The population has long since stopped bringing up the subject in public – and even sometimes in private. Self-censorship is widespread.

Censorship is enforced inconsistently and varies in accordance with what is happening in the country. During President Karimov's visit to Russia from 19 to 20 April 2010, some articles on the Ria Novosti website were blocked in Uzbekistan. Internet service providers sometimes block articles on Uzbekistan published on news agency websites such as lenta.ru or newsru.com.

Officially, however, the government denies that it censures the Net. In March 2010, when asked by the NGO Forum 18 why such sites as Ferghana.ru or Rferl.org were being blocked, Elbek Dalimov, Head of the Press Service of Uzbekistan's State Agency of Communications and Information, claimed that his agency did not block websites. He merely acknowledged that access to some "terrorist" or "pornographic" websites was banned in licensing agreements with Internet service providers.

FACEBOOK BLOCKED SEVERAL HOURS

One piece of news which caused quite a stir was that access to Facebook was blocked in the country for several hours on 21 October 2010, but not uniformly. According to Neweurasia.net, a source with the main Internet service provider, TshTT, confirmed that an order had been given to block Facebook for just a few days . Some access providers did as instructed, others did not. Users protests demanding that Facebook contact local Internet access providers to find out what was going on allegedly resulted in the block being lifted.

Certain users welcome the addition on Facebook pages of ads for some of the blocked sites – ferghana.ru, Uznews.net and neweurasia.net – which allow them to access said websites. Nonetheless, the social network is said to be accessible via mobile phones. Mobile phone operators, such as MTS-Uzbekistan, are not state-owned.

Attempts to block social networks have been viewed by Uzbek netizens as a way for the government to prevent the dissemination of information and as a test for the future implementation of even more drastic restrictions on social networks.

ONLINE JOURNALIST FIRST SENTENCED, THEN PARDONED

Vladimir Berezovsky, Russian editor of the Tashkent-based news website vesti.uz, was convicted on defamation charges on October 13, 2010 and released on the occasion of the 19th anniversary of the country's independence. Charges were brought against Berezovsky the day after Vesti published an article criticising the authorities' decision to rename a street in the capital which originally bore the name of a Russian-born Uzbek citizen.

TOUGHER LAWS FOR ONLINE PUBLICATIONS

Internet access is governed by Article 29 of Uzbekistan's Constitution, which prohibits anyone from seeking, obtaining and disseminating any information directed against the existing constitutional system or divulging any state secret or confidential corporate information.

The 2002 Law on Principles and Guarantees of Freedom of Information authorises the government to restrict this freedom of information when necessary to protect any individual from "the psychological impact of negative information." Order no. 216 of 2004 prohibits Internet service providers and operators from disseminating certain types of information. A broad interpretation of the targeted content is made by the national operator Uzbek Telecom. The 2007 Media Law renders editors and journalists liable for the "objectivity" of their publications and applies to online media. The January 2010 amendments to this law now obligate Internet websites, as well as all other media, to register and to provide information on their employees and copies of their articles to the government.

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

NETIZENS UNDER SURVEILLANCE

The one thousand or so cybercafés operating in the country are not evenly monitored. There is a widespread use of spyware. Tests conducted by Reporters Without Borders have shown that certain café managers reacted when anti-spyware software was installed on one of their computers, while in other cybercafés, such tampering went unnoticed. Some censorship circumvention tools may have been used in certain cafés, but not in others. Several OpenNet Initiative researchers were questioned in 2007 while they were testing website filtering systems.

E-mails are also under surveillance, as are chat rooms, particular those of ICQ and Mail.ru Agent. Several people were supposedly arrested in January 2010 for their alleged membership in extremist religious organisations after they were spotted based on the content of their chats on Mail.ru Agent.

A new law in effect since 18 May 2010 is aimed at "improving young people's conduct" to prevent them from "engaging in criminal activities." Accordingly, the government decreed that young people under the age of 18 could not go into bars, restaurants, cinemas, nightclubs or even cybercafés unless accompanied by a legal guardian. One way of controlling the information available to young people is to deprive them of Web access. This law has obviously been ignored by those most concerned. Many minors can be seen alone in these places at night.

In May 2010, MPs and government representatives considered restricting young people's use of their mobile phones in schools and universities, among other options.

THE GOVERNMENT POSITIONS ITSELF ON UZNET

The main websites used by the government to relay its online propaganda are Press-uz.info, GT.uz and Gorizont.uz. In addition, some sites registered in Kazakhstan or in Kyrgyzstan are used to compromise human rights activists, members of the opposition, or journalists. They also provide a means to justify certain decisions made by the government and the president.

WHAT IS THE INTERNATIONAL COMMUNITY DOING?

In September 2010, Dunja Mijatovic, the Representative on Freedom of the Media for the Organization for Security and Co-Operation in Europe (OSCE) publicly shared her concern about the judicial pressures which are still being brought to bear on independent journalists in Uzbekistan.

In addition, U.S. Secretary of State Hillary Clinton, during her visit to Tachkent in early December 2010, asked President Karimov to "demonstrate his commitment through a series of steps to ensure that human rights and fundamental freedoms are truly protected."

These few examples of encouraging interventions remain the exception. In October 2009, the European Union lifted its remaining sanctions against Uzbekistan in order to encourage "Uzbek authorities to take further substantive steps to improve the rule of law and the human rights situation." Democracy and human rights have thus been sacrificed on the altar of energy and military co-operation.

The government knows he is in a position of strength while he is trying to emerge from its isolation and attract foreign investors. Uzbekistan is an important transit hub for getting supplies to Western troops deployed in Afghanistan. The country also has substantial energy resources.

VIETNAM

INTERNET ENEMY

Population: 86 million
Penetration rate: 27.3 million Internet users - 31% of the population, according to the General Statistics Office of Vietnam
Average monthly salary: 126 U.S. dollars
Number of jailed netizens: 17

The 11th Vietnamese Communist Party Congress of January 2011 marked the start of a more hard-line approach on the part of the regime to its critics, and was preceded by a new, particularly harsh wave of repression aimed at those who dare to exercise their freedom of expression. A lead weight is bearing down on the country's dissidents. There has been massive use of cyberattacks to silence dissenting opinion. Blogging has become dangerous.

THE "INTERNET THREAT"

Internet use continues to spread among the population: 31% of Vietnamese are now connected. Young people are particularly keen about spending time online. Facebook users now number two million and 70% of them are 14 to 24 years old.

The blocking of Facebook, intermittent in 2009, accelerated in December 2010, to its users' great dismay. The latter "gathered" on the social network, forming several groups. One of them, known as "A million signatures to protest Vietnamese ISPs blocking FB," has attracted, to date, over 46,000 Internet supporters since February 2011.

Online media and blogs, mainly those hosted on Wordpress, Multiply or Blogspot, thanks to contributions from citizen journalists, have acquired a de facto status equivalent to a sort of independent private press and are having a growing impact on public opinion. Websites such as Vietnam Net and Vietnam News cover such topics as corruption, social issues and the political situation. Bloggers are carrying out actual field surveys whose results could not be published in the traditional media. Thanks to the Internet and to the debate and opinion-sharing spaces which it offers, a virtual civil society has emerged. Pro-democratic activists and critics of the government have found refuge there, which worries the authorities.

The most widely discussed topics are territorial disputes with China, corruption, disagreements over land ownership and freedom of expression – subjects which are rarely, if ever, mentioned in the traditional media. China's bauxite mining activities and the related environmental risks are taboo, particularly because they are causing rifts within the party itself.

The filtering of Internet websites seems to have neither increased nor declined in the last few months. The majority of bloggers practice self-censorship for fear of becoming a target for the authorities. Certain bloggers have indicated that when they write on “sensitive” subjects, their posts are deleted by “third parties.”

Authorities close down websites or blogs in the open. On 5 May 2010, Gen. Vu Hai Trieu, Deputy Director of the Public Security Ministry, announced: “Our technical departments have destroyed 300 Internet web pages and blogs posting unsuitable contents.” ,

Filtering is no longer the main method used to curtail Internet freedom. The Vietnamese regime prefers to deploy cyberattacks and spyware, and to steal users’ IDs and passwords from opposition website administrators.

THE AUTHORITIES: INSTIGATORS OF ANTI-FREEDOM CYBERATTACKS

Cyberattacks have become commonplace, most often in the form of a "Distributed Denial-of-Service" (DDoS). This is a type of cyberattack aimed at putting a site out-of-service, by submerging it with unnecessary traffic. Although over one thousand sites were affected in 2009 – twice as many as in 2008 – according to the official Vietnamese press, that figure is said to have increased ten-fold in 2010.

Among the sites targeted is the “Anhbasam” blog, well-known for its insightful content and political analyses, created by former police officer Nguyen Huu Vinh. Other targeted websites are DCV Online, bauxitevietnam.info and Doi Thoai, as well as danluan.org, danchimviet.info and danfambao.com. In late August 2010, many opposition sites and blogs were simultaneously attacked for several days, coinciding with the national holiday of 2 September. The main focus of these attacks were anti-government websites, implying that the attacks may have been orchestrated.

The government involvement argument is shared by technology sector professionals. The computer security company McAfee stated in April 2020: “We believe that the perpetrators may have political motivations and may have some allegiance to the government of the Socialist Republic of Vietnam.” According to the company, a malware began circulating in December 2009. A hacker broke into the California-based Vietnamese Professionals Society’s website and replaced a Vietnamese-language keyboard programme with a malware programme, which then infected the computers of anyone who downloaded it. According to a McAfee study conducted in October 2010, domain names ending in “.com” are the most at risk and at a country level, Vietnam is now the most at risk.

American Internet giant Google has also been accusing Vietnam of carrying out cyberattacks and online surveillance to muzzle critical opinions. It claims that tens of thousands of people may have been affected. The sites targeted are said to be those which discuss the highly controversial issue of the bauxite mining being done by Chinese companies, despite activists exposing them as having a harmful impact on the environment and China’s growing influence in this strategic region. Nart Villeneuve, of Toronto University’s Citizen Lab, stated to Associated Press on 1 April 2010 that these attacks and malware programmes had made it possible to infiltrate and place under surveillance human rights activists’ websites.

UNMOTIVATED ASSAULTS AND PRESSURE OF ALL KINDS: ROGUE METHODS

The pressures exerted on the writers and editors of the online magazine To Quoc tightened in 2010. After being threatened, army officer Dang Van Viet asked for his name to be withdrawn from the editorial board. In early February 2010, Assistant Editor Nguyen Thuong Long and journalist Nguyen Phuong Anh were interrogated by the police. In early March, security agents told the wife and children of retired Colonel Pham Que Duong, To Quoc’s former publisher, that they would have serious problems finding work if they did not get him to stop collaborating with the magazine.

To Quoc’s founder, geologist Nguyen Thanh Giang, was recently summoned, threatened and interrogated several times in a police station. On 23 March 2010, some hoodlums broke into the home of physician Pham Hong Son, who had written articles posted on To Quoc, and threatened to splash urine and excrement in his house if he did not stop writing articles for the magazine.

Now gravely ill, Father Nguyen Van Ly, a Roman Catholic priest who had been arrested in 2007 and later sentenced

to eight years in prison for his writings, was granted an early release in March 2010 and is currently under house arrest. His case will be reexamined mid-March. He has come to symbolize pro-democracy and non-violent protest against Vietnam's single-party regime. In January 2011, public security agents prevented American diplomat Christian Marchant and Australian MP Luke Simpkins from visiting him. Christian Marchant was roughly treated and taken to a police station, which raised an official protest from the U.S. Department of State.

The government is not satisfied with mere pressure tactics. It arrests dissidents, journalists and netizens all the time.

LITANY OF ARRESTS

Arrests are part of a cycle which began in 2007, intensified in 2009, and has been accelerating in the last few months. They have revealed the authorities' increased sensitivity to dissidence during the run-up to the January 2011 Communist Party Congress. Dissidents have been paying a stiff price for the party internal disputes on topics such as the bauxite mining issue and corruption cases, topics disseminated on the Web.

Vietnam is currently the world's second biggest prison for netizens, with seventeen detainees: Nguyen Van Tinh, Nguyen Manh Son, Nguyen Van Tuc, Ngo Quynh, Nguyen Kim Nhan, Phan Thanh Hai, Pham Van Troi, Vu Van Hung, Tran Quoc Hien, Tran Duc Thach, Truong Quoc Huy, Dieu Cay, Nguyen Tien Trung, Nguyen Xuan Nghia, Vi Duc Hoi, Le Cong Dinh and Pham Minh Hoang. In addition, three journalists – Tran Khai Thanh Thuy, Truong Minh Duc and Nguyen Van Ly – are still behind bars.

Blogger Dieu Cay, who should have been released in October 2010 after having served his two and one-half year prison sentence, is in detention, now charged with propaganda against the State and the Party by virtue of Article 88 of the Vietnamese Penal Code. Arrested in April 2008, he had been sentenced in September 2008 to two and one-half years for "tax fraud" by a Ho Chi Minh City Court. The Vietnamese authorities were actually seeking to silence this dissident, who had publicly called for people to boycott the Ho Chi Minh City leg of the Olympic torch relay on the occasion of Beijing's 2008 Olympic Games. The blogger also had been placed under close watch since taking part, in early 2008, in demonstrations against the Chinese policy in the archipelagos of Paracels and Spratley.

Phan Thanh Hai, also known as Anh Ba Saigon, was arrested in October 2010. The police allegedly questioned him in his home and seized three of his computers. According to the blogger's wife, the police stated that her husband – later charged with promoting "propaganda against the State" – had been arrested for spreading false information on his blog, where he had discussed topics such as maritime disputes with China and bauxite mining operations, and had actively supported Vietnamese dissidents.

Franco-Vietnamese blogger Pham Minh Hoang, arrested on 13 August 2010, was officially charged, on 20 September 2010, with "carrying out activities with the intent of overthrowing the government" by virtue of Article 79 of the Penal Code. and for having joined Viet Tan, the banned opposition party. The government accuses him of publishing on his blog (www.pkquoc.multiply.com) thirty opposition articles under the pen name Phan Kien Quoc. He also stands accused of organising an extra-curricular group of some forty students whom police claim he had intended to train to be future Viet Tan members. According to his wife, Le Thi Kieu Oanh, Pham Minh Hoang was arrested because of his opposition to a Chinese company's plans to mine bauxite in central Vietnam's high plateau region.

Netizen Nguyen Tien Trung, a pro-democracy activist, was arrested in his parents' home on 7 July 2009 for violating Article 88 of the Penal Code. He was sentenced to a seven-year prison term in January 2010 for having "attempted to overthrow the government.

Tried together on 20 January 2010, Le Thang Long, Le Cong Dinh and Tran Huynh Duy Thuc: the first two defendants were sentenced to five, and the latter to sixteen years in prison – a judgement which was upheld on appeal on 11 May 2010. Le Cong Dinh, a well-known human rights activist who had penned numerous pro-democracy articles and defended several bloggers and freedom-of-expression activists, was arrested on 13 June 2009. He was also sentenced to three years of house arrest. Le Cong Dinh and Tran Huynh Duy were both charged with "attempting to overthrow the people's government" and with "subversion" under Article 79 of the Vietnamese Penal Code. In January 2010 human rights activist Thang Long was given a seven-year prison sentence and placed under a three-year house arrest.

Cyberdissident Vi Duc Hoi, a former Party official, was sentenced on 26 January 2011 to an eight-year prison term and a five-year house arrest for spreading anti-government propaganda and violating the laws on national security based upon/by virtue of Article 88 of the 1999 Penal Code. His lawyer, Tran Lam, announced that he would appeal. In 2007, he had been expelled from the Party after calling for democratic reforms and posting online comments about topics which the government deemed sensitive, such as expropriations, corruption and multi-party systems. His house had been searched on 7 October 2010. Arrested officially twenty days later, he was facing up to twenty years in prison. Vi Duc Hoi is a member of Bloc 8406, a pro-democratic network.

Nguyen Dan Que, an independent journalist, was arrested in Ho Chi Minh City, in the south of the country, on 28 February for urging the population to "be inspired by the pro-democracy movements in Africa and the Middle East" and to "get rid of the communist dictatorship and to build a new, free, democratic, human and progressive Vietnam." He was released 48 hours later on condition that he would cooperate closely with the authorities.

Le Nguyen Huong Tra, 33, better known under her blog name "Co Gai Do Long," was released on bail in January 2011. However, the blogger remains charged with "defaming a senior Communist Party official" and his family. She is facing a possible seven-year prison term. She had been arrested on 22 October 2010, for having called the son of a political leader a "womaniser." Deputy national criminal police chief Maj. Gen. Cao Minh Nhan stated that the blogger had been released because her "crime had been clarified." The blogger allegedly admitted to having posted defamatory statements. Allegedly, some restrictions have been placed on her movements.

Blogger Vu Quoc Tu and his wife, blogger Trang Dem, were arrested on 1 May 2010 and prevented from leaving the country for their honeymoon. They had both participated in the January 2008 demonstration organised by blogger Dieu Cay in Saigon to oppose the Ho Chi Minh City leg of the Olympic torch relay. Blogger Ta Phong Tan, who was arrested in April 2010, has finally been released.

The goal of these arrests is to prevent certain dissidents from pursuing their activities, and to persuade others to practice self-censorship. Since such measures do not seem to suffice, the regime adopted a new legal framework to control information.

NEW LEGAL AND TECHNICAL RESTRICTIONS

SPYWARE?

In April 2010, the Vietnamese authorities issued "Decision 15," ordering over 4,000 cybercafés and Internet service providers in Hanoi to install a government-supplied software programme which might – like its temporarily suspended Chinese equivalent Green Dam – block access to some websites and set up surveillance of netizen activities.

NEW CYBERCAFÉ RESTRICTIONS

In August 2010, the Vietnamese authorities decided to close, by the end of 2010, all cybercafés located within a 200-metre radius of schools, in an attempt to curb online game addiction and access to "inappropriate content." This measure allegedly concerns over 800 establishments, primarily in Saigon and Hanoi, but its enforcement has been sketchy, primarily due to economic reasons. Moreover, technical measures are expected to be implemented in order to suspend Internet links in all of the capital's cafés from 11:00 p.m. to 6:00 a.m., and all violators will be fined.

A spokesman for the Vietnam Ministry of Foreign Affairs has indicated that the authorities were trying to ensure "security and a healthy/sound use" of the Internet in public places, and rejects any accusation that this constitutes a violation of freedom of expression. The Ministry had recently denounced the growing use of the Internet and of "violent and pornographic" content.

A NEW DECREE TO "REGULATE" JOURNALISTS AND BLOGGERS

In the midst of the Communist Party Congress, the Hanoi government demonstrated its determination to tighten its grip on information by adopting, in January 2011, a new decree regulating journalists' and bloggers' activities. This decree, which was added to one of the world's most repressive legislative arsenals, notably provides for fines of up to 40 million dong (2,000 U.S. dollars), in a country where the average salary consists of about 126 U.S. dollars.

