INTERNET ENEMIES REPORT 2012

REPORTERS WITHOUT BORDERS
FOR FREEDOM OF INFORMATION

BESET BY ONLINE SURVEILLANCE AND CONTENT FILTERING, NETIZENS FIGHT ON

This report, which presents the 2012 list of countries that are "Enemies of the Internet" and "under surveillance," updates the report published on 12 March 2011.

The last report, released in March 2011 at the climax of the Arab Spring, highlighted the fact that the Internet and social networks have been conclusively established as tools for protest, campaigning and circulating information, and as vehicles for freedom. In the months that followed, repressive regimes responded with tougher measures to what they regarded as unacceptable attempts to "destabilize" their authority. In 2011, netizens were at the heart of the political changes in the Arab world and elsewhere. They tried to resist the imposition of a news and information blackout but paid a high price.

At the same time, supposedly democratic countries continued to set a bad example by yielding to the temptation to prioritize security over other concerns and by adopting disproportionate measures to protect copyright. Internet users in "free" countries have learned to react in order to protect what they have won. Some governments stepped up pressure on technical service providers to act as Internet cops. Companies specializing in online surveillance are becoming the new mercenaries in an online arms race. Hactivists are providing technical expertise to netizens trapped by a repressive regime's apparatus. Diplomats are getting involved. More than ever before, online freedom of expression is now a major foreign and domestic policy issue.

New media keep pushing back the boundaries of censorship

Online social networks complicate matters for authoritarian regimes that are trying to suppress unwanted news and information. It was thanks to netizens that Tunisians learned about the street vendor who set himself on fire in Sidi Bouzid and Egyptians learned about Khaled Said, the young netizen who was beaten to death by police outside an Alexandria Internet café. It was thanks to social networks that Sidi Bouzid and Khaled Said became news stories and went on to become cornerstones of the Arab Spring.

The revolution of microblogs and opinion aggregators and the faster dissemination of news and information that results, combined with the growing use of mobile phones to livestream video, are all increasing the possibilities of freeing information from its straightjacket. The mixing of journalism and activism has been accentuated in extreme situations such as Syria, where ordinary citizens, appalled by the bloodshed, are systematically gathering information for dissemination abroad, especially by the international news media, so the outside world knows about the scale of the brutal crackdown taking place

The crackdown on the pro-democracy movement in 1988 in Burma involved a great deal of bloodshed in part because very few photos and video footage of it reached the outside world. But Burma's Saffron Revolution in 2007 took place live in front of the world and triggered a strong international reaction that partly accounts for the country's recent – albeit still limited – reforms.

Even the total news and information blackout in North Korea, the "Hermit Kingdom," is being challenged. Mobile phones give those who live near the Chinese border the possibility of being linked to the rest of the world. And the border is sufficiently porous to allow mobile phones, CDs, DVDs and USB flash drives containing articles and other content to be smuggled in from China.

In Turkmenistan, an "Information 2.0" war was started by a deadly explosion at an arms depot in the Ashgabat suburb of Abadan in July 2011. For the first time, netizens managed to break through the regime's wall of silence by using their mobile phones to film video of the explosion and its aftermath and post it online. They subsequently paid a high price.

Saudi Arabia's relentless censorship has not been able to prevent women from fighting for the right to drive or vote and getting their fight relayed on the Internet, attracting the international community's attention and, as a result, a degree of attention within the country.

In 2011, use of online information to rally support was not limited to "political" goals. The Internet also buzzed with condemnation of corruption and social abuses, including the protests by the residents of the Chinese village of Wukan against the seizure of their farmland by unscrupulous officials, and the documentation of electoral fraud in Russia.

In Vietnam, it is still dangerous to blog about the Chinese-run bauxite mines and their disastrous impact on the environment. The highland region where the mines are located is virtually sealed off. Its few visitors cannot take cameras, video-cameras or smartphones with them. The aim is to prevent the dissemination of potentially-embarrassing video footage. The Bauxitevietnam.info website is nonetheless managing to obtain information and is doing its best to cover the situation.

Internet and mobile phone shutdowns become commonplace

Repressive regimes have learned the lesson. Keeping the media at bay, intimidating witnesses and blocking access to a few news websites are not enough to ensure the success of a news blackout. A much more effective way is to seal off the area concerned to prevent unwanted witness from entering and any digital content from leaving, and to cut off communications by blocking SMS messaging and by shutting down Internet access and mobile phone services in a temporary or targeted manner.

Egypt showed the way at the height of the demonstrations at the end of January 2011 by cutting Internet access for five days, an unprecedented move. Other countries, such as Democratic Republic of Congo, Cameroon and Kazakhstan, have done the same during elections or unrest, or even ahead of anticipated unrest. China uses the well-tested tactic of suspending communications in cities or provinces when it loses control of the situation. Tibet, Xinjiang and Inner Mongolia were the first victims.