The text, signed by Prime Minister Nguyen Tan Dung, en-

tered into effect in February 2011. The primary targets for sanctions are authors who post information which is either "unauthorised" or "not the interests of the people." By interpreting these vague definitions broadly, the Vietnamese government will have leeway to increase the number of arrests of bloggers and journalists. The decree also provides for fines of up to 3 million dong (155 U.S. dollars) for publishing documents or letters online without revealing their sources or their own identity, and fines of 20 million dong (1,000 U.S. dollars) for publishing any documents connected with an official inquiry.

This decree attempts to apply to blogs the censorship already in force with the traditional media. It also seriously threatens the protection and confidentiality of information sources. The government is targeting online anonymity by trying to prevent bloggers from using pseudonyms, which could make it easier for the authorities to harass them, as well as to arrest and jail them.

HUMAN RIGHTS: NON-ESSENTIAL?

Crackdowns tend to intensify before each Congress and then relax somewhat. This time, repression was particularly harsh and the latest legal measures taken by the government bode ill for the future. The Communist Party seems to be pursuing a policy of economic openness while maintaining an iron grip on the country's political and social life.

Last year, Vietnam concluded its term as rotating Chair of the Association of Southeast Asian Nations (ASEAN). Under its presidency, the Human Rights Committee was never called into action.

Even though, in July 2010, U.S. Secretary of State Hillary Clinton said that she was "concerned" by the human rights situation in Vietnam, the human rights dialogue between the United States and Vietnam provided an opportunity to denounce multiple violations of freedom of expression and despite international criticism, Hanoi's attitude has not softened. Priority is being given to the domestic political situation and to maintaining control. Stability is the key focus

The control measures taken by the authorities translate the regime's concern over growing number of cybernauts who openly express their views online and use the Net as a means to compensate for the lack of freedom of expression in Vietnamese society. In growing numbers, they are demanding the right to express their opinions without being harassed by public security officers. Out of a sense of solidarity, Vietnamese bloggers chose the day when Dieu Cay was expected to be released from prison, 19 October 2010, to set up a non-official "Blogger Day". They circulated an open letter so that everyone could pressure authorities to demand the release of all jailed bloggers and the end of Internet surveillance and censorship.

AUSTRALIA

UNDER SURVEILLANCE

Domain name: .au
Population: 22,551,660
Internet-users: 17,033,826
Average annual salary: $28,290
Netizens in prison: 0

The government has not abandoned its dangerous plan to filter online traffic, even though this will be hard to get parliamentary approval.

A HARSH FILTERING SYSTEM

After a year of tests in cooperation with Australian Internet service providers, telecommunications minister Stephen Conroy said in December 2009 the government would seek parliamentary approval for mandatory filtering of "inappropriate" websites. Blocking access to a website would BE authorised not by a court but by a government agency, the Australian Communications and Media Authority (ACMA).

The ACMA is already empowered to issue "take down" notices to Internet Service Providers under the Broadcasting Services Act of 1992. It maintains a "blacklist" of banned sites without transparent processes or criteria for the bans. (See http://www.smh.com.au/articles/2009/03/19/1237054961100.html).

The filtering would target websites with "refused classification" (RC) content, a category already applied to mainstream media, and would therefore apply to content unrelated to government efforts to combat child pornography, defamation or copyright, so creating a risk of overblocking. Topics such as aborigines, abortion, anorexia, or laws about the sale of marijuana might all be filtered, along with media reports or related medical information. The government says filtering would be 100% effective – a claim disputed by experts – but Wikileaks has revealed that the blacklist includes harmless sites such as YouTube links, poker games, gay networks, Wikipedia pages and Christian sites.

Several examples of censorship have appeared. Pages of Wikileaks content on the SBS (Special Broadcasting Service) news site were reportedly blocked, leading to a demonstration in Sydney by supporters of the Pirate Party (http://www.sbs.com.au/news/article/1227392/%27Pirates%27-protest-Internet-blacklist)

All the country's main ISPs (Telstra, Optus and Primus) are thought to have formally agreed to instal voluntary filters from July 2011. The government still hopes to introduce mandatory filtering, with the support of independent and Green members of parliament, but it does not yet have such backing.

AN UNPOPULAR BILL

Journalist Ben Grubb, of The Age newspaper, said in July 2010 the government censored 90% of an official account of a meeting about censorship with ISPs and business

figures in March that year before releasing it to the media. Australian law allows full access to all government documents. Claudia Hernandez, of the attorney-general's office, said releasing an uncensored version could have set off "premature unnecessary debate." Deputy senate opposition leader George Brandis said the episode showed how "truly Orwellian" the government had become.

Minister Conroy has made debate very difficult by calling his critics child pornography advocates. A Fairfax Media poll of 20,000 Australians in December 2009 showed 96% strongly opposed to the bill. Internet firms, including Google and Yahoo, are against the measure and the U.S. government said in March 2010 it was concerned about the proposal, noting the importance of freedom of expression. Hundreds of Australian websites protested against the bill in a national "Internet Blackout" day in January 2010.

BAHRAIN

UNDER SURVEILLANCE

Domain name: .bh
Population: 738,004
Number of Internet users: 49,300 Internet users as of June
Average monthly salary: Women: USD 10,496; Men: USD 29,796
Average cost of a one-hour cybercafé connection:
Number of imprisoned netizens: 0

In the last two years, Bahrain authorities had resolved to set up a targeted filtering system and to arrest netizens on the pretext of fighting terrorism and maintaining national stability. Since early 2011, while democratic demands and popular protest movements have been rocking the Arab world, their strategy has been vacillating between intensifying censorship of the political opposition and concessions in the form of released prisoners.

AN INGRAINED TARGETED FILTERING SYSTEM

The authorities' efforts to pursue technological innovations has gone hand-in-hand with a tightening of Internet control. A strict filtering policy governs Internet use, focused on contents related to political or religious issues, or which are deemed to be obscene or capable of tarnishing the royal family's reputation. Among the sites blocked are opposition websites and those considered "anti-Islamic," discussion forums on taboo subjects and certain news websites. Online news websites such as www.ezaonline.com, and various forums such as Sitra www.sitraisland.net and Bharainonline.org have been made inaccessible.

In early 2009, Sheikha Mai Bent Mohammed Al-Khalifa, Bahrain's Minister of Culture and a member of the royal family, launched a "anti-pornography campaign" which led to the closing of 1,040 websites, even though some of them had nothing to do with the subject. The blocking of the Arabic Network for Human Rights Information (ANHRI) and of the Bahrain Centre for Human Rights betrays the government's intention of attacking sites critical of the regime, the royal family or the Parliament. Some YouTube, Wikipedia and Facebook pages have been adversely affected by this campaign.

This selective filtering policy also applies to social networks, particularly when they discuss topics deemed controversial. On 9 October 2010, for example, the Facebook page of opposition leader Abdul Wahab Hussein was blocked. Facebook currently has 253,000 members in Bahrain.

However, the use of proxy servers such as Hotspot Shield and Your Freedom, is increasingly common in the kingdom.

A NEWS-REACTIVE INTERNET CENSORSHIP

The government reacts swiftly to breaking news. Following the pro-democratic demonstrations which began on 14 February 2011 in Manama, the country's capital, filtering was intensified thanks to software supplied by the U.S. company SmartFilter.

The authorities resorted to blocking the accounts of Bambuser, a streaming platform which allows users to directly share online videos made with cell phones. YouTube pages containing videos of the protests were rendered inaccessible. One Facebook group of 6,000 members which had called for a demonstration against the regime on 14 February was censored by the authorities two days after the page was opened. The Twitter account @Nabeelrajab, which belongs to the President of the Bahrain Human Rights Centre, was among those censored.

Furthermore, high-speed Internet connections have been slowed down since 14 February, undoubtedly to hinder the uploading and downloading of videos and the dissemination of live photos of the demonstrations. According to the company Arbor Networks, Internet traffic to and from Bahrain in mid-February fell 20%, as compared to the three preceding weeks.

On 14 February 2011, King Hamad ben Issa Al-Khalifa made a televised speech to express his condolences to the families of the two demonstrators killed while crowds were being dispersed, and ordered an commission of inquiry to be set up. According to the Bahrain Youth Society for Human Rights, some anonymous SMS messages were sent which called for pro-government demonstrations.

CELL PHONES UNDER PRESSURE

In 2010, the repression spread to cell phones. On 7 April 2010, the Ministry of Culture and Information banned a Blackberry cell phone chat group and threatened the offenders with legal action. Mohamed Suleiman, a journalist who was relaying via his "Urgent News" application free daily news briefs from six of the country's leading dailies, was forced to stop transmitting these news alerts. The Assistant Underscretary of Press and Publications, Abdullah Yateem, justified this ban by pointing out that certain newspapers and telephone messaging services had not been approved by the authorities. He expressed concern about the impact on the public that such news might have and the "chaos and confusion" it could cause among readers.

These chat groups are very popular in Bahrain. They allow users to exchange various types of information such as traffic updates, the presence of police speed traps (radar), cultural exhibits, religious information, etc. Eleven thousand people were receiving "Urgent News" alerts.

EXCESSIVE LAWS AND DECREES

Numerous cybercafés are under tightened surveillance and are prohibited from having a separate closed room that could allow Internet users to privately consult websites. In fact, each screen must be visible to all in order to make surveillance easier. This control is coordinated by a commission comprised of four ministries, which monitors compliance with the rules governing the non-admittance of minors and computer station visibility.

The Internet is governed by the Telecommunications Regulatory Authority (TRA), established by Legislative Decreee No 48 of 2002 promulgating the TelecommunicationsLaw. Its scope of application was extended to online media. Although a 2008 amendment eliminated prior censorship and prison sentences for reporters, journalists and netizens can still be prosecuted by virtue of the anti-terrorism law or the Bahrain Penal Code.

Two decrees that specifically concern the Internet were adopted in 2009. The first allows websites to be closed without a court order, merely at the request of the Minister of Culture. The second requires the growing number of Internet service providers – currently about 20 – to block pornographic websites or those likely to incite violence or racial hatred.

NETIZENS UNDER PRESSURE

Committed to a security-based approach in reaction to the Shiite minority protests in the summer of 2010, the regime detained two bloggers under inhuman and degrading conditions and openly flouted their rights, in violation of international agreements signed and ratified by the Kingdom.

Judged alongside some 20 other human rights activists, bloggers Ali Abdulemam and Abduljalil Al-Singace, who had been arrested on 4 September 2010, were harshly treated while in jail. According to the Bahrain Centre for Human Rights, blogger Ali Abduleman allegedly stated during the trial: "I ws tortured, beaten and insulted. They threatened to get my wife and other members of my family fired from their jobs. I was questioned without a lawyer present and the officer there with me looked as though he were a security agent. He ignored my denial of the accusations made against me. He never let me answer his questions and answered them himself." When he appeared before the court, Abdeljalil Al-Singace protested against the "moral and physical torture" to which he had been subjected and the threats of rape made against his relatives. He suffered four heart attacks while in custody. Allegedly, he also pointed out that he was deprived of medical care by the guards and that, despite his rapidly deteriorating health, he was never given any medication.

On 22 February 2011, as a gesture to appease the opposition and demonstrators, the authorities suddenly released th two bloggers as well as 21 other opposition and human rights activists who had been on trial at the same time, after multiple hearings and a trial parody marked by the collective resignation of the initial defence lawyers. The latter had demanded that the trial be suspended and an investigation started into the torture allegations, as provided by law. Nabeel Rajab, Director of the Bahrain Centre for Human Rights, stated on U.S. TV channel CNN that some 400 prisoners were still behind bars.

Abdeljalil Al-Singace, spokesperson and head of the human rights office of the Haq movement of Civil Liberties and Democracy, had already been arrested in 2009 for allegedly launching a government-targeted estabilisation campaign. On his blog, http://alsingace.katib.org, he denounced the anti-Shiite discriminations, as well as the deplorable status of public freedoms in his country. Ali Abdulemam, a very active blogger considered by Bahraini netizens as an Internet pioneer, had been arrested in 2005 for posting criticisms of the regime on his blog. As a contributor to the blogger worldwide network Global Voices, he has spoken in numerous international conferences to denounce human rights abuses in Bahrain.

The two netizens were charged with defaming the kingdom's authorities and publishing "false information about Bahrain's internal affairs" with the aim of destabilising the country.

Mohammad Al-Rashid was also victimised as a result of the government's repressive policy. The netizen was arrested in October 2010 for "spreading false information with the aim of undermining public security." On 4 January 2011, he was released after posting bail in the amount of USD 530. He is now restricted in his displacements and his trial is still underway. According to the Bahrain Centre for Human Rights, this cyberdissident was known for denouncing – mainly on online forums and websites such as Bahrain Online and AlJazeera Talk – human rights violations in the country and the lack of professionalism of journalists with close ties to the regime. He acted as a relayer of opposition views often omitted in the traditional media.

Defenders of netizens and human rights activists have not been spared. Nabeel Rajab was denied entry into the courtroom when the bloggers' third hearing began. On 2 December 2010, already the victim of obvious harassment, the human rights activist was questioned for over an hour by national security agents in the Manama airport as he was preparing to board a flight to Greece. Prior to his release, he had been threatened. His personal computer and cell phone were allegedly confiscated and all the personal files and information stored on these devices were copied without a warrant. In the fall of 2010, he had also been the target of a smear campaign in the state-controlled media. He had discovered after reading the newspapers on 5 September 2010 (specifically the Gulf Daily News) that he was considered to be a member of a so-called "sophisticated terrorist network."

Journalist Nicholas Kristof of The New York Times, who did an outstanding job of covering these events, was the target of an online smear campaign most likely spearheaded by the authorities. The regime, which has been brandishing national security as a reason to muzzle dissident opinion in the last few months, has so far shown itself to be pragmatic. The future of the Internet and freedom of expression in Bahrain therefore depends on how the political situation will evolve and what latitude the regime believes it can afford.

BELARUS

UNDER SURVEILLANCE

Domain name: .by
Population: 9,648,533
Number of Internet users: 4,439,800
Average monthly salary: USD 500
Number of imprisoned netizens: 0

Until now Belarus' sole space for freedom, the Internet, has just been put under a regulatory microscope by the government in the wake of a repressive order which entered into effect in July 2010. The suspicious death of an online journalist has traumatised the profession. In the run-up to the elections, and during the demonstrations following the disputed re-election of Alexander Lukashenko, "Europe's last dictator," civil society has witnessed crackdowns both offline, against demonstrators and journalists, and online, via blockings, cyberattacks and tampering.

SETTING UP AN INTERNET FILTERING SYSTEM

Decree No. 60 issued in February 2010, entitled "On measures for improving use of the national Internet network," entered into effect on 1 July 2010. It establishes extensive control over Internet content and provides a framework for network access. It requires Internet Service Providers (ISPs) to register with the Ministry of Communications and Information and to provide it with technical details on the country's online networks, systems and information resources.

This decree also obliges ISPs to identify all the devices (including computers and mobile phones) which are being used to connect to the Internet. Similarly, all users going online in a cybercafé or using a shared connection (for example, in a condominium) now have to identify themselves, and a record of all online connections must be kept for one year. The aim of this measure is to dissuade citizens from continuing to inform themselves on independent and opposition websites.

The decree also provides for the creation of a Centre of Operations and Analysis (COA) attached to the president's office, whose task it will be to monitor all content before it is put online. This measure clearly institutes censorship at the highest level of government. Any request by this Centre for a website closure will have to be carried out by the ISP concerned within 24 hours. Any protest against a website's closing will need to be referred to a court.

The Ministry of Communications and Information has formulated a new regulation, effective as of 1 July, setting up a filtering system for controlling access to websites considered dangerous, including "extremist" sites, those linked with trafficking in arms, drugs, or human beings, and those which are pornographic or incite violence. Sites deemed as such will be banned by order of the Ministry of

Communications and Information, the Committee for State Control, or the COA and will be rendered inaccessible from government organisations, state-owned companies and cybercafés. They could also be blocked from other Internet users by ISPs, which had until 1 September to procure the equipment needed to carry out the regulations.

INCREASED PRESSURE ON THE MEDIA DURING THE RUN-UP TO THE PRESIDENTIAL ELECTION

Intimidation campaigns against journalists and dissidents intensified during the run-up to the 2010 presidential election.

WEBSITE BLOCKINGS AND HARASSMENT FOLLOW THE ENTRY INTO FORCE OF DECREE NO. 60

On 6 July 2010, the Vitebsky Kuryer newspaper's website (www.kurier.vitebsk.by) was blocked by the Beltelecom national telecommunications operator, which controls bandwidth. The website, not registered with the authorities for ideological reasons, has now been blocked under Decree No. 60, and has had to migrate to another platform with the URL http://vitebsk-kurier.info/.

A news website based in the town of Vileika, vilejka.org, was blocked for several days as the result of a police investigation into comments posted by cybernauts. On 1 July, the police questioned one of the site's users, Mikalai Susla, and confiscated his computer because they suspected him to be the site's director. The latter said that the site had been blocked because of unfavourable comments about local and national policies, and that the crackdown was related to the fact that Decree No. 60 had just come into effect.

Natalia Radzina, chief editor of the opposition website charter97.org was again interrogated by police in Minsk on 1 July 2010 in connection with litigation over a comment made on her website. This was her fourth interrogation in four months.

On 23 June 2010, nine activist members of the Nazbol (National Bolshevik Party) staged an unauthorised demonstration on Freedom Square in Minsk, waving placards and wearing T-shirts with the words "Internet Freedom." They were arrested and found guilty of "violating procedure for holding demonstrations." Their leader, Yawhen Kontush, was fined 875,000 Belarus roubles (about USD 324). The other participants were each sentenced to pay a fine of 175,000 roubles (about USD 65).

JOURNALISTS' PERSONAL DATA IN JEOPARDY

In April 2010, a senior police officer authorised police computer experts to access the e-mail accounts and Skype instant messages of several independent journalists whose computers had been seized during raids of their media offices and homes on 16 March. This happened as a result of defamation suits which a former KGB official, Ivan Korzh, brought against relatives of police officers arrested in connection with a case involving allegedly illegal hunting practices.

Natalia Radzina, Svyatlana Kalinkina and Maryna Koktysh of the opposition newspaper Narodnaya Volya, as well as Iryna Khalip of the independent Russian daily Novaïa Gazeta are also concerned.

The authorities' decision to access journalists' e-mails and instant messaging constitutes a serious violation of both these media professionals' communication methods and their privacy. Such practices place the reporters' sources in jeopardy. Belarus authorities are particularly interested in identifying and monitoring contributors to Charter 97's website. Police investigator Alyaksandr Puseu told Natallya Radzina that they had discovered no documents related to the defamation suit in the seized computers, but had found over 3,000 articles containing the keyword diktatura (dictatorship). The journalist was questioned in detail about how the website operates.

In 2009, Ivan Korzh had lodged a complaint in the aim of having an article posted on Charter97.org removed, entitled: "Relatives of arrested policemen complain about dictatorship."

IMPUNITY PROMOTES SELF-CENSORSHIP

On 3 September 2010, Oleg Bebenine, a Charter 97 journalist known for his criticisms of Belarus' leadership, was found hanged in his country house near Minsk, the capital. The official finding of suicide is denied by his close rela-

tives and associates, who believe that it was a politically motivated crime. Journalists covering this case have received death threats.

The Belarusian Association of Journalists (BAJ) – a Reporters Without Borders' partner organisation and a 2004 Sakharov Prize recipient – sent letters to the Minister of Interior and to the public prosecutor calling for an objective and transparent investigation. To date, impunity reigns over this matter, adding to the oppressive climate of intimidation against media professionals and motivating them to resort to self-censorship.

DEMONSTRATIONS AGAINST LUKASHENKO'S RE-ELECTION: ATTEMPTS TO BLOCK INFORMATION

The president of Belarus, who has been in power for 16 years, was officially re-elected as a result of the December 2010 elections, which international observers have labelled "undemocratic."

On 19 December 2010, protest demonstrations were held in Minsk after the announcement of the outgoing President's victory with nearly 80% of the votes. Large gatherings were violently dispersed and over 600 people were arrested, including some 30 journalists.

Pressures also intensified online and on communications via cell phone. Calls made on 19 December around 8:00 p.m. could not get through anywhere in Belarus. A number of opposition and independent news sites were the victims of DdoS attacks which either made them inaccessible or caused them to display pseudo or "counterfeit" websites disseminating false information to which visitors were redirected. Thus, some sites with similar names, but registered with the suffix ".in," appeared in place of charter97.org, as well as Belaruspartisan and Gazetaby, and even the newspaper Nasha Niva.

Blog platforms such as the highly popular LiveJournal experienced operating problems as of 19 December. In the early morning of 20 December, security agents entered the offices of the website charter97.org and several of their members were arrested by the KGB. Editor Natalia Radzina was struck in the head by police on 19 December. Released in late January 2011, she is still under house arrest and is being prosecuted for "participation in mass riots." She may face a prison term of up to 15 years.

CONTINUED REPRISALS AND INTERNATIONAL SOLIDARITY FOR VOICES CRITICAL OF THE REGIME

Repression continued to plague Belarus' society in the weeks following the election protests.

Several unprecedented cases of house arrests, coupled with the posting of security officers at opposition members' homes and strict isolation measures, have been observed. Some of the latter have been barred from Internet access and from watching TV news.

In view of the extent of the protests, the well-known Polish dissident and politician Lech Walesa predicted that Belarusians would use new technologies to follow in the footsteps of Tunisia and relieve President Alexander Lukashenko of his duties.

In the meantime, the international community has been expressing increased solidarity with Belarusian civil society.

Since 2011, the European Union and the United States have imposed new sanctions against Minsk which include asset freezes and refusals to grant visas to the Belarus president and 150 of his close associates.

Estonia, a Balta state renowned for its expertise in the technology sector, stated in January 2011 that it was ready to put its cyber-expertise to work on behalf of the Belarusian opposition to teach them "how to manage their Internet websites and protect them against cyberattacks." The NATO Cyber Security Centre is based in Estonia. The United States is said to have offered to join Estonians in their efforts to aid Belarus.

Human rights activists, who have already demonstrated how innovative they are by their successful online mobilisation efforts, are often skilled users of certain techniques for circumventing censorship and protecting personal data. However, in confronting a regime resolved not to loosen its grip, international assistance may prove to be a valuable asset to Belarusian netizens.

EGYPT

UNDER SURVEILLANCE

Domain name: .eg
Population: 83,082,869
Internet-users: 17,060,000
Average charge for one hour's connection at a cybercafé: about $0.20
Average monthly salary: $50
Netizens in prison: 1

The Internet was not censored under President Hosni Mubarak, but his regime kept a sharp eye on the most critical bloggers and regularly arrested them. At the height of the uprising against the dictatorship, in late January 2011, the authorities first filtered pictures of the repression and then cut off Internet access entirely in a bid to stop the revolt spreading. Journalists were also beaten. Mubarak's fall is a chance to entrench greater freedom of expression, especially online.

LANDMARK RELEASE, PROSECUTIONS AND ARRESTS UNDER MUBARAK'S RULE

RELEASE OF KAREEM AMER

Blogger Kareem Amer was freed on 15 November 2010, ten days after expiry of his three-year term after more than four years in prison. He had been sentenced on 22 February 2007 for supposedly inciting hatred of Islam and insulting President Mubarak. On his blog (www.karam903.blogspot.com) he criticised the government's religious and authoritarian abuses and he was arrested a first time in 2005. He also often wrote about discrimination against women and criticised the Sunni Al-Azhar University where he had studied law. Many support groups were set up around the world, encouraged by the Free Kareem Coalition, to demand his release. Reporters Without Borders awarded him its Cyber-freedom Prize in December 2007.
Prosecution of bloggers and human rights activists

Bloggers and human rights campaigners have been hounded and prosecuted in recent months but the cases were dropped. They included Gamal Eid, head of the Arabic Network for Human Rights Information (ANHRI), Ahmed Seif El Islam Hamad, founder of the Hisham Mubarak Law Centre (HMLC), and bloggers Amr Gharbeia and Wael Abbas.

A NETIZEN TOO INQUISITIVE ABOUT MILITARY MATTERS

Netizen Ahmed Hassan Basiouny was sentenced to six months in prison by a military court on 29 November 2010 for putting secret defence documents and information about the army online. He had created a Facebook page in 2009 called "Enrolment and recruitment in Egypt and answers to questions from young candidates," which

provided information and advice about how to join the army. Basiouny was not involved in any subversive or harmful activity and in fact encouraged people to join up. His conviction showed how far the army was an off-limits topic, whether comment was favourable or critical.

A NETIZEN TOO INQUISITIVE ABOUT MILITARY MATTERS

Netizen Ahmed Hassan Basiouny was sentenced to six months in prison by a military court on 29 November 2010 for putting secret defence documents and information about the army online. He had created a Facebook page in 2009 called "Enrolment and recruitment in Egypt and answers to questions from young candidates," which provided information and advice about how to join the army. Basiouny was not involved in any subversive or harmful activity and in fact encouraged people to join up. His conviction showed how far the army was an off-limits topic, whether comment was favourable or critical.

KHALED SAID, VICTIM AND SYMBOL OF IMPUNITY

Khaled Mohammed Said, a 28-year-old human rights activist, was murdered in Alexandria on 6 June 2010. He was beaten to death in the street after being arrested in a cybercafé by two plainclothes policemen, according to the café's owner. Local human rights organisations said he has posted online a video about police corruption. The authorities claimed he died of a drug overdose. Two policemen, Mahmud Salah Amin and Awad Ismail Suleiman, were arrested and put on trial for killing him, but they escaped from prison in January 2011. The trial was due to resume on 6 March.

Said became a symbol and several thousand people demonstrated for police to be punished for all brutality and violence. The protest was very strong online because of the problems of demonstrating in the street. Wael Ghonim, Google's marketing director for the Middle East and North Africa, who was prominent in anti-government protests in February, admitted he ran a Facebook group called "We Are All Khaled Said," which has nearly 100,000 members (http://www.facebook.com/elshaheeed.co.uk?v=wall).

Some saw the protests about Said as precursors of the Egyptian uprising.

BLOGGERS FIGHT CENSORSHIP OVER ELECTORAL FRAUD

Censorship was increased during the December 2010 parliamentary elections in a bid to conceal the fraud involved. Some websites were blocked for hours at a time, including that of the Muslim Brotherhood (Ikhwan Online) and its online forum Al-Moltaqa (http://www.ikhwan.net/forum/). Seven other sites were intermittently disrupted over 24 hours: www.shahid2010.com/, shababelikhwan.net/ib/index.php, www.sharkiaonline.com/, www.amlalommah.net/, www.nowabikhwan.com/, www.egyptwindow.net/ and www.ikhwanweb.com/.

The authorities, mainly the Information and Decision Support Center (IDSC), which reports to the cabinet, was in charge of this censorship, working with Internet service providers TEDATA, ETISALAT and LINK DSL.

Bloggers were very active during the election, organising networks to gather and put out news. They went to polling stations to watch the voting and take photos and videos. Some who saw fraud were pestered by police and sometimes briefly detained.

THE INTERNET AND BLOGGERS IN THE REVOLUTIONARY FERVOUR

THREATS, FILTERING, AND CUTTING OFF THE INTERNET

When Egyptians took to the streets on 25 and 26 January 2011, inspired by the Tunisian revolution, the authorities did their best to keep the media away to prevent them taking and distributing pictures. They disrupted mobile phone networks at demonstration sites in Cairo on the first day.

Twitter was blocked at the same day, along with the video-streaming site bambuser.com. The hashtag #jan25 (named after the protests) was very active. Facebook has for several years been widely used by Egyptian dissidents and civil society to put out news and mobilise people, especially around the 6 April protest movement. Access to Facebook was blocked intermittently on 26 January, according to ISPs.

Slower connections were also reported, especially to on-

line newspaper sites Al-Badil, Al-Dustour, Al-Masry Al-Youm, Al-Badil and Al-Dustour, which were later blocked. The Al-Masry Al-Youm site was seriously disrupted and was down all of the afternoon of 25 January. These online media outlets played a key part in reporting the events in Tahrir Square.

The bloggers and the demonstrators who became citizen-journalists were very important in covering the protests. They tweeted from Tahrir Square, posted videos on YouTube, and linked up to the Bambuser.com site to report on the situation, including the brutalities of regime supporters who came to the square.

The government, feeling overwhelmed, cut off all Internet access and mobile phone service late on 27 January, with only the small ISP Nour able to continue for a while longer.

But netizens found many ways round the blockage to get the news out. Foreign ISPs offered them modem connections, since fixed phone lines were still working. French ISP French Data Networks gave out a phone number (+33 1 7289-0150) available through a user-name and the password "toto." Sweden's Telecomix offered another number (+46 85 000 999 0) and the password "telecomix."

Google and Twitter joined the battle against censorship by setting up a system of voice tweets. Netizens could call foreign numbers +1 650 419-4196 or +39 0662-207294 or +97 316 199-855 and leave messages that were instantly posted on Twitter followed by the hashtag #egypt.

Internet access was restored on 2 February after being down for five days. The OECD put the country's economic losses resulting from the cut-off at $90m.

At least 75 journalists have been physically attacked and 81 imprisoned since 2 February, according to Reporters Without Borders.

Blogger Asma Mahfouz, who urged Egyptians to take to the streets on 25 January, told BBC TV on 5 February that she got many phone calls from Mubarak supporters threatening to kill her and her family. Blogger Kareem Amer was arrested on 7 February on his way home from a demonstration and was not released until three days later.

New disruptions of mobile phone networks and Internet access from Tahrir Square occurred on 7 February 2011.

AFTER THE REVOLUTION, FREEDOM OF EXPRESSION?

Egypt is preparing for constitutional reforms but the future of the revolution seems uncertain, with tension between the army and the protesters who forced Mubarak out. New clashes occurred in Tahrir Square on 25 February. The army apologised afterwards to the demonstrators, calling them "sons of the revolution" on its Facebook page, perhaps a sign that times have changed.

The heavy filtering at the height of the revolution has reportedly ended.

The Internet in Egypt is in full expansion and people who had never taken part in politics are joining online discussions about the country's future and various causes. They are no longer afraid to speak up.

But some bloggers are still worried about continued action by state security police against former regime opponents and dissidents.

The government and the army must improve online freedom of expression and openly dismantle the Mubarak regime's online spying apparatus and surveillance system. The Egyptian revolution has just begun and bloggers, the standard-bearers of free expression, remain alert.

ERITREA 

UNDER SURVEILLANCE

Domain name: .er
Population: 5,792,984
Number of Internet users: 250,000
Average cost of a one-hour cybercafé connection: about 1 U.S. dollar
Average monthly salary: 92 U.S. dollars
Number of imprisoned netizens: N/A

At a time when many Arab-world dictators are losing their power, Asmara's brutal and repressive regime is eager to prevent any attempt to destabilise the government. It continues to use a variety of tactics – including technical barriers and netizen intimidation – to keep the population from gaining access to the Web and its potential as a protest vehicle.

TECHNICAL BARRIERS

To date, the Internet is the only space in which Eritreans are free to voice their opinions in a country which President Issaias Afeworki rules with an iron hand. The independent press was wiped off the map in 2001. The state-controlled media merely relay the regime's ultra-nationalist ideology.

The government has proven reluctant to accept Internet growth, fearing the Web's potential for disseminating independent information. In this last African country to connect to the Net, in 2000, the penetration rate now hovers around 3.5%, which means that virtually all of the population has been excluded from the digital era.

Telecom operator EriTel, which owns the network's infrastructure, is directly controlled by the government. The Eritrean Ministry of Information granted a licence to the country's four Internet service providers from whom EriTel rents its bandwidth. Since EriTel is under the authorities' orders, network surveillance and slowing down bandwidth speed are easy tasks.

The government has chosen not to increase bandwidth speed – a major technical barrier to connection – which explains why, more than sending e-mails (which can take a very long time) – chat has become the most popular way to communicate. Yahoo Messenger and Facebook's "chat" function are constantly being used in cybercafés, where connection speeds are particularly slow.

In fact, most of the Eritreans who connect to the Web do so from cybercafés, since they cannot access the Internet from their cell phones. To enjoy private access, netizens need to obtain a high-cost special authorisation from the regime.

INTIMIDATION OF NETIZENS: ARRESTS, BLOCKING TACTICS, AND SURVEILLANCE

Although the government has not set up any widespread automatic Internet filtering system, it has not hesitated to order the blocking of several diaspora websites critical of the regime. Access to these sites is blocked by two of the Internet service providers, Erson and Ewan, as are pornographic websites and even YouTube. The latter would require too much bandwidth.

Sometimes surveillance and self-censorship are enough. The two other Internet access providers, Eritel and Tifanus, do not block opposition websites, since they know that the great majority of Eritrean surfers would never dare to openly consult them for fear of being arrested and imprisoned.

The few netizens and webmasters courageous enough to create an independent website, or collaborate in its development, are being threatened and closely monitored. It is commonplace for the authorities to intercept e-mails from individuals whom they consider "suspect."

The forty-odd Internet cafés, most of which mainly operate in Asmara, the capital, and in two or three other Eritrean cities, are constantly closely watched, particularly during periods of social unrest, or when compromising news about the regime is circulating abroad. At least two cybercafés are said to have been closed in 2010 and their owners arrested. The official excuse was that they were used for showing pornography to young netizens.

In January 2011, several Internet users and bloggers were allegedly arrested in cybercafés, most of them in Asmara. Questioning such people has had a dissuasive effect on other Internet users.

PROPAGANDA AND CYBERATTACKS

In the last few years, the government has been waging an anti-Internet smear campaign in the traditional media – over which it has total control – accusing it of being devoted to pornography and media wars and of challenging the country's cultural values and creating security problems.

However, the regime also uses the Internet as a tool to disseminate its propaganda. The two official websites, Shabait.com and Shaebia.com, respectively owned by the Ministry of Information and the country's sole party, the People's Front for Democracy and Justice (PFDJ), disseminate only government propaganda. Online chat sessions are held to defend the authorities' views. Some sites hosted in Europe or the United States relay the same positions, including www.meadna.com, www.eastafro.com, www.ertra.com, www.alenalki.com, and www.biddho.com. The topics are often belligerent, nationalist, anti-West and extremely aggressive towards the regime's critics.

Cyberattacks are regularly launched on sites based abroad and managed by dissidents, such as www.asmarino.com, www.assenna.com and www.awate.com. It is thought that the government and its supporters are behind these attacks.

RESPONSE TO UPRISINGS IN THE ARAB REGION

The regime is wary of the popular uprisings which have recently shaken the Arab region, particularly in Tunisia and Egypt in late 2010 and in 2011. News about these events has been muzzled by the state-controlled media – the only legal means to circulate updates, while Eritreans have turned to satellite television and international radio broadcasts to keep informed.

The Eritrean National Security Office (NSO) is allegedly examining the option of restricting the population's access to satellite TV channels, which are very popular in the country. In this context, the launching of the terrestrial Channel 2 TV sports and entertainment network, could be seen as a first step towards a gradual ban on satellite dishes, on the pretext that sports and entertainment coverage no longer requires satellite access.

At the first sign of unrests, the regime is prepared to cut off the country from the Internet, as was done in Egypt. In a country as repressive and sealed off from the world as Eritrea, Internet users are not as organised as in Egypt or Tunisia, where netizens are the civil society's vital force. Meanwhile, most online mobilisation efforts are being launched from abroad.

FRANCE

UNDER SURVEILLANCE

Domain name: .fr
Population: 64,768,389
Number of Internet users: 44,625,300
Average monthly salary: USD 1,8245
Number of imprisoned netizens: 0

With the implementation in France of the "three-strikes" legislation and of a law providing for the administrative filtering of the web and the defense of a "civilised" Internet, the impact of recent legislation and government-issued statements about the free flow of online information are raising serious concerns. The year 2010 was difficult for several online media and their journalists targeted for office break-ins and court summons and pressured to identify their sources. For the first time, France has been added to the "Countries Under Surveillance" list.

2010: A CHALLENGING YEAR FOR ONLINE JOURNALISTS AND THEIR SOURCES

In October 2010, break-ins occurred in the offices of several journalists investigating the Woerth-Bettancourt case. The Mediapart news website reported the "disappearance" of computers and hard disks containing information about the heiress to the L'Oréal empire. These thefts, as well as the phone-tapping and undercover methods used by French intelligence agents to track the site's journalists inquiring into the Karachi and Bettancourt cases, are placing the protection of sources principle in serious jeopardy.

In November 2010, Claude Guéant, who was at that time the Elysée General Secretary, lodged a "defamation" suit against Mediapart, which had accused him of being responsible for the undercover surveillance of its journalists. A few weeks earlier, several majority members had verbally harshly criticised Edwy Plenel's website. Then Health Minister Xavier Bertrand labelled the newspapers' methods as "fascist." Nadine Morano, Minister for Apprenticeship and Professional Formation, accused Mediapart of being a "gossip website."

In November 2010, news website Rue89's offices were burgled and more than 20 computers stolen. The offices of news site MyEurop info, located in the same building, were also "visited." Lastly, in June 2010, Augustin Scalbert, a Rue89 journalist, was indicted for "receiving stolen goods" for having published an article accompanying an "off-air" video clip of Nicolas Sarkozy on the France 3 TV network. The video showed the French Head of State reprimanding a studio technician for not responding to his greeting prior to an interview.

The website Bakchich.info is said to have obtained a copy

of a message from a private detective agency addressed to the Elysée about the latter's own spy services. According to Nicolas Beau, the website's director, it supposedly contains "tips on how to most effectively promote the site," for "making it more middle-class and institutionalised," and for turning it into "a source with a pro-government viewpoint."

WIKILEAKS: THE FRENCH DEBATE

The debate over the WikiLeaks website, which released U.S. diplomatic cables to the public via such media as Le Monde and The New York Times, aroused sharp criticism from officials in the French government. In December 2010, Eric Besson, Minister of Industry, Energy and the Digital Economy, tried to prohibit WikiLeaks from being hosted France. The Minister asked the General Council of Industry, Energy and Technology (CGIET) to study what actions could be taken "to ensure that this Internet website will no longer be hosted in France." In a letter addressed to the Council, he justifies himself as follows: France cannot host Internet sites that violate the confidentiality of diplomatic relations and put in danger persons protected by diplomatic secrecy," to which he added, "One cannot host Internet sites described as criminal and rejected by other states because of attacks on their fundamental rights."

On 3 December 2010, in response to these statements, French host server OVH applied for a summary judgement against the ruling, affirming that a minister is not entitled to decide the legality of a website nor its host "location." The court has declared itself incompetent to rule on the matter and has asserted the need for an "open debate."

The French Foreign Ministry stated: "We firmly condemn the deliberate and irresponsible disclosure by the WikiLeaks site of U.S. diplomatic correspondence." The government denounced this "threat to state sovereignty." Former Minister of the Interior Brice Hortefeux had labelled the site's action as "totalitarian."

TROUBLING LAWS FOR INTERNET FREEDOM

HADOPI: THE FIGHT AGAINST ILLEGAL FILE DOWNLOADING (INTERNET PIRACY)

HADOPI, the "Creation and Internet" law, is a "law promoting the distribution and protection of creative works on the Internet" and its aim is to facilitate the fight against illegal downloading by expanding the availability of legally downloadable material and by setting up a "graduated response" system against Internet users who download files containing copyrighted material. Such users receive a first e-mail warning. If they recommit the offence within a six-month period, a registered letter and a second e-mail warning are sent. If the Internet user continues the pirating practices, after the matter is referred to the Public Prosecutor's office by Hadopi's Copyright Protection Commission and a judge's decision is rendered, the user may be penalised by a suspension of his or her connection for a one-month period.

Reporters Without Borders believes that Internet access is a fundamental right and that the recourse of suspending a connection is a violation of the public's freedom to access information. Moreover the law known more precisely by the acronym Hadopi 2, is a complement to the French law concerning the Penal Protection of Literary and Artistic Property on the Internet ("Hadopi 1"), which had been partially censored by the French Constitutional Council. In its 10 June 2009 decision on Hadopi 1, the Council asserted that restricting Internet access is an abuse of freedom of expression: "Taking into account the terms of Article 11 of the Declaration of the Rights of Man and Citizens of 1789: 'The free communication of ideas and opinions is one of the most precious of the rights of man. Every citizen may, accordingly, speak, write, print freely, except that he must answer for abuse of this freedom as determined by law'" [and that] nowadays, in light of the generalised development of the Internet and its importance for participation in democratic life and the expression of ideas and opinions, [such right implies] the online public's freedom to access these communication services." They also stipulated that only a judge can restrict Internet access.

In order to bypass the Council's decision, the French government promulgated the non-censored articles of Hadopi 1, and introduced a complementary text (Hadopi 2) providing for a simplified procedure which enables a

single judge to render a decision without the accused being present and by court order. If the judge should then decide to cut off Internet access, such procedure does not guarantee the rights of the defence: the judge renders his verdict without open debate, upon examining the case and without having to explain the basis of his decision.

The main Hadopi provisions raising concern are the following:

- The judge's intervention does not provide sufficient judicial guarantees

- The Internet user will be presumed guilty and must prove his innocence, reversing the burden of proof

- He shall have no possible recourse against sanctions

- If his Internet connection is hacked and used by a third party to download files, the user will be penalised by having his connection suspended for one month for "characterised negligence in the surveillance of Internet access," and could end up having to pay a fine of about USD 1,900. This provision, which imposes on users the obligation to secure their own networks, does not take into account the diverse levels of the French population's computer knowledge

- If one member of a household engages in illegal downloading activities, the entire household's Internet access will be cut off

- The law is already obsolete: the streaming of file content is not considered.

Quadrature du Net, an advocacy group promoting online freedom, calls Hadopi a would-be "punishing machine" (…) "without any consequence" on culture or its dissemination on the Internet.

In an effort to make the provision more effective, in the night of 1 to 2 February 2011, the French National Assembly adopted an amendment that would allow Hadopi to grant subsidies to the private sector to help Hadopi carry out its mission "of monitoring the licit and illicit use of copyright-protected works online" (Art. L331-13 of the French Intellectual Property Code). This amendment now makes it possible to pay private-sector companies to conduct online surveillance and filtering. Sixty Socialist and Communist Party deputies and as many senators have referred this amendment, which they called a "legislative knight" to the Constitutional Council for a validity ruling. The opposition has denounced the perverse effects of the law, asserting that "the news services of the United States and the United Kingdom have complained to their French counterparts, that the law had contributed to the soaring use of encryption among Internet users, making the fight against terrorism more complicated." The French Law Commission and certain majority deputies also oppose the adoption of this text.

NET FREEDOM: A VICTIM OF THE DEBATE ON SECURITY ISSUES?

The French Parliament enacted the "law on guidelines and programming for the performance of internal security" (Loppsi 2) on Tuesday 8 February 2011, by 171 to 151 votes. Under the pretext of fighting child pornography, Article 4 of the law institutionalises an administrative filtering of the Web, without a court order. Article 2 is likely to criminalise the use of pseudonyms on the Internet, and Article 23 permits cybersearches.

Loppsi 2 poses a critical threat to freedom of expression, because it provides the option of censuring content deemed suspect by implementing an administrative filtering of the web. Yet filtering often results in over-blocking, which can drag into its net websites or pages whose content has nothing to do with that which is covered by the law, as well as slow down bandwidth speed.

Article 4 provides for the blocking of websites containing "pornographic photos or representations of minors" by Internet service providers. A "black list" drawn up by the Central Office for the Fight Against Criminality Connected with Information Technology and Communication, reporting to the Ministry of the Interior, will be delivered to Internet service providers in France so that they can censor the sites concerned. The fight against child pornography is totally legitimate. However, the arbitrary and non-transparent nature of the chosen procedure, which excludes any control by an independent judge, is raising genuine concern.

In addition, there is a real danger that the implementation of a filtering system may be extended to matters totally unrelated to child pornography. Once the "psychological threshold" has been exceeded, the filtering could be extended to include other offences such as piracy, defamation and insulting the president. The French Association for Internet

Names and Cooperation (AFNI) shares this fear that the filtering might be extended to other domains than the fight against child pornography.

The effectiveness of filtering technology has already been questioned in numerous reports. A 3 July 2009 "Study on the impact of blocking child pornography websites" commissioned by the French Federation of Telecoms and Electronic Communications claims that such devices do not prevent Internet users who exchange child pornography content from circumventing the filtering system. Reporters Without Borders believes that withdrawal of content at the source by website hosts is a much more targeted and better way to tackle online child pornography.

According to the "Ange Bleu" association, , which combats paedophilia, Loppsi is an "ineffective," counter-productive" and "dangerous" law that uses the pretext of protecting children "as a Trojan horse for generalised online filtering."

Filtering-related precedents, particularly in Australia, have confirmed fears that this practice might become widespread. In February 2011, the United States Department of Homeland Security blocked more than 80,000 websites, including blogs and vendor sites, in an attempt to seize ten domain names suspected of sheltering paedophilia websites. It took three days to straighten out the error. Some countries, including Germany, reversed course and decided to abandon similar projects.

Article 23 of that law, which contains no guarantee of source confidentiality, authorises the police to install remotely-introduced spyware in the suspects' computers under an investigating judge's supervision. In the course of their investigation, should the authorities discover an offence totally unrelated to the purpose of the spyware installation, the suspects could still be prosecuted for that offence.

Article 2 of the proposed law would make identify theft punishable by a fine of up to about USD 20,800 and a prison sentence, and would criminalise the online use of pseudonyms or the creation of satirical profiles of known people.

On 15 February 2011, Social and Communist groups in the National Assembly and Senate challenged the constitutionality of the Loppsi 2 domestic security law before the Constitutional Court. The deputies and senators mainly took issue with Article 4. They argue that the text "does not provide sufficient guarantees against the possibility of arbitrary violations of freedom of expression."

GOOD RESOLUTIONS FOR 2011?

A "FRENCH NATIONAL COUNCIL OF DIGITAL TECHNOLOGY" AND HADOPI 3: A SEDUCTIVE APPROACH

The government has clearly indicated its desire to "spruce up" the image of an unpopular law. During a meeting at the Elysée on 16 December 2010 organised by the President of the French Republic to which Internet personalities, entrepreneurs and influential bloggers were invited, Nicolas Sarkozy is thought to have suggested creating a "Hadopi 3" in order to make the law "more appealing."

The Head of State also allegedly expressed his wish to create a French National Council of Digital Technology (CNN), which would have only an advisory status and would be consulted with regard to any legislation related to digital technology or the Internet. Its apparent objective would be to improve the dialogue between politicians, the Internet sector, and the new technologies. In a report obtained by Agence France-Presse on 25 February 2011, Pierre Kosciusko-Morizet, whom the French government appointed to spearhead consultations in the aim of setting up the Council, explained that the CNN must "address one of the criticisms issued by the digital sector: the impression of a lack of recognition of the sector's influence," that it "must have a forward-looking role in helping to define the digital policy" of France and advise the authorities "as far upstream as possible" about "any proposed legislation." The Loppsi and Hadopi laws are given as "examples in which digital economy actors were opposed, often vigorously so, to a public policy initiated by the government or parliament." The report's author recommends that members of the CNN be elected and that the Council be funded by the state and attached to the Office of the Prime Minister.

NET NEUTRALITY IN JEOPARDY

On Tuesday 8 February 2011, in a speech on the digital economy given during parliamentary meetings, Eric Besson cast doubt on the future of Net neutrality. Under the pretext of a likely increase in Internet traffic, the Minister called for that traffic to be regulated and for abandoning the Net's absolute neutrality principle. He stated that he wanted content providers to pay for access, arguing that "absolute neutrality would impede the growth of services and undermine the objective that it seeks to pursue." He added that this "neutrality absolutism would mean the end

of certain types of services, such as IP telephony or IP television. These statements are inconsistent with the report submitted by deputies Laure de La Raudière (UMP) and Corinne Erhel (PS), whose initiative Eric Besson "had welcomed."

In April 2008, Eric Besson, then Secretary of State for the Digital Economy, nonetheless had declared: "Clearly, I will not be the Minister of Internet castration."

The bill introduced by Socialist deputy Christian Paul, which called for "making Net neutrality a principle and not the exception" and "prohibiting discriminations associated with content, or with those who send or receive digital data exchanges," was defeated by one vote in the French National Assembly on 1 March 2011. The government had issued an unfavourable opinion on the full text.

Reporters Without Borders regrets that this proposed law guaranteeing Net neutrality and providing a framework for the filtering system introduced by Loppsi, was apparently not adopted.

Christian Paul's bill also proposed to reinstate court competency on the Net filtering issue, institutionalised without judicial approval under Article 4 of Loppsi 2.

FRANCE'S ROLE IN PROMOTING ONLINE FREEDOM OF EXPRESSION

An international conference on online freedom of expression initiated by Bernard Kouchner, then French Minister of Foreign Affairs, in partnership with his Dutch counterpart, has suspended his meetings, which have not resumed since the ministerial reshuffling in France and the Netherlands. The latest meeting, initially scheduled for 15 October 2010, was postponed until an undetermined date. This postponement followed arduous negotiations between the various States involved about the content of this conference's final statement and the very definition of online freedom of expression. Some countries apparently had reservations about the "hadopising" nature of this statement.

In addition, a few days before the conference, the Quadrature du Net had published a letter to the Head of State addressed to Bernard Kouchner and containing some recommendations on the conference content. Nicolas Sarkozy asked his Minister to ensure the promotion of a "civilised Internet" and to make this conference "an occasion to promote balanced regulation initiatives taken by France during the past three years, especially the Hadopi law in the field of copyright.".

In a 2007 speech, Nicolas Sarkozy had already asserted that "France (should) reclaim its position as a leading country in the campaign to civilise the new networks."

In December 2010, President Nicolas Sarkozy stated that he was planning to assemble the main Internet actors within the framework of the G8 meeting in Deauville, scheduled for May 2011. Rather than directly tackle the online freedom of expression issue, the debates of the upcoming G8 and G20 meetings will focus on the challenges posed by issues relating to copyrights.

The French government apparently favours a security-oriented approach as it relates to copyright protection, to the detriment of freedom of expression and information access. The time when Hillary Clinton's speech called for Net freedom to be the cornerstone of U.S. diplomacy still inspired emulation in the French Foreign Office already seems to have been forgotten. France has missed an opportunity to take a position of leadership in a debate that has become even more crucial since the Arab world's recent uprisings in which the Internet and social networks played a major role. Tunisian and Egyptian netizens, however, have successfully shown how truly essential online freedom of expression has become.

LIBYA

UNDER SURVEILLANCE

Domain name: .ly
Population: 6,324,357
Internet-users: 323,000
Average monthly salary: $200
Netizens in prison: undetermined

Col Muammar Gaddafi has launched a fierce attack on the Internet as the country teeters on the brink of civil war. The mainstream media have long been under his control and now the regime is trying to completely stifle the news in a bid to crush the revolt and the reporting of its repression.

PROGRESS BEGUN IN 2007 REVERSED SINCE 2010

The regime began to increase civil liberties in 2007 but they are now shrinking. Oea and Quryana, the first privately-owned newspapers founded then by Gaddafi's son Seif Al-Islam's firm Al-Ghad, have been closed.

Foreign-based independent news websites such as Libya Al-Youm, Al-Manara, Jeel Libya, Akhbar Libya, Libya Al-Mustakbal and Libya Watanna were blocked inside Libya on 24 January. Access to YouTube has been blocked since videos were posted there of protests in Benghazi by families of inmates killed in Abu Salim prison in 1996, as well as pictures of Gaddafi's family at parties, according to Human Rights Watch.

The authorities have hounded journalists critical of the regime, especially when the criticism was posted online. Two of them, news website contributors Atef Al-Atrash and Khalid Mohair, were arrested in July last year for reporting administrative and financial corruption. The same day, journalist Mohamed Suraiti was questioned by the Benghazi prosecutor for posting on Al-Jazeera Online and elsewhere news of sexual harassment at a clinic in the city.

STIFLING DISSENT AT ALL COST

From the start of the uprisings in Tunisia and then Egypt, Col Gaddafi understood the dangers of them spreading to Libya. Calls for demonstrations in Libya were made on Facebook as the overthrow of the Tunisian and Egyptian dictators became known there and access to social network sites has been very erratic since mid-February.

Writer and political commentator Jamal al-Hajji, who called online for peaceful protests for freedom in Libya, was arrested on 1 February by plainclothes state security police, according to Amnesty International.

When the Libyan uprising began on 16 February, state security police picked up the director of local news site Irasa, Taqi Al-Din Al-Chalawi, and its editor, Abdel Fattah Bourwaq, according to the daily paper Libya Al-Youm. The same day, blogger Mohammed Al-Ashim Masmari

was arrested and his computer seized after he reported on the demonstrations for several Arabic-language satellite TV stations, including the BBC and Al-Jazeera.

Al-Jazeera has been officially excluded from the cable TV network but can still be received by satellite. To combat the unrest, regime media launched a campaign against those who it said were "cheapening the blood of martyrs," according to the Arabic-language news site Shaffaf. The authorities also prevented journalists moving freely around the country.

The international media were virtually absent from the country and at the start the new media played a key part in the protests as the only ones able to report what happened and the regime's brutal reaction. For several days, amateur videos posted online were the only pictures available before foreign journalists managed to get into the country.

The regime seriously disrupted the Internet, slowing it down or cutting it off completely, to restrict the posting of compromising photos and videos and prevent protesters organising online. It has been cut off completely several times since 18 February, according to the Internet security firms Arbor Networks and Renesys. Traffic has resumed afterwards but Internet has been disconnected again since the evening of 3 March. The leading Internet Service Provider, whose owner is none other than Mohamed Gaddafi, one of Muammar Gaddafi's sons, cooperated to the regime's demands. All fixed and mobile phone lines were cut off on 21 February and remain very unreliable.

The regime is meanwhile trying to use new technology to get its voice heard and to rally support. It sent out text-messages urging people not to demonstrate, though sometimes with contradictions. British teacher William Bauer, who was repatriated from Benghazi, told the French news site Rue89 that the telecoms operator Al-Madar sent a text-message on 21 February saying that nothing was happening in Libya, but that protesters were drugged.

NETIZENS RESPOND

Libyan Internet-users have tweeted their revolution and tried their best to get out news of the regime's abuses and its use of mercenaries.

At the beginning, when the flow of refugees was not very big, some netizens crossed into Egypt to post online videos and photos taken with mobile phones. Others tweeted news about the supply convoys arriving in the country.

The activist hacker group Anonymous provided Libyan netizens with tools to get round the censorship and some of its members reportedly managed to set up illegal parallel networks. The group also helped people to pass on photos and videos. "We want to tell the world about the horror in Libya," one member told the French weekly Nouvel Observateur. "We're passing on pictures of burned and mutilated bodies. It's a bloodbath. Tripoli is a slaughterhouse."

The outcome of the Libyan crisis is increasingly uncertain, with the regime apparently ready to use unlimited violence against the rebels. The United Nations has denounced its actions as "crimes against humanity." The attempts to stifle news and disrupt the Internet may give the regime a chance to crush the uprising ferociously and in secret.

MALAYSIA

UNDER SURVEILLANCE

Domain name: .my
Population: 28 250 000
Number of Internet users: 16 902 600
Average monthly salary: between $850 and $900
Number of imprisoned netizens: 0

While the role of the Internet and of the new media is expanding, the opposition press is being subjected to censorship, and the government is attempting to prepare the media landscape for the approaching elections. In view of the proposed cyber sedition law, and the fact that bloggers and critics are still under pressure, social networks seem to be the most effective cure for any impulse to practice self-censorship and the best stage for much-needed debates which the traditional media cannot cover.

NEW MEDIA, NEW POLITICAL SCENE

News sites and blogs have flourished as an alternative to the state-controlled traditional media. The new media have earned genuine credibility. High-quality online journalism has emerged which is tackling crucial topics on websites such as NutGraph, Malaysian Insider and Malaysiakini, and on blogs like Articulations, Zorro Unmasked, People's Parliament and Malaysia Today.

At the same time, the government decided, in June and July 2010, to limit distribution of the daily Harakah and to suspend the publication of Suara Keadilan, Kabar Era Pakatan and Rocket – four opposition newspapers – by means of the annual publishing permit renewal system.
The authorities seem to be paving the way for media coverage of the upcoming general elections, which may be held in 2011.

The regime's persecution of political caricaturist Zunar seems to confirm the theory that the authorities have taken over the country's political communications. The latter has been charged with "sedition" for having published drawings critical of Malaysia's political and social situation. An obsolete publishing law (the Printing and Publication Act) promotes censorship and bans the circulation of his books, notably his "Cartoon-o-phobia" collection." These caricatures, which are in no way seditious, illustrate with finesse the evils of Malaysian politics and mock the ruling coalition, the Barisan Nasional (BN).

Given the context, the new media have a crucial role to play. The Internet – a relatively free space compared to the traditional media – is an unequalled discussion and debate platform for dissidents and an effective remedy against self-censorship, which dominated the nation a few years ago. The blogosphere is particularly buoyant. In view of the upcoming elections, the social media are an invaluable tool which the political parties need to exploit in order to better reach their constituents, appear more sensitive to their concerns and hear what they have to say.

The opposition was very quick to use these new media, and the government and incumbent party followed suit. By enabling them to reach a heterogeneous audience, the Internet challenges the barriers of traditional censorship. Viewpoints never aired in the press are discussed on the social networks. A ministerial order can event be criticised there, especially when sources within the government leak breaking news. In August 2010, Premesh Chandran, founder of the news website Malaysiakini, told Agence France-Presse that the new media have "changed the way journalists work" and that this "new immediacy hampers government attempts to control the way journalists report a story," since the latter now have access to live reactions from experts and members of the opposition. Often debates started in the Assembly continue in the "Twitterverse." For example, Khairy Jamaluddin, leader of the ruling party's youth wing, swiftly responded to the government's decision to maintain the ban on students joining political parties, labelling it as "gutless and indicative of outdated thinking." An example of successful online mobilisation was the protest launched on Facebook against the construction of a 100-story tower, which recently had a positive outcome.

In 1996, within the framework of a campaign promoting its IT sector, the authorities had promised not to censor the Internet. They were launching the Multimedia Super Corridor, a special economic and technological zone – a promise they had repeatedly made to Reporters Without Borders in 2009.

However, rumour has it that the government may have created a group of several hundred bloggers to inject positive pro-regime content online and entice opposition bloggers to commit violations or give out false news. Their aim is supposedly to neutralise netizens critical of the government.

PROTEST AGAINST THE "WHITE TERROR"

On 1 August 2010, two associations held peaceful vigils in several of the country's cities in order to press the authorities to abolish the ISA (Internal Security Act). Suaram, a human rights organisation (www.suaram.net/) and Gerakan Mansuhkan ISA (himpunanmansuhisa.wordpress.com/), a movement specially created to urge the repeal of these draconian laws, organised the peace rally on the occasion of the law's 50th anniversary.
Although violating the Malaysian Constitution and the country's international commitments, the Internal Security Act, nicknamed the "white terror," is an effective political strategy for suppressing any form of opposition. Under Section 8, the police can detain anyone without trial for up to two years based on a ministerial order which can be renewed indefinitely. It was enacted in 1960 to combat a Communist insurrection. This law flouts international human rights standards such as the ban on arbitrary detention and the right to due process and an impartial trial. The authorities abuse the ISA to serve their political ends by pursuing and locking up journalists, bloggers and opposition leaders.

The crackdown on these protests was excessive. Despite their peaceful intentions, demonstrators were chased, beaten and arrested. The police questioned blogger Badrul Hisham Shaharin (chegubard.blogspot.com/); the editor of the civil society organisation SABM's website, Ambrose Poh (http://www.sayaanakbangsamalaysia.net/); Enalini from the association co-organising the protest, SUARAM; Syed from the other co-organiser, GMI; and S. Arutchelvan, Secretary-General of the PSM (Malaysia's Socialist Party) and editor of its publication (http://www.parti-sosialis.org/). They were all released within twelve hours of their initial interrogation.

A cyber sedition bill is said to be under review. Introduced in the Council of Ministers in December 2010, it poses yet another danger to online freedom of expression in Malaysia. The Minister of the Interior supposedly announced that the text would dictate what can be deemed illegal on the Internet and would be based on the extremely repressive 1948 Sedition Act.

The Sedition Act is already very harsh: it punishes incitement to hatred, criticism of the government, promotion of hostility between "races" or social classes, and challenges to the established order or the ruler's sovereign rights and privileges. Anyone found guilty faces up to five years in prison and a fine of 5000 ringgits (1,640 U.S. dollars). Some thirty other laws may also be used to control the media and the Internet, including the ISA, the 1984 Press and Publications Law, the 1998 Communications and Multimedia Act, and the Sedition Act.

BLOGGERS AND NETIZENS UNDER PRESSURE

The case receiving the broadest media coverage is undoubtedly that of blogger Raja Petra Kamarudin, known by the anagramme RPK, host of the Malaysia Today website. He was detained for 56 days under ISA charges, starting on 12 September 2008, but was freed by court order in November that year after his lawyer petitioned for a writ of habeas corpus with a Malsysian High Court. The authorities appealed. Hated by the regime for his repeated allegations of corruption and abuse of authority, he is still facing sedition and defamation charges for suggesting that the Prime Minister and his wife were involved in a murder linked to alleged kickbacks surrounding the purchase of French submarines. Forced then to flee the country, he has been living in exile ever since and is now being sought by Malaysian authorities. In November 2010, the latter announced that RPK was free to return to his homeland, since the two-year charges against him had expired. For now, the blogger is opting to remain in exile until he receives firm government guarantees that he will not be retried, because the authorities could possibly make new accusations against him.

Irwan Abdul Raman, better known as Hassan Skodeng, was charged on 2 September 2010 with having published on 25 March 2010 a satirical article about Tenaga, a state-owned energy firm, on his blog (http://nose4news.wordpress.com/). He is being sued by the Malaysian Communications and Multimedia Commission (MCMC) for his post entitled "TNB to sue WWF over Earth Hour," under Article 233 (1)(a) of the 1998 Communications and Multimedia Act for "improper use of the network by making, creating, soliciting and initiating the transmission of obscene, indecent, false, menacing or offensive in character with malicious intent." He faces up to a one-year prison term and a fine of 50,000 ringgits (16,400 U.S. dollars). In this post, he allegedly announced the false news piece that the national public utility company, Tenaga Nasional Berhad (TNB), Malaysia's main energy provider, allegedly planned to file a lawsuit against the WWF for its Earth Hour demonstration against global warming. The blogger deleted the post but pleaded not guilty. The Malaysian opposition has called the trial "ridiculous."

In 2010, several bloggers were prosecuted, including Khairul Nizam Abd Ghani, who was charged with "insulting royalty." This freelance computer technician had posted on his blog, adukataruna.blogspot.com, comments critical of Sultan Iskandar Ismail of the State of Johor, who died in January 2010. He is facing up to one year in prison and a fine; even though he has apologised and withdrawn the incriminating article from his blog.

Malaysian bloggers are still under strong pressure, and their positions are finding substantial support among Malaysian citizens, who are no longer content with the official version of "the facts." For now, it is the blogs, news websites and social networks which are reporting events in the Arab world, while the traditional media provide minimal coverage. In view of the approaching elections, the arm wrestling between bloggers and the authorities is likely to get tougher.

RUSSIA

UNDER SURVEILLANCE

Domain name: .ru
Population: 141,927,297
Number of Internet users: 59,700,000
Average monthly salary: about 740 dollars
Number of imprisoned netizens: 0

2010 was the year when the Internet galvanised Russian society, exerting its influence on the country's politics and current events despite government efforts to make the Russian Web suit its own purposes. Enhanced collaboration between bloggers, online media and certain traditional media outlets may have a positive impact on the right to information, bucking the trend towards a large-scale erosion of freedoms in Russia.

IS RUSSIA BECOMING MORE "CONNECTED"?

According to a study by the Berkman Center for Internet and Society, most Internet users in Russia are members of an urban and educated population found to be very active online, particularly via social networks and blogs. The still somewhat low penetration rate, estimated at about 37% of the total population, reveals obvious gaps between the cities – which offer abundant opportunities for Internet access – and the country. Authorities have promised new initiatives to bridge the digital divide.

Political leaders, foremost among them President Medvedev, are expanding their presence on the Web. Russia's President, who is already well-known as a blogger, began tweeting in June 2010.

According to RuMetrica, the RuNet space – including Russian-speaking countries and the diaspora – now reaches a total audience of 38 million people, or 40% more than it did last year.

THE BLOGOSPHERE'S CONTRIBUTION TO THE RIGHT TO INFORMATION

Last year also brought the recognition of bloggers as active actors in the dissemination of information.

Russian blogs are said to number 30 million. The Public.ru media observatory claims that the traditional media cited information originating from the blogosphere 6,000 times in 2010: 30 times more than it did five years ago.

Among the key issues which bloggers have tackled – successfully compensating for the absence of coverage by the traditional media – is the fight to preserve the Khimki Forest, on the outskirts of Moscow. Several journalists and bloggers were assaulted and arrested for having presented a version of the facts different from the official one.

The Help Map project, which relies on the Ushahidi collaborative platform, has enabled Russian netizens to warn

firefighters about the spread of forest fires and to grant or offer help to those most affected by this disaster. To date, the website has had more than 200,000 visitors.

REGIONAL FILTERING ATTEMPTS

Russia is not enforcing a website filtering policy like that of China, for example, but its leaders are using more subtle control methods designed not to prevent the transmission of information but to shape it, often by resorting to genuine propaganda and by placing pressure on Internet access providers.

Regional-level attempts to filter the Internet were observed in 2010, when local access providers tried to block certain IP addresses – initiatives less likely to raise a public outcry and which directly affect the target population. While such attempts failed, they may be the first signs of delocalised censorship.

On 16 July, 2010, Judge Anna Eisenberg, presiding over the court of Komsomolsk-on-Amur (Russian Far East), ordered the local access provider RA RTS Rosnet to block access, as of 3 August 2010, to three online libraries: Lib.rus.ec, Thelib.ru and Zhurnal.ru, as well as to YouTube and to Web.archives.org. The latter website keeps copies of old or removed Web pages. YouTube was accused of hosting a nationalist video entitled "Russia for the Russians," which is on the list of extremist content banned by the Russian Ministry of Justice. The four other websites were allegedly hosting copies of Hitler's Mein Kampf. The blocking of YouTube – a first in Russia – was ultimately not enforced.

A similar case occurred in the Republic of Ingushetia in July 2010. A regional court forced a local access provider to block LiveJournal. In August, the Tula region's local telecom operator temporarily blocked access to the independent Internet news website Tulksiye Priyanki.

The list of "extremist" content held by the Ministry of Justice includes close to 500 terms and is constantly growing under the watchful eye of the "E departments" responsible for quashing extremist activities. Article 282 of the Russian Criminal Code defines extremism as "xenophobia" and "incitement of enmity" by relying on a social group, among others. This was the reason invoked by the authorities in closing down the website ingushetiya.ru, the only news portal in the Ingush language reporting on acts of violence in Ingushetia.

The opposition website, 20marta.ru, which focused on the "Day of Wrath" protests, was also shut down for inciting anti-government sentiment.

MORE SUBTLE FORMS OF CONTROL: SUBCONTRACTED SURVEILLANCE AND CONTENT REMOVAL

The Internet in Russia is regulated by the Federal Service for Monitoring Communications, Information Technology and Mass Communications, whose director is appointed by the Prime Minister. With the installation of such software as SORM-2, the government has acquired the necessary tools to carry out, if it so wishes, a form of Internet surveillance. Yet it does not intend to initiate a global surveillance of RuNet. Its "K department" is focusing its surveillance efforts on a few known dissidents and bloggers who are already being watched offline.

Controlling RuNet begins with a notification to remove the content. In order to tighten their grip on cyberspace, Russian authorities increasingly depend upon Internet access providers and the various blog and social network platforms, thus to some extent privatising their surveillance and control. This is all the easier to implement in that popular social networks such as Vkontakte and the LiveJournal blogs platform were bought out by oligarchs with close ties to the Russian leadership.

Following the December 2010 nationalist riots in Moscow triggered by the death of a soccer fan, the Vkontakte.ru social network instructed its 600 moderators to monitor news circulating online and to remove all content likely to "incite hatred." The most popular blog platform, LiveJournal, responded to users' denunciations of abuse, then introduced stricter rules providing for the automatic suspension of blogs discussing the difficult situation of minorities. The blogs of at least three popular political bloggers: pilgrim 67, rakhat aliev and sadalskij were removed.

Internet specialist Evgeny Morozov revealed that the Kremlin asked Yuri Milner, Silicon Valley-based CEO of Digital Sky Technologies and an investor in Russian social networks and in Facebook, to bring together Internet access providers with a view to harmonising their position on ways to manage "illegal" material on the Internet.

In addition, a decision rendered on 15 June 2010 by Russia's Supreme Court made it mandatory for online media to eliminate or edit on their websites comments deemed "inappropriate" within 24 hours of notification, under penalty of losing their media accreditation. Outlawed subjects include inciting hatred, terrorism, pornography, and divulging state secrets. An initial e-mail warning was sent to the Agency for Political News (APN) for posting comments allegedly calling for violence against certain judges.

This new regulation induced these sites' webmasters to come up with creative solutions. They removed spaces reserved for posting comments underneath accompanying articles and replaced them with links to forums hosted on other websites which they control. Netizens can continue to express themselves freely on these other forums.

PROPAGANDA AND MANIPULATION: A NATIONAL RUNET ALTERNATIVE?

After being blacklisted by their peers, the pro-Kremlin blogger group apparently has been losing some of its influence.

Some bloggers also revealed that certain unscrupulous netizens were accepting money to post comments or information promoting a particular cause. Some Kremlin bloggers were caught in the act of trying to corrupt their peers in order to convince them to post links to their websites. Police officers were also caught trying to launch a pro-police campaign. Netizens have been mobilising more and more frequently to resist such manipulation attempts and to achieve Internet transparency.

Cyber attacks have continued, yet it is still difficult to trace them back to the perpetrators. The website of the independent daily Novaya Gazeta was paralysed for a week in late January 2010 after several denial-of-service (DdoS) attacks.

According to the RBC Daily, authorities are in the process of setting up a national search engine which would exclude certain research topics such as pornography or extremism, and whose task would be to focus on government information. A 110 million-dollar budget is thought to have been earmarked for this project – information denied by the Russian Ministry of Telecommunications. The government already owns a share in Yandex, the country's most popular search engine.

BLOGGERS UNDER PRESSURE?

No Russian blogger has been imprisoned these past months.

However, Vladimir Li'yurov, commenter on the online media forum Komi Republic, was given a six-month suspended prison sentence for making anti-Semitic statements – accusations which he denied.

Alexander Sorokin has been the subject of criminal proceedings since August 2010 on charges of f libel against Kemerovo governor Arnan Tuleev. On his blog, Sorokin had compared Russian regional governors to Latin American dictators.

Alexeï Navalny, a young lawyer who has been denoncing on his blog officials' corruption for years, has just created a website Rospil that has been labeled the "Russian WikiLeaks". He exposed a state company's illegal activities while building a pipeline in Siberia. He is now sued by the authorities for financial embezzlements.

More importantly, the well-known blogger Oleg Kachine, read by thousands of Internet users every day, and a journalist with the daily Kommersant, was brutally attacked near his home in Moscow in the night of Friday to Saturday, 5 and 6 November 2010. He had devoted many blogs to opposition movements such as Oborona and NBP and the pro-Kremlin youth movements. He had recently covered the dispute over the Khimki Forest and the iron deadlock between the officials supporting the freeway construction project and the environmentalists opposing it.

The attack on Kachine had an enormous psychological effect on Russian bloggers and sent an unmistakeable message to the blogosphere: everyone shall be held responsible for what he or she writes and may get into serious trouble for it: a sure way of inducing people to practice self-censorship.

This situation is all the more certain since impunity still prevails. Magomed Yevloyev, one of the developers, and the owner, of the Ingush news website http://ingushetiyaru.org, was killed in August 2008 while being held by agents of the autonomous republic's Ministry of the Interior: a crime which so far has gone unpunished.

ONLINE ACTIVISM: A MIRAGE OR A TRUE SUCCESS?

The Internet is also used in Russia as an online mobilisation tool. While anyone can speak out against the abuses perpetrated by those in power, that does not necessarily mean justice will be served. For example, Anatoly Barkov, Vice-President of the Lukoil company, caused a car accident which killed two people. He managed to circumvent the wheels of justice, despite information provided by bloggers and a massive protest on the Web.

However, Global Voices highlighted a few examples of successful online mobilisations:

- The murder of a young woman, Anna Buzilo, was solved thanks to the collaboration of netizens on the drom.ru forum and her murderer was arrested.

- The "Live Barrier" case: a police officer was given a one-year prison term in November 2010 for having stopped some vehicles and forced them to form a barricade during a car chase in pursuit of an alleged criminal.

Denouncing corruption remains one of the bloggers' favourite pastimes. They have drawn citizens' attention to government IT project tenders which have attained astronomical amounts. Some of them were cancelled as a result, thereby avoiding illegal dealings and the waste of public funds, in sums estimated at over one million dollars.

Local elections have shown the capacity of bloggers to denounce instances of fraud and to document them. The Russian blogosphere and online media will probably be tested during the upcoming 2012 presidential elections, despite President Medvedev's statement in May 2010 that Russia is entering an era that will mark a return "from representative democracy to direct democracy to a certain extent with the help of the Internet."

SOUTH KOREA

UNDER SURVEILLANCE

Domain name: .kr
Population: 49,232,844
Number of Internet users: 39,440,000
Average annual salary: USD 1500
Number of imprisoned netizens: 0

South Korea, the world's "most wired" nation, has intensified its censorship of pro-North Korean websites. Determined to maintain public order in a period of political tensions and social unrest, President Lee Myung-bak's government sometimes resorts to excessive methods and a liberticidal legislative arsenal to compel netizens to practice self-censorship.

CENSORSHIP STRENGTHENED IN REACTION TO NORTHERN PROPAGANDA

For several years, South Korea has been practicing selective blocking: it has rendered inaccessible some forty websites which extol the Pyongyang regime, as well as websites which deal in pornography and online betting, or promote suicide. By virtue of the country's National Security Law, any individual who publicly supports North Korea can be charged with "anti-statist" activity and can face up to seven years behind bars. This law also applies to both traditional and online media.

Website blocking is carried out via access providers by order of an administrative authority, the Korean Communications Commission, which is also responsible for Internet surveillance.

Censorship is thought to have greatly increased in 2010. According to the Korea Times, based on figures disseminated by Ahn Hyoung-hwan, a spokesman of the ruling Grand National Party, the police forced Internet website administrators to delete 42,784 pro-North Korean posts in the first six months of 2010, which is one hundred times more than five years ago.

Lastly, in retaliation against North Korea's new online propaganda offensive (see the section on North Korea), the government has blocked a dozen accounts with probable ties to the Pyonygang regime on social networks such as Twitter, Facebook and YouTube, most often under the user name "Uriminzokkiri, which means "our nation" in Korean. This North-linked reinforcement of censorship is not very popular with Internet users, and is only partially effective, since netizens can use circumvention tools. North Korean accounts remain accessible to those who use Twitter via iPhone.

INTERNET CRACKDOWN IN REACTION TO SOCIAL AGITATION AND CRITICISM OF THE AUTHORITIES

South Korea has resumed disseminating propaganda messages by radio following the March 2010 torpedoing of one of its warships, which it blamed on North Korea. Its censorship decisions are motivated by a resolve to prevent its citizens from having access to Northern propaganda.

Moreover, the 2008 demonstrations linked to the scandal over beef imported from the United States were very unsettling for the incumbent leadership. According to the regime, these demonstrations were caused by netizens' calls for action via the famous discussion forum Agora, which has become the authorities' favourite target. In June 2008, President Lee Myung-bak had clearly expressed his distrust of the Internet: "The Internet needs to be a place of trust. The strength of the Internet can be poison instead of medicine if people cannot have faith in it."

EXCESSIVELY HARSH LAWS

Article 7 of the National Security Law prohibits promoting or encouraging anti-statist groups, including North Korea. In paragraph 5 of this Article, any publication in support of the enemy or the mere reprinting of a document on the subject is also prohibited. Article 8 also prohibits any contact or communication with anti-statist groups. Recently the police began to investigate a cybercafé from which pro-North Korean messages had allegedly been posted. The owner was charged with violating the National Security Law.

Article 47 of the Telecommunications Code states that it is illegal to "disseminate false news intended to damage the public interest." The penalty for any violation can mean up to five years in prison. The electoral law was amended in 2004 to prohibit the dissemination via the Internet of defamatory statements about politicians running for office in an election campaign. The Penal Code, notably the provisions against insult and defamation – even when the statements turn out to be true – is also used against Internet users (Article 307).

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

ANONYMITY IN DANGER ?

Yet another regulation calls into question netizen anonymity. Article 44-5 of the above-mentioned Act requires that Internet users register under their real names and that they provide their national ID card number when visiting portals with over 100,000 members. On the other hand, only the users' pseudonyms appear online. YouTube has refused to apply this measure. Consequently, since April 2008, YouTube users who identify themselves as based in Korea cannot upload or download their videos on the website. Since February 2009, one of the country's main portals, Nate, has been requiring surfers to display their real name in order to leave comments online.

ABUSE OF POWER?

South Korean authorities sometimes seem to abuse their powers. On 9 July 2010, prosecutors ordered Prime Minister Chung Un-Chan's offices to be searched. Two years earlier, his agents in charge of ethical matters had investigated and illegally maintained surveillance on a businessman, the director of a small finance company, who had posted online a video criticising the president. The prosecutors seized the computers and other documents of four of the Minister's staff members. The agents in charge of ethical issues regularly investigate government officials suspected of corruption or malevolent acts, but they are not authorised to investigate ordinary citizens.

The authorities use criminalisation of defamation against their critics and do not hesitate to make examples of them. Since June 2008, a dozen Internet users have been briefly arrested and interrogated for having posted online negative comments related to demonstrations against the importing of beef from the United States.

NETIZENS TARGETED

The well-known blogger Minerva, whose real name is Dae-Sung Park, learned at his own expense that the government considers protecting the financial markets more important than defending freedom of speech. Arrested in January 2009 for having criticised the regime's economic policy, he

could have faced up to five years behind bars and a fine of 50 million Won (USD 44,500). He was acquitted on 20 April 2009, the Public Prosecutor having dropped his appeal following a Constitutional Court decision.

The blogger had asked for an inquiry into the constitutionality of the Telecommunications Code, and more specifically Article 47, paragraph 1, which prohibits the dissemination of false news. The Constitutional Court ruled on 28 December 2010 that the Article was in fact illegal, since it relies on "obscure" terms and stipulates excessive penalties. Over 47 people accused of defamation should therefore be cleared of the charges against them.

Minerva may face other problems, however. He is still being threatened and was even assaulted once in November 2010 while giving testimony as a witness in another case. In June 2010, Minerva filed a complaint against four people whom he accused of harassing him.

Despite constant pressure from the authorities, South Korean netizens are among the most active online. As a result of its persistent attacks on websites spreading North Korean propaganda and its draconian surveillance policy, the government is running the risk of alienating the part of the population which desires more openness and views censorship as a sign of the regime's lack of trust in its own citizens, who are scarcely likely to let themselves be influenced by Northern propaganda.

One blogger cited by Daily NK summarises this mindset: "No offence, North Korea, but except for a very small minority, no one believes in its propaganda (…). North Korea needs to realise that propaganda only works in a restricted environment and that this already limited space is gradually shrinking."

SRI LANKA

UNDER SURVEILLANCE

Domain name: .lk
Population: 20,238,000
Number of Internet users: 1,776,200
Average monthly salary: USD 310
Number of imprisoned netizens: 0

Online journalists and media continue to be targeted for violence. Impunity persists, and the regime does not hesitate to use censorship when its efforts to induce self-censorship no longer suffice.

THE CENSORSHIP REFLEX

Some independent news websites – LankaeNews, LankaNewsWeb, InfoLanka and Sri Lanka Guardian – were blocked in January 2010 a few hours before the presidential election results were announced. Since then, they have all been unblocked with the exception of LankaNewsWeb, which the country's main access provider, Sri Lanka Telecom, has rendered inaccessible since 11 July 2009. TamilNet is still blocked, even after the government's military victory over the Tamil Tiger rebels.

In an interview for Reporters Without Borders, LankaNewsWeb editor-in-exile Chandima Withanaarachchi explained that his website focuses on "human rights abuses, corruption and malpractices of political leaders." Despite its having been banned in Sri Lanka one and one-half years ago, the site gets between 3 and 4 million hits per month in Sri Lanka, and 30 to 40 million hits worldwide. In his opinion, "the only glimmer of hope for press freedom in Sri Lanka is preserved through websites." These sites must, however, defend themselves against regular attempts on the part of the government to control them.

ARSON AT LANKAENEWS WEBSITE'S OFFICES

An arson destroyed offices of the online news website LankaeNews in the night of 30 to 31 January 2011 in Malabe, a Colombo suburb. The main building which housed the online newspaper's library and computers was gutted, putting the website out of business. The site is known for being critical of the authorities. The arson method indicates that it had been prepared well in advance. The fire erupted a few days after the publication of an article challenging the testimony given by Gotabaya Rajapakse, the Secretary of Defence and President's brother, during the trial of the former Sri Lankan Army commander, Sarath Fonseka.

A suspect was apprehended in the evening of 31 January. The police reported that he is a member of a gang which works on contract. A second suspect managed to escape while being arrested. Dozens of Sri Lankan journalists paraded through Colombo's streets in support of LankaeNews, and to protest the latest attacks on press freedom, which occur far too often in the country. After receiving threats, the website's editor, Sandaruwan Senadheera, and his family were forced to seek asylum in the United Kingdom last year.

In July 2010, a similar attack was perpetrated by a dozen armed men on the Voice of Asia group's offices. These frequent aggressions, which can range from murder to forced disappearance, have made the country's journalists feel threatened, which is causing them to avoid a certain number of topics and resort to self-censorship.

MORE THAN A YEAR AFTER HIS DISAPPEARANCE, STILL NO NEWS OF CARTOONIST PRAGEETH EKNALIGODA

On 24 January 2010, a Sri Lankan political analyst and cartoonist, Prageeth Eknaligoda, who worked for the news site LankaeNews, went missing in Colombo. One year later, no progress has been made with his case. The investigation has been hampered by a severe lack of resources despite the authorities' initial promises – a situation criticised by his wife, Sandya Ekneligoda – who wrote a letter to both the former and the still-acting Ministers of Information on 13 December 2010.

To mark the solemn one-year anniversary of the journalist's disappearance, Cartooning for Peace and Reporters Without Borders launched an international support campaign on his behalf, collecting cartoons created by a dozen world-renowned cartoonists from around the world.

AN IMPENDING FILTERING SYSTEM: VIGILANCE REQUIRED

In February 2010, the Sunday Times weekly and the news website LankaNewsWeb exposed the authorities' plan to set up – after the elections – an Internet filtering system with the help of Chinese experts, and to make Internet website registration a requirement. Since the public denunciation of that project by the World Bank, which funds the country's Telecommunications Development Programme via the Institutional Development Fund (IDF), the authorities had backed down – but for how long?

Net censorship will not contribute to national unification. The latter can only be achieved by eliminating impunity, particularly for crimes against media professionals who are doing their best to keep their fellow citizens informed.

THAILAND

UNDER SURVEILLANCE

Domain name: .th
Population: 65 493 298
Internet users: 17 486 400
Average cost of a one-hour cybercafé connection: entre 0,5 et 1 dollar
Average monthly salary: 620 dollars
Number of imprisoned netizens: 0

The spring 2010 crisis had a negative impact on online freedom of expression. The state of emergency was marked by an escalation of censorship, while the various factions continue to use the lèse majesté crime against their political opponents, allegedly to protect the King and to ensure the country's stability.

STATE OF EMERGENCY AND CENSORSHIP

A state of emergency was imposed on 7 April and lifted on 22 December 2010, but it was replaced by the Internal Security Act (ISA) which provides Thailand's leaders and the army with the means to censor without having to resort to judicial procedures.

While the state of emergency was being imposed, in many Thai provinces and notably in Bangkok, control was considerably intensified over the media affiliated with, or with close ties to, the "Red Shirt" movement – led by partisans of former Prime Minister Thaksin Shinawatra. A TV network and some radio stations, Internet websites and publications were censored, banned and forcibly shut down or are involved in legal proceedings. Most of these media supported the « Red Shirts » demonstrations and even occasionally called for insurrection, but they also relayed the legitimate demands of a part of the Thai society. Although it is to be the public prosecutor's office is entitled to prosecute media outlets which circulted calls for violence, any sentence brought against a media outlet should have been issued by judicial authorities, which was not the case at the height of the crisis.

Even though the Internet websites of the leading Thai media outlets were not affected by the were not censored, alternative sources suspected of backing the Red Shirts' movement were sometimes rendered inaccessible. The situation differed from one Internet service provider to the next. Official sites such as www.uddthailand.com or www.norporchorusa.com and news sources such as www.http://thaienews.blogspot.com or http://www.thaifreenews2.com were blocked. The website www.nocoup.org, moderated by the Red Shirt activist Sombat Boonngamanong, was closed on the day the state of emergency was declared. Spaces conveying statements by charismatic opposition leaders were specifically targeted, for example the Facebook page of former union leader Somyos Pruksakasemsuk.

The independent news website Prachatai, which supplied first-rate coverage of the events as they unfolded, was also censored and had to change its URL address several times in order to keep its online website active. www.prachatai.com became www.prachatai.net, then www.prachatai.info and most recently www.prachatai2.info. From the moment the crisis began in mid-March 2010, the news site, as well as its page on the social networks Facebook and Twitter, were blocked countless times by the Center for Resolution of Emergency Situation (CRES).

From then on, online censorship reached new heights. An exact figure is difficult to determine, but it is estimated that from 80,000 to 400,000 URLs were blocked in January 2011. According to the iLaw Project report (http://ilaw.or.th/node/632), 74,686 URLs were blocked by court order between July 2007 and July 2010. This number excludes the sites which the Thai police and army blocked without a court order (which is permitted under a state of emergency or the State of Security Act). The situation has scarcely changed since the state of emergency was lifted.

SURVEILLANCE IS BECOMING THE NORM

Under normal circumstances, the Internet is controlled and monitored by the Thai Ministry of Information and Communication Technology, which blocks those sites which it deems offensive, mainly those charged with violating the lèse majesté law. However, since the authorities view this crime as an offence against national security, the army and police force are also implicated.

Informing is also encouraged. Internet users can denounce any site which commits a lèse majesté crime by telephone, simply by calling 1111, the number of the Prime Minister's cabinet, or by accessing these websites: http://123.242.139.201/main.php?filename=index_complaint or http://www.mict.go.th/re_complaint.php.

The Ministry of Justice also created a "Cyber Scouts" unit consisting of volunteers who monitor the Internet and denounce activities which, according to the authorities, should not occur there. The authorities plan to train several hundred Cyber Scouts. See the official Thai-language website: www.justice-cyberscout.org/General/home.aspx.

REVIVAL OF CRIME OF LÈSE MAJESTÉ

King Bhumibol Adulyadej is revered by the population. He is considered as the guarantor of the unity of a country accustomed to changes in government. There are serious concerns about his state of health. During his last public appearance – the first in months – he offered his New Year greetings seated in a wheelchair. The subject is virtually never mentioned in the press: it is practicing self-censorship from fear of being charged with lèse majesté.

It is dangerous, even under normal circumstances, to discuss the King or his family in Thailand. In a period of crisis, the risks are monumental. His image is even more protected than usual. Anyone who dares to malign his reputation will be charged with lèse majesté. Article 112 of the Thailand Penal Code provides for a sentence of from three to fourteen years against "whoever defames, insults or threatens the king, the queen, the heir-apparent or the regent." The most dissuasive aspect is the conviction rate, which is approximately 95%. Most of the time, the defendants prefer to plead guilty, which reduces their sentence, and then request the royal pardon.

On 15 June 2010, the Thai government approved the creation of an agency specialised in cracking down attempts to malign the monarchy's image on the Internet, the Bureau of Prevention and Eradication of Computer Crime. The authorities justified its creation by explaining that "the monarchy is crucial for Thai national security because it is an institution that unifies the entire nation."

This agency has strengthened an already dissuasive legislative arsenal, including the lèse majesté (criminal) law and the 2007 Computer Crimes Act. Internet users will pay a high price because of it.

A DOZEN NETIZENS CAUGHT IN A VICIOUS LEGAL CIRCLE

According to the December 2010 iLaw Project report (http://ilaw.or.th/node/632), 31 cases of lèse majesté have been recorded, eleven of which violated an article of the Computer Crimes Act. A judgement was rendered in four such cases, court proceedings are underway in three others, and twenty-four of them are still in the investigative stage. Sixteen of these cases were instigated by the Ministry of Information and Communication Technology.
In these cases, a dozen Internet users were being pro-

secuted for violating the lèse majesté laws or the Cyber Crimes Act. Among them were Jonathan Head, a British BBC correspondent in Southeast Asia who has since left Thailand, Giles Ji Ungpakorn, a political science professor who has sought asylum in Great Britain and Nat Sattayapornpisut, a blogger. Another case is Praya Pichai, who was prosecuted for offending a foreign Head of State, namely Kim Jong-Il, North Korea's leader. He pleaded guilty and was given a suspended prison sentence. On the other hand, Tasaparn Rattawongsa, a doctor at Thon Buri Hospital; Theeranan Wipuchan, a former UBS Securities executive; Katha Pajajiriyapong, an employee at the KTZ-MICO brokerage house; and Somchets Ittiworakul are all charged under section 14 of the 2007 Computer Crime Act with posting "false information endangering national security." The netizens had explained the steep fall in the Bangkok stock market last October by the poor health of King Bhumibol Adulyadej, who had been hospitalised since September 2009.

The most widely covered lawsuit to date concerns Chiranuch Premchaiporn (nicknamed Jiew), director of the online news website Prachatai, who has been the target of a genuine judicial harassment campaign. Twice charged in two different cases, she risks being given a prison sentence of up to 70 years. First of all, Jiew stands accused of violating the Computer Crimes Act and of having taken too long to remove ten comments about the crime of lèse majesté posted on the website between April and August 2008. By virtue of this law, Internet website owners will henceforth be liable for statements made by visitors to their sites. They must assume the legal consequences in court. Chiranuch Premchaiporn is facing a 20-year prison term. Her trial has been postponed to September 2011.

A second complaint against her was filed on 28 April 2008 by Syunimit Chirasuk, a Khon Kaen province resident, because of comments associated with an interview – published by Prachatai – of Chotisak Onsoong. The latter was charged with lèse majesté for failing to stand when the national anthem was played before the showing of a film in a movie theatre. As the website's director, Chiranuch Premchaipoen is charged with "defaming, insulting and threatening the King and the royal family" (lèse majesté), and of having " made public statements inciting disorder" (Article 112 of the Thai Penal Code).

Internet user Suwicha Thakor, sentenced on 3 April 2009 to 10 years in prison for a "lèse-majesté crime," was pardoned by the King on 28 June 2010. He was accused of having disseminated on the Web photos which the Royal Family deemed "offensive."

Thanthawuthi Thaweewarodom, webmaster of a " red" website, was arrested on lèse majesté charges on 1 April 2010 by virtue of the Computer Crime Act. His verdict should be known on March 16, 2011.

Warawout Tanangkorn (Suchart Nakbangsai), a "red shirt" activist, pled guilty and was sentenced to three years in prison on 24 November 2010. He will ask for a royal pardon.

These multiple prosecutions are also intended to intimidate other Internet users likely to criticise the King and to force them to practice self-censorship. Other netizens have been briefly arrested or interrogated, but their exact number is difficult to determine, because many of those charged are avoiding any publicity for fear of reprisals and the authorities are obliged to open an inquiry whenever a lèse majesté complaint is filed.

Despite the fact that the country is emerging from a serious crisis, the authorities response in the form of an upsurge in the use of censorship, is not a solution likely to favour national reconciliation. An urgent reform of the archaic lèse majesté law and Computer Crimes Act is needed. Only then will journalists and netizens be able to fulfill their role of informing the public, denouncing the authorities' abuses, and discussing the country's future without having a "sword of Damocles" suspended over their heads.

TUNISIA

UNDER SURVEILLANCE

Domain name: .tn
Population: 10,486,339
Internet-users: 3,500,000
Average monthly salary: €310
Average charge for one hour's connection at a cybercafé: between €0.50 and €1
Number of netizens in prison: 0

The country is awakening to Internet freedom after being one of the world's most harshly censored under the rule of President Zine El Abidine Ben Ali, who was overthrown in January. But the national censorship body, nicknamed Ammar 404, has not been completely dismantled.

THE ROLE OF THE SOCIAL NETWORKS IN COVERING "#SIDIBOUZID"

The popular uprising sparked by what happened in Sidi Bouzid exploded at a time when news was totally controlled by the regime.

The government imposed a blackout on all news of protests there that followed the 17 December 2010 self-immolation of unemployed fruit and vegetable seller Mohamed Bouazizi. Police physically attacked journalists who tried to reach the town or spoke to foreign media outlets. For several days, no news of the revolt came out of the deprived region of the country away from the coastal tourism centres and other economic development.

The silence of the mainstream media was broken by social network sites such as Facebook and Twitter and news sites such as Nawaat.org, which were the sources and conveyors of news. The Twitter hashtag #sidibouzid was very popular among users in Tunisia, and then the region and the rest of the world, as international solidarity grew.

Facebook especially was a platform for comments, photos and videos, allowing people to keep up with expanding protest movements in Sidi Bouzid, Kasserine and Thala and see for themselves the police repression and violence. For nearly three weeks, amateurs posting photos and camera-phone images provided the only pictures of what was happening in Tunisia.

The regime realised the importance of Facebook in early January 2011 and stepped up online censorship, trying to curb distribution of photos of the protests and repression, to hide them from an increasingly interested foreign media.

The head of the Agence Tunisienne d'Internet (ATI) said the number of websites blocked by the authorities doubled in just a few weeks. More than 100 Facebook pages about the Sidi Bouzid events were blocked, along with online

articles about the unrest in foreign media, including France24, Al-Jazeera, the BBC and Deutsche Welle. Photos and videos could no longer be downloaded on Facebook inside Tunisia. The best-known video and photo sharing sites such as Flickr, YouTube, Dailymotion and Vimeo, had already been blocked for months. Police also hacked into Facebook accounts to steal activists' passwords and infiltrate networks of citizen-journalists that had grown up around the Sidi Bouzid events. Many e-mailboxes were broken into. Four bloggers were arrested on 6 January.

A trial of strength developed between Ammar 404 and the country's netizens, who had worldwide support. The activist hacker group Anonymous made cyber-attacks (Operation Tunisia) in January on government websites, including those of the president and prime minister, to protest against online censorship. Egyptian Internet-users provided technical ways to get round the censorship and passed on news and demands from inside Tunisia.

President Ben Ali was forced to flee the country on 14 January after 23 years in power, The revolution was a human one but the online social networks helped make it happen.

The information ministry was abolished under the new provisional national unity government announced on 17 January. Well-known blogger Slim Amamou, freed four days earlier, was named secretary of state for youth and sports. The government proclaimed immediate and total freedom of news and expression.

END OF CENSORSHIP AND SURVEILLANCE ?

The Internet was seen as a threat to the country's stability and image abroad by the Ben Ali regime, which maintained very strict monitoring and filtering of traffic and hounded opponents. Website addresses and keywords were blocked and filtering was done with Smartfilter and Websense programmes, that also enabled monitoring and interception of e-mail, which was permitted by the 1998 postal law if messages "endangered public order."

The authorities claimed they only blocked terrorist and pornographic sites, but those of political opponents, human rights organisations and independent news agencies were also censored. They included Tunisnews and Nawaat, as well as the sites of the Parti démocrate progressiste (PDPinfo.org) and the Al-Nahda (Renaissance) movement, Tunisonline, Assabilonline, Reporters Without Borders and Al-Jazeera in Arabic. Searches for banned sites produced an "Error 404 - page not found" message, which led to the nickname "Ammar 404" for the state censorship operation.

Hacking into dissidents' Facebook pages was frequent, as well as blocking the sites of specific groups. Other steps against dissidents included cutting off their Internet connection, port blockage, sending viruses and malware to them and infiltrating discussion forums.

Censorship was ended by the new government on 14 January, but the Nawaat site told its visitors on 25 January that some sites were still blocked. The ministry of technology and communication had said on 21 January that all sites were freely accessible but partial censorship was being maintained of sites that "offended public decency, through violence or incitement to hatred." It gave an e-mail address, contact@web-liberte.tn, for "the public and civil society groups" to raise matters of online freedom. [1]

The situation has since improved and Reporters Without Borders has learned that no sites are now blocked and bloggers and Internet-users are no longer being hounded. The interior ministry has even set up a public relations office and started a Facebook page for Internet-users: www.facebook.com/ministere.interieur.tunisie?ref=ts&v=wall

But questions remain about the future of the censorship machinery.

NEED TO DISMANTLE CENSORSHIP APPARATUS

While censorship has disappeared, many Internet-users and bloggers have shown concern that the machinery to censor material still exists. The government must openly dismantle it.

Those who were involved in censorship have been speaking freely. ATI chief Kamel Saadaoui told Wired magazine [2] he regretted his agency had been seen as an oppressive censor when it had just been following the regime's orders. Under the new government, the ATI was helping to open up the Internet, he said, and just sticks to maintaining the network. "We have filtering engines but we

give access to them to other institutions mandated by the government to choose which sites should be blocked. We don't even know what sites they are banning because the list is encrypted."

Whatever the past role of the ATI, which many suspected was infiltrated by the secret police, the government still has the means to block websites. Saadaoui promises it will be used only to block sites involving pornography, child pornography, nudity and "hate." But it would now have to be done with a court order. He said the current filters were necessary but "the limits are symbolic." But he admitted that "it's really useless to block. Whatever we do, there are ways to get round it."

Slim Amamou, the blogger now in the government, told Reporters Without Borders on 23 February that the ATI was "drafting suggestions about its future." He talked about making "an inventory of the online structure" and said he also discussed opening up the Internet service provider market with the technology minister, who agreed with the idea. Currently all telecom operators still have to use ATI as their online gateway.

The government reportedly has plans to set up an online censorship committee, but its composition and attitudes are not yet known. Would it just block very specific sites if the source of objectionable content could not be removed and would a court order be required for each blockage? If not, a drift back towards old censorship habits is possible.

Freedom of expression is a major victory of Tunisia's "Jasmin Revolution" but new "red lines" seems to be appearing (http://en.rsf.org/tunisie-reporters-without-borders-in-10-02-2011,39519.html). Violence by police and troops, corruption by powerful old regime figures still in the country and the transition government's problems are still covered very little by the media. Such red lines must not give rise to new Internet filters.

Tunisia has given an example to everyone who dreams of freedom, by overthrowing a dictator with the help of social network websites. Including Internet access as a basic right in the new national constitution would be greatly welcomed by Tunisians. Other key moves would be to open up the ISP market and dismantle the censorship machinery. Tunisians have won their freedom partly thanks to the Internet and it should now underpin that freedom.

TURKEY

UNDER SURVEILLANCE

Domain name : .tr
Population : 77 804 122
Internet users : 35 000 000
Average monthly salary : 560 dollars
Number of imprisoned netizens : 0

The year 2010 was marked by the widely covered deblocking of the video-sharing website YouTube which, unfortunately, did not equate to a lifting of online censorship in Turkey. In a country where taboo topics abound, several thousand websites are still inaccessible and legal proceedings against online journalists persist.

THE YOUTUBE SAGA

Much was written throughout Turkey in 2010 about the fate of the Google-owned video-sharing website YouTube. Blocked in Turkey since May 2008 because of videos which Ataturk, the founder of the Republic and the nation, deemed “offensive,” it was rendered accessible again in October 2010 after a series of unexpected developments.

In June 2010, the Turkish Supreme Council for Telecommunications and IT (TIB) asked Internet service providers to block new YouTube-linked IP addresses. Certain Google services, such as Google Analytics, Google AdWords and Google Docs were also frozen.

On 5 July, the Turkish media pointed out certain contradictions in the authorities’ statements about this blocking. Judge Hayri Keskin affirmed that the site was being censored for violating the Internet law, while Transport Minister Binali Yildirim implied that the government was seeking to tax YouTube’s ad revenue.

In statements reported by several Turkish media, President Abdullah Gul nonetheless said that he was opposed to censorship and called for the law to be changed. "I do not want Turkey to be included among the countries that ban YouTube and prevent access to Google. If there are problems due to our legislation, there should be ways to overcome that.”

On 30 October 2010, an Ankara court lifted the ban on YouTube, a decision which the international community welcomed as an encouraging first step.

Yet the saga does not end there. On 2 November 2010, an Ankara court placed a new ban on YouTube as the result of a complaint filed by Deniz Baykal, former head of Republican People’s Party (CHP), the country’s main opposition party. He had been forced to resign after a video was circulated on the Internet showing an individual resembling him, implicated in an adulterous relationship. The court then referred the matter to the TIB, which ordered the website’s administrators to remove the compromi-

sing videos under penalty of being blocked – a request with which YouTube complied.

There is no certainty that YouTube will not be blocked again should a new complaint be made. The Turkish courts or the TIB may also have social networks such as Facebook in their line of sight. It would not be a first: myspace.com was blocked in September 2009 for "copyright infringements," then unblocked the following month. The Vimeo video-sharing website was banned for several days in September 2010 on personal "offence" charges following a "preventive" decision by the Ankara public prosecutor's office at the request of CHP Deputy Chairman Mehmet Akif Hamzaçebi.

In March 2011, Google-owned Blogger plateform was rendered inaccessible in Turkey. A local court banned the entire service, used by some 600 000 Turkish bloggers, in response to a complaint by satellite TV firm Digitürk that streaming media feeds from local soccer games were appearing on multiple Blogger websites, violating copyrights.

THOUSANDS OF SITES BLOCKED

YouTube's fortunate outcome should not be a pretext to ignore the extent of online blocking and censorship in the country, or the arrests and legal proceedings against bloggers and netizens.

According to engelliweb.com, some 8,170 Internet websites are currently inaccessible either as the result of a court decision or at the initiative of the TIB. In June 2010, the Organization for Security and Co-operation in Europe (OSCE) estimated that "over 5,000 sites" had been blocked in the last two years. In 2009, it had estimated 3,700, some for "arbitrary and political reasons." Notwithstanding, if the figures have increased, it does not necessarily mean that the number of news websites concerned has risen. Most blocked sites are erotic or pornographic, or devoted to games of chance, or soccer match coverage. Others focus on the gay community or dissemination news, for example about the Kurd issue, criticise high-ranking officials, or discuss what are deemed to be terrorist organisations.

Ataturk, the Turkish Army, the nation, the issue of minorities – notably the Kurd – and the so-called "terrorist" organisations are still highly controversial topics. Denouncing abuses committed by senior officials is becoming an increasingly risky undertaking. Access to the website of Çine U ur, the local newspaper in the southwestern province of Aydin in western Turkey, was banned by a September 2010 court decision because of a critical article about Çine's District Governor, Celalettin Cantürk. The newspaper's publication director Yilmaz Saglik, who is now being sued, was forced to remove the incriminated article. Any strong language in a discussion forum is likely to trigger the blocking of the website hosting the latter, as was the case for gazetevatan.com and egitimsen.com.tr.

A LEGISLATION-BACKED CENSORSHIP?

Turkish Law 5651 on the Internet provides for the widespread mass blocking of websites. The OSCE therefore called for Turkey to implement reforms promoting freedom of expression. Article 8 of this Law authorises blocking access to certain websites if there is even an "adequate suspicion" that any of the following eight offences are being committed: encouraging suicide, sexual exploitation or abuse of children, facilitating the use of narcotics, supply of unhealthy substances, obscenity, online betting; or anti-Ataturk crimes. It is this latter provision which causes difficulties. In its name, websites hosted in Turkey are often shut down, and those hosted abroad are filtered and blocked by Internet service providers. Denunciations are encouraged: Internet users can call a hotline to report prohibited online content and illegal activities. Over 80,000 calls were recorded in May 2009, as compared to 25,000 in October 2008.

Site-blocking is carried out by court orders or by administrative orders of the Supreme Council for Telecommunications and IT. Such administrative decisions are arbitrary and preclude the possibility of a fair trial. This entity, which was created in 2005 in the aim of centralising surveillance and the interception of communications (including on the Internet), has not issued its blacklist of blocked websites since May 2009 – indicating a troubling lack of transparency. In May 2010, Yaman Akdeniz, professor of Internet law at Istanbul's Bilgi University, filed a complaint against the TIB for having neglected, for one year, to meet its obligations to provide statistics of censured websites.

According to the OSCE, over 80% of the blockings observed in May 2009 were the result of administrative orders. The majority of them were made on grounds of "obscenity"

and “the sexual exploitation of children.” However, in addition to these site blockings, 158 “illegal” contents dealing with Ataturk were allegedly removed at the request of the TIB. By virtue of Article 9 of Law 5651, individuals who feel that their rights have been violated may request that the site or its host remove the incriminated content.

More troubling is the fact that nearly 200 court decisions were recorded in 2009 ordering website blockings for reasons beyond the scope of Law 5651, thereby rendering the blockings unjustified. For example, the independent news site www.istanbul.indymedia.org was suspended for “insulting Turkish identity” – a crime which falls within the jurisdiction of the Turkish Penal Code and not Law 5651. The other counts of indictment used were “dissemination of terrorist propaganda” (by virtue of the Anti-Terrorist Law) and “incitement to hatred” (by virtue of the Turkish Penal Code). Some Internet sites were also rendered inaccessible as the result of libel suits.

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

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

NETIZENS “HARASSED” FOR EXPRESSING THEIR OPINIONS

As of this date, no online journalist or blogger is behind bars in Turkey. Some have even been acquitted while on trial, but many court proceedings are underway.

Baris Yarkadas, an online journalist working for the newspaper Gercek Gündem (“Real Agenda”), was acquitted on 9 June 2010 of the charge of having "insulted the President of the Republic." He was facing a sentence of 5 years and 4 months in prison by virtue of Article 299, paragraph 2, of the Turkish Penal Code for having failed to withdraw from his newspaper’s website a critical article posted by an Internet user. Yet the journalist is still being sued by Nur Birgen, Chair of the Institute for Forensic Medicine’s Third Specialisation Board, who filed a complaint against him for “personally offending” her by referring in an article to allegations of human rights violations which several NGOs had made against her.

Ali Baris Kurt and Mehmet Nuri Kokcuoglu, the owner and director of the pro-Kurd website www.gunesincocuklari.com (“Günesin Cocuklari,” or “Children of the Sun”), were acquitted in July 2010. They had been charged with “alienating the public from military service,” “inciting hatred and racial hostility,” and “praising a crime,” for having posted a news article in 2006 entitled “The military service means murder," for which they faced a possible ten-year prison term.

After ten months of detention pending trial, Aylin Duruoglu, Director of the Vatan website (www.gazetevatan.com) and Mehmet Yesiltepe, an employee of the magazine Devrimci Hareket (“Revolutionary Movement”) were granted a conditional release. They remain charged with being members of the armed military group, “ Devrimci Karargah” (“Revolutionary Headquarters”), an accusation which Aylin Duruoglu firmly denies. The trial is still in progress.

Cem Buyukcakir, the general publications director of the Turkish Haberin Yeri (“news site”), was given a suspended eleven-month prison sentence for having “insulted President Gul” for having published following a comment posted by a reader in 2008. He appealed the decision, but the appeals court will not hear his case for one year.

In May 2010, Erdem Büyük, a student, was given an eleven-month suspended jail sentence on a five-year probation period for “attacking personal rights” after posting a caricature of Yilmaz Büyüker en, the city of Eskisehir’s mayor, on his Facebook page, even though he had only transferred this caricature, not created it.

The trials of Hali Sebnem, Korur Fincanci and Adnam Demir are still in progress. Savda is scheduled to apprea before the Third Chamber of the Beyodu Criminal Court in Istanbul on the 24 March 2011

Lastly, Soner Yalçin, the owner of the Oda TV news website, Baris Pehlivan, the site’s editor, and Baris Terkoglu, one of its reporters, were arrested on February 14 when counter-terrorism police raided the website’s Istanbul headquarters. They stand accused of “inciting hatred and

hostility through the media," membership of a "terrorist organization" and obtaining and publishing confidential state documents. They are facing possible sentences of more than 20 years in jail. The "terrorist organization" referred to in the charges is Ergenekon, an alleged secret network of senior army officers, academics, businessmen and others who have been on trial since October 2008 on charges of plotting to use terrorist methods to overthrow Recep Tayyip Erdogan's government. Reporters Without Borders has urged the judicial authorities handling this sensitive case to adhere strictly to the law. Four other journalists from odatv.com were also arrested on 6 March 2011 : Müyesser Yildiz, Dogan Yurdakul, Coskun Musluk et Sait Cakir.

REVENGE OF THE NETIZENS?

In order to protest against censorship, in mid-June 2010, hackers blocked for ten hours the websites of the TIB (www.tib.gov.tr), the Turkish Telecommunications Authority (www.tk.gov.tr), the Information and Communication Technologies Authority (ICTA) - http://www.btk.gov.tr) and The Scientific and Technological Research Council of Turkey (www.tubitak.gov.tr). Several hours later, the blocking was lifted and the following message appeared on the sites concerned: "This is being done to show our good will."

In fact, online censorship is widely criticised in Turkish society, as attested to by the online mobilisations and protests demanding that it stop.

The anti-Net censorship campaigns launched in 2010 met with various degrees of success, such as the one initiated by http://yeter.neonebu.com/InternetteSansureHayir.aspx* ("Stop Internet Censorship in Turkey!"), or the website http://sansuresansur.blogspot.com/2010/10/jet-hzn-da-site-kapatan-kampanya.html ("Censor Censorship"), or the one entitled "Internet sansür degil, Hiz Ister" ("The Internet needs speed, not censorship"). These campaigns, among others, were well-covered online.

Online protests have been backed by several real-life demonstrations. In July 2010, for the first time, over 2,000 people paraded down Istanbul's Istiklal Avenue, answering a call by sites campaigning for freedom of expression on the Net, for example the "Common Platform Against Internet Censorship" (www.sansursuzinternet.org.tr). They called for the end of Web censorship and denounced the authorities' lack of response to calls for amending Law 5651 on Internet-related offences. The blocking of YouTube was highlighted as a source of embarrassment for Turkey.

Some time has passed since then and the deblocking of YouTube – which could be called into question at any time – must not be allowed to mask the extent of Web censorship in the country, or the archaic nature of the Internet laws. Vigilance is needed after a year as sombre for freedom of expression in Turkey as 2010 proved to be.

UNITED ARAB EMIRATES

UNDER SURVEILLANCE

Domain name: .ae
Population: 4,975,593
Internet users: 3,777,900
Number of subscribers: 1.4 million
Average monthly salary: 25,000 U.S. dollars
Average cost of a one-hour cybercafé connection:
Number of imprisoned netizens: 0

The Internet and the new media relayed information about a wide range of sensitive topics in 2010 such as corruption and criticism of the government, causing online repression and censorship to intensify. The attempts to access Blackberrys datas contrast starkly with the image of modernity that the United Arab Emirates is trying to cultivate.

A TECHNOLOGICAL LEADER

The United Arab Emirates is a technological leader in the Arab world, thanks primarily to Dubai Media City and Dubai Internet City, free economic zones where key IT and media sector companies have set up offices. In March 2009, the authorities decided to display the UAE's domain name in Arabic in order to expand the use of this language on the Internet. They plan to invest several billion dollars into developing Internet infrastructures and access, particularly in government offices and schools. A very large portion of the UAE's population (75 %) has Internet access.

A TARGETED AND UP-TO-DATE FILTERING SYSTEM

A very strict filtering system targets any pornographic content. Websites discussing topics such as dissenting political opinions, or non-orthodox views of Islam, or criticisms of society – particularly the royal family – or of religion or human rights, are also rendered inacessible. The sites localnewsuae.com, arabtimes.com, uaepriosn.com, uaetorture.com and uaehewar.net, not to mention the Facebook page and Twitter group of the latter, are regularly blocked or banned. The economy is another highly sensitive subject: Mujarad Ensan's blog (www.mujarad-ensan.maktooblog.com) was blocked after it referred to the repercussions of the economic crisis on the Kingdom. Sites providing access to content deemed "obscene," or to censorship circumvention tools, are no longer accessible.

The now-blocked UAEhewar website offered the only forum which allowed the Emiratis to freely discuss subjects considered taboo in their country, and notably to post comments critical of their leaders. It also formerly published interviews of prominent opposition figures such as Dr. Christopher Davidson, who has written several books on Dubai, activist Mohammed Al Mansoori and political science professor Dr. Ebtisam Al Ketib. The authorities therefore decided that the website had gone too far.

Although websites such as Flickr, myspace.com and http://www.ahewar.org are still accessible, Twitter, Facebook and YouTube are paritally censored by the regime. Facebook has 1.2 million users in the UAE. The forums are filtered according to what news and topics are broached by the netizens.

Authorities are said to have blocked five hundred key words. Decisions to block websites are made jointly by the Telecommunication Regulation Authority (TRA) and the Ministry of Communications, and enforced by the country's two Internet service providers, Etisalat and Du. The latter use SmartFilter, a software program produced by Secure Computing, which the American firm McAfee acquired in 2008.

EXTENDING SURVEILLANCE TO MOBILE TELEPHONES

Mobile telephones are also being filtered. The latest victim is the Blackberry, whose Internet access has been filtered since December 2009. In July 2009, the authorities made an unsuccessful attempt to install spyware on these smartphones . They made another attempt in 2010. In the Emirates, some 500,000 people are now using Blackberrys and their popularity is constantly growing. Their potential for mobilising dissatisfied citizens worries the regime, which, in 2010, took some dissuasive steps to crack down on Blackberry users.

Badr Ali Saiwad Al Dhohori, an 18-year-old youth residing in the emirate of Ras Al Khaimah, was arrested on 15 July 2010 for allegedly using his Blackberry to try to organise a (peaceful and ultimately cancelled) protest against a gasoline price increase . Although he was released on 28 August 2010, Badr Ali Saiwad Al Dhohori had lost his job. Pressures on users have been coupled with those exerted on the Blackberry's Canadian manufacturer, Research In Motion (RIM). The Emirates had given RIM an ultimatum to comply by 11 October 2010, under threat of cuttingoff certain Blackberry services, such as instant messaging, which the regime deemed "non-compliant with official and social norms," citing the pretext of "national security".

A great deal of conflicting information has been circulating as to the substance of the negotiations due to a lack of transparency on the part of both parties. Yet, according to information received by Reporters Without Borders, the Emirati authorities and RIM have allegedly reached an agreement on access to the smartphones' encrypted data. The Emirati government has stated that Blackberrys are now in compliance with the law, without specifying the scope of the concessions which RIM may have had to make.

The U.S. company Apple also had to accept certain government stipulations and was notably obliged to sell the Iphone 4 to the Emirates without its flagship "FaceTime" application, which allows users to enjoy live video chats.

CYBERSURVEILLANCE

Cyberpolice have been monitoring the Web since December 2008 to keep a close watch on netizens. It processed over 200 cases in 2009, most of them linked to cybercrime and hacking, according to the authorities.

Although the country now has several hundred cybercafés, they are not the populations' main access point, since Internet users surf the Web in their homes and workplaces. Some new rules – apparently not enforced – require that users show an ID and record their personal data.

In addition to the intensifying surveillance, a new freedom-restricting legal arsenal is now being implemented. According to certain articles of the 2006 law on cybercrime, an Internet user can be imprisoned for "opposing Islam," "insulting any religion recognised by the state" or "contravening family values and principles."

Despite the fact that, according to a survey published by the newspaper Khaleej Times, 95.5% of respondents are opposed to the present filtering system, it has been made even more restrictive. Dubai Internet City and Dubai Media City, which had been spared to date, are now targets of the filtering, despite promises made to investors.

NETIZENS DEMONSTRATE INCREASING ACTIVISM

A highly committed netizen community has emerged. Bloggers tackle public interest concerns, though they often feel compelled to practice self-censorship. Not all netizens have given up: an ever-greater number of them know how to bypass censors and express their views. Some discuss highly sensitive subjects and are willing to bear

the consequences.

On 13 January 2010, the Abu Dhabi Court of Appeals upheld the fine of 20,000 dirhams (3,755 euros) and damages of 10,000 dirhams (1,877 euros) that a lower court had imposed on Ahmed Bin Gharib, editor of the news website Hetta.com in a defamation suit brought by the Abu Dhabi Media Company over comments posted by netizens in response to an article about the company published on the website. The latter found the comments defamatory and offensive. The court also ordered that the site be closed for one month.

Thanks to online forums, social networks and even Blackberrys – not to mention the popular Blackberry Messenger – netizens have been able to share opinions on controversial topics banned in the traditional media, such as human rights, the harassment and jailing of activists, freedom of expression, political reforms, corruption and even WikiLeaks.

Certain online campaigns like those launched by UAZHewar.net and lawyer Abdul Hameed Al Kumaiti have led to mass mobilisation on such matters as torture, Blackberrys and corruption. Abdul Hameed Al Kumaiti is notably defending freelance journalist Mark Townsend, whose trial will take place on 16 March, 2011. This netizen was charged with defamation last August.

Despite the censorship, the website uaetorture.com had managed to post a nearly one-hour-long video of Sheikh Issa bin Zayed al-Nahyan – brother of Sheikh Khalifa bin Zayed al-Nahyan, Abu Dhabi's ruler and President of the United Arab Emirates – torturing a young Afghani, Mohammed Shah Poor. This video was massively circulated online, causing a huge public outcry.

In 2010, the new media managed to spearhead and host debates on core issues within the UAE's society. Despite the authorities' repressive response, those discussions were able to take place both online and offline.

VENEZUELA

UNDER SURVEILLANCE

Domain name: .ve
Population: 28,686,633
Internet users: 8,846,535
Average cost for a one-hour cybercafé connection: 1 U.S. dollar
Average monthly salary: environ 550 $
Number of imprisoned netizens: 0

President Hugo Chávez, who is systematically covered by all traditional media, could not resist the temptation to increase his exposure on the Internet and to try to regulate this space over which he had previously eluded his grasp. He succeeded in 2010, amidst increasing tension between leaders and the opposition media. Although there is still free Internet access in the country, tools for controlling access are in place and self-censorship is on the rise. Discussion forums are being closely monitored by the authorities.

ALMOST ONE-THIRD OF THE POPULATION ARE CONNECTED

Almost one third of the population is connected in Venezuela, making it the Latin American country with the fourth highest number of Internet users after Argentina, Colombia and Chili. Social networks are popular there. As of March 2010, Facebook had 5.3 million registered users, compared to Twitter's 500,000 in that same period.

The government facilitated the population's access to the Internet by setting up state-sponsored access centres. In 2009, the Canaima Project was launched with the aim of providing every primary school student with his or her own computer. To date, more than 60% of the 8.8 million Internet users originate from the working classes.

Venezuela's leading telecom operator and Internet service provider, CanTV, which is state-owned, has a monopoly on the provision of ADSL services. Its 2007 nationalisation marked the first stage of the government's efforts to tighten its control of the Internet.

2010: CHÁVEZ' MUCH-TOUTED ENTRY INTO WEB 2.0

Not satisfied with his coverage in the traditional media, President Hugo Chávez threw himself wholeheartedly into Web 2.0 in 2010. Last April he created his own blog, www.chavez.org.ve, "a page for communicating with the world." In this blog, he reports on his interviews with foreign leaders and the latest government statistics confirming a drop in the homicide rate, or presents commentary on sports events. The site also features speeches by the Head of State, videos, photos and a form which visitors can use to contact the president's staff.

In April 2010, he also created his own Twitter account @chavezcandanga, which had over 1,150,000 subscribers as of January 2011. Chávez even publicly urged Cuban

and Bolivian leaders to join Twitter!
Many Venezuelans have ridiculed the Head of State, wondering how such a verbose man – one so accustomed to making speeches several hours long – could limit himself to 140-character posts.

Chávez justifies his presence on social networks by stating his intention of becoming a "cybernetic activist of the Bolivarian revolution" in order to "counter the opposition's influence on the social networks." He joyfully announced that "the people are taking over the Internet," stating that conspirators use the Web to try to spread false information and stir up coup d'états against him.

The President still has a long way to win netizen support. Seven out of the ten most popular accounts in Venezuela are critical of Chávez, while his most fervent supporter is ranked 66th (www.twitter-venezuela.com). The presidential account was allegedly hacked in September 2010.

In February 2010, the hashtag #freevenezuela used by the opposition in response to Chávez attacks against freedom of the press, was the 4th most-commented-on subject on Twitter worldwide, with over 60,000 entries. The Facebook page "Let's see if I can find a million people that hate Chávez" has a total of nearly 750,000 fans, while pro-Chávez pages have only a few tens of thousands of subscribers .

Both the president and the opposition have been making extensive use of social networks, particularly Twitter, trying to induce Venezuelans to vote in the September 2010 legislative elections.

Chávez had accused social network users of being "instruments of capitalism." Now accused in turn of being a capitalist, his response is that "This isn't capitalist or socialist, technology depends on how you use it."

RELENTLESS ATTACK ON NOTICIERO DIGITAL

On 13 March 2010, President Chávez called for criminal sanctions to be imposed on the news and opinion portal Noticiero Digital, accused of having posted false information.

Two Internet users had incorrectly announced on Noticiero Digital's forum that Infrastructure and Telecommunications Minister Diosdado Cabello had been assassinated. According to the President, the information remained online for two days. The website managers admitted that two new members of the forum had posted these false news items and pointed out that the latter had been removed a few hours after they were notified of it. The website applies a standard procedure to all Internet forums: it does not a priori censor them, but does so if its terms of use have been violated. The website managers' good faith is thus not in question. The forum has over 120,000 members.

After this episode, Hugo Chávez asked Minister Diosdado Cabello to "regulate the Internet."

On 8 June 2010, acting under a presidential order, the Venezuelan Public Prosecutor's Office (Fiscalia) initiated proceedings against Noticiero Digital for allegedly "attacking constitutional order" and "supporting a coup d'état." These new proceedings were prompted by an opinion piece posted on the Noticiero Digital website on 2 June by Roberto Carlos Olivares that discussed mobilisation efforts being made by "retired military officers and patriots" with a view to engineering a "civil-military transition" at the head of government, possibly in 2011. In this extremely vehement text, the author obviously expresses his wish to see such a "transition" succeed. However, voicing this opinion was meant to induce others to make comments and no conclusion can be made that the Noticiero Digital media was "supporting a coup d'état."

In an interview granted to Reporters Without Borders, Noticiero Digital's director, Juan Eduardo Smith, deplores the fact that the government's "ever more forceful reaction to any views contrary to its own vision of the world."

PREMISES OF CENSORSHIP? BLOCKINGS, CLOSINGS AND SELF-CENSORSHIP

In the wake of the proceedings initiated against Noticiero Digital, several Internet websites decided to tighten their forum's controls in order not to expose themselves to any judicial problems. Such is the case, for example, of Noticias24 – one of the country's leading news websites – which has set up a system to review in advance all comments to be posted, which it reserves the right to delete, as stated in its terms of use. The website explains that it will not tolerate insults, personal attacks, racist or sexist

slurs, incitements to violence or anything else which violates applicable laws.

In addition, from 26 to 27 September 2010, the leading Internet access provider, CanTV, blocked without notice some blogs hosted on the Wordpress platform. The bloggers @alfrediux [http://zuplemento.wordpress.com], @ ConIdayVuelta [http://conidayvuelta.wordpress.com] and @elena_victoria [http://elenaenvacaciones.blogspot.com] then stated on lapatilla.com that their blogs were nonetheless accessible from Spain or Venezuela via proxy servers.

During the same period, the National System of Telematic Incident Management (VenCERT) allegedly carried out a special surveillance operation involving 1500 Internet websites in order to supervise the publication of electoral-related contents. According to VenCERT, 48% of the sites reviewed did post illegal electoral content. The blocking of certain media and blog Web pages therefore was done "to protect the integrity and availability of public information on the official pages of the national authorities' and ministries' media." VenCERT did not indicate which websites are concerned, nor what they are being charged with.

SOME TWITTER USERS TARGETED TO SET AN EXAMPLE

Jesús Majano, an engineer with Corpoelec, Venezuela's National Electricity Corporation, was arrested on 8 September 2010 for having circulated some tweets "instigating a murder" and "inciting the commission of a criminal offence" against President Hugo Chávez. After being released on parole, he now must continue to appear before the court every fifteen days.

Two other Twitter users, Luis Acosta Oxford (@leaoxford) and Carmen Cecilia Nares (@carmennares), who reside in the State of Bolivar (in southeastern Venezuela), over 500 km from Caracas, were arrested on 8 July 2010 and charged with "spreading false news" with the intent of destabilising the banking system and damaging the country's economy, by virtue of Article 448 of the 2001 Banking Law.

Following a hearing on Monday 12 July 2010, the two individuals were granted parole in anticipation of a future trial. They must continue to appear before the court every fifteen days. They are also prohibited from circulating any messages on the bank issue, as provided for in Article 256 of Venezuela's Criminal Code, under penalty of an eleven-year prison sentence.
On 30 June 2010, Luis Acosta Oxford (@leaoxford) posted the following message on his Twitter account: "Ladies and Gentlemen, so you may not say no one warned you … leave today. I assure you that there are very few days left." [Señores para que no digan que no se les dijo retiren hoy de... quedan pocos días, se les dijo.]

Since November 2009, more than a dozen banks have been closed or placed under government control. Inquiries into the spreading of rumours and false news about the banking system began in March 2010, when the police detected the presence of a number of postings warning the public about a so-called "financial crash."

Until 12 July 2010, Luis Enrique Acosta had 225 subscribers and had posted 201 messages, while only six people were following Carmen Cecilia Nares, who had not posted a single tweet. Their obviously limited influence on the Web belies the government's theory that these two individuals could have been engaged in efforts to undermine the national banking system. Instead, they seem to have been assigned the role of scapegoats, while the authorities were publicly railing against their detractors' use of the social network.

The various accusations which the government has been making against certain Internet users, the proceedings brought against Twitter users and the non-stop harassment targeting Noticiero Digital are so many phases of what appears to be an impending government strategy to take control of the Net: a prelude to imposing presidential rules.

A GAG LAW FOR THE INTERNET

On 11 July 2010, former vice-president José Vicente Rangel stated that certain Twitter users in Venezuela were devoting themselves full-time to spreading rumours. Hugo Chávez had announced during a televised speech on Saturday 13 March: "The Internet cannot be something open where anything can be done and said. No, every country has to impose its rules and regulations."

It was in this frame of mind that, under pressure from the government, the National Assembly delivered a new blow

to freedom of expression and information on 20 December 2010, by approving two bills amending the Organic Law on Telecommunications (Lotel) and the Social Responsibility in Radio, TV and Electronic Media Law (Resortemec). The latter's aim is to facilitate Web control and surveillance, notably by setting up an Internet filtering system.

The Resortemec Law provides for stiffer fines and the suspension – which could mean definitive closure for repeat offenders – for media which circulate messages (including Internet user postings) that:

- incite or promote hate and intolerance for religious or political reasons, on the basis of a gender difference or because of racism or xenophobia;
- incite or promote criminal activity;
- engage in war propaganda;
- cause panic or disturb public order;
- discredit legitimately constituted authorities;
- incite murder;
- incite or promote non-respect for the laws in force.

Although points 1 and 6 are admissible and valid in any legislation, point 3 – which is also admissible – will presumably not be applied to the government's often bellicose propaganda. Points 2, 4 and 5 represent a major threat to freedom of expression and information because they are too broadly and vaguely defined. It appears that website moderators will inevitably have to close their discussion forums. Point 5 regarding the "legitimately constituted authority" also concerns the next National Assembly, which was elected on 26 September 2010. One positive aspect of the new Resortemec Law is that it no longer contains the controversial provision for a single Internet access point.

Still pertaining to Article 28 of the Law, Internet access providers will have "to establish mechanisms for restraining the circulation of messages" concerned by such prohibitions without specifying the technicalities involved. This provision is an open door for introducing a Net filtering system.

The application of this law, as well as the self-censorship momentum which could result from it, must be kept under close watch in the months ahead. Some are rightly concerned about sanctions being tailored in such a way that the electronic media and websites with close ties to the government will receive special treatment, while those of the opposition will experience a much harsher interpretation of the law, thereby extending to the Net the extremely polarised opinion already evident among the traditional media.

Considering his experience with the so-called "traditional" media, President Chávez' latest enthusiasm for the electronic media while he is endowed with full powers may well cause concern about the future of online freedom of expression.

REPORTERS
WITHOUT BORDERS
FOR PRESS FREEDOM

International Secretariat
REPORTERS WITHOUT BORDERS

47 rue Vivienne, 75002 Paris, France - Tel: 33 1 4483-8484 - Fax: 33 1 4523-1151 - Website: www.rsf.org - E-mail: rsf@rsf.org - Ambroise Pierre - Africa desk: afrique@rsf.org - Benoît Hervieu - Americas desk: ameriques@rsf.org - Vincent Brossel - Asia desk: asie@rsf.org - Johann Bihr - Europe desk: europe@rsf.org Soazig Dollet - Middle East desk: moyen-orient@rsf.org - Lucie Morillon - Internet desk: internet@rsf.org - Press contact: presse@rsf.org

REPORTERS WITHOUT BORDERS is an international press freedom organisation. It monitors and reports violations of media freedom throughout the world. Reporters Without Borders analyses the information it obtains and uses press releases, letters, investigative reports and recommendations to alert public opinion to abuses against journalists and violations of free expression, and to put pressure on politicians and government officials.

General secretary : **Jean-Francois Julliard** I Chief Editor : **Gilles Lordet**