Nonetheless, shutting down the Internet is a drastic solution that can create problems for the authorities and can hurt the economy. Slowing the Internet connection speed right down is more subtle but also effective as it makes it impossible to send or receive photos or videos. Iran is past master at this. Syria's censors also play with the Internet connection speed, fluctuations being a good indicator of the level of repression in a given region.

Bahrain is an example of a news blackout succeeding thanks to an impressive combination of technical, judicial and physical censorship methods.

More content filtering

As soon as the uprisings in Tunisia and Egypt got under way, most regimes that censor the Internet quickly reinforced online content filtering in a bid to head off any possibility of similar unrest spreading to their own countries. Some regimes have adopted filtering as standard tool of governance, one that strengthens their hold on power. Livestreaming sites and social networks are often the most affected.

In Uzbekistan, the government blocked access to forums where ordinary members of the public discussed the Arab revolutions. In China, the word "Jasmine" and the word "Occupy" followed by the name of a Chinese city were blocked online. In Belarus, where there were major demonstrations, the social network Vkontakte was rendered inaccessible. The Kazakh authorities reacted in a similarly disproportionate manner, blocking not only a few "extremist" sites but also the entire LiveJournal blog platform.

Turkey seems to have backed away from an announced plan, bordering on the ridiculous, to censor 138 words online. It has nonetheless created a system of online content filtering which, although optional, is seen as a veiled form of censorship.

The new Thai government boasts that more online content has been blocked in the past few months than in the previous three years. The grounds given for this new threat to freedom of expression is the need to combat lèse-majesté.

Continuing vigilance is needed in Tunisia where Ammar 404, the nickname for the online filtering and surveillance system established by deposed President Ben Ali, could be revived as a result of a possible judicial decision to require filtering for pornographic content.

South Korea has decided to increase the number of blocked websites in response to the North's propaganda. Tajikistan, which does not figure in this report, has blocked Facebook and news websites while Pakistan is accused of wanting to build its own Great Electronic Wall.

More content removal, pressure on technical service providers

Censors are increasingly trying to enlist private-sector Internet companies in online surveillance and censorship. Some cooperate, others resist. Under government pressure, Chinese micro-blogging websites such as Sina Weibo have had to hire thousands of moderators and now require users to register under their real name.

Website hosting companies are under growing pressure to remove content in response to "withdrawal notifications," a procedure likely to lead to abuses, as UN special rapporteur on freedom of expression Frank La Rue has stressed. In Thailand, *Prachatai* news website editor Chiranuch Premchaiporn is facing a possible 20-year jail sentence for failing to react with sufficient speed when told to remove comments posted by site visitors that were critical of the monarchy.

India is one of the countries where more and more pressure is being put on Internet service providers and website hosting companies. The authorities there are trying to persuade them to provide a preview of content so that anything "shocking" or liable to provoke sectarian strife can be eliminated.

Threat to Net neutrality and online free speech from "right to be forgotten"

More and more individuals are requesting that information involving them be deleted from online archives on the grounds of a supposed "right to be forgotten" or "right to digital oblivion." European commissioner for justice Viviane Reding fuelled concern on 8 November by referring to a proposed directive that would allow anyone to request the deletion of content of a personal nature "for legitimate reasons."

A generalized "right to oblivion," enshrined in a law, would be hard to reconcile with online freedom of expression and information. Such a law would be hard to implement in practice and could place an impossible obligation on content editors and hosting companies – the complete erasure of online content. A thorough debate is need to determine whether individual rights are not already sufficiently guaranteed by existing legal provisions on the right to privacy, media offences, personal data and recourse to the courts.

Surveillance getting more effective and more intrusive

Internet content filtering is growing but Internet surveillance is growing even more. Censors prefer to monitor dissidents' online activities and contacts rather than try to prevent them from going online. The police chief in the United Arab Emirates, for example, has acknowledged that the police monitor social networks.

It is a human failing. The security services no longer interrogate and torture a prisoner for the names of his accomplices. Now they want his Facebook, Skype and Vkontakte passwords. It is the same in Bahrain, Turkmenistan or Syria. The response of some dissidents is to create false accounts or to give access codes to a trusted friend so that, in the event of arrest, the friend can take control of the account and thereby ensure that contacts are not endangered.

The protection of networks of dissidents and reporters' sources is one of the leading challenges in the fight for information. Foreign reporters visiting sensitive countries should take special precautions in accordance with local conditions. It is no longer enough to take a bullet-proof vest when setting off for a war zone or troubled region. A "digital survival kit" is also needed to encrypt information, anonymize communications and, if necessary, circumvent censorship.

Attempts to "phish" for social network usernames and passwords have been reported in Syria and Iran, as well as the use of false security certificates. The attempts were reported in Syria after the authorities had stopped blocking access to Facebook – something that was clearly done not as a conciliatory gesture but in order to facilitate surveillance.

The neutralization of encryption, anonymization and circumvention tools is also being prioritized by repressive regimes. Iran is now capable of blocking https and the ports used by Virtual Private Networks. China is able to restrict the number of IP addresses that can connect to the international network at the same time.

To enhance their surveillance abilities, repressive regimes turn to specialized companies for ever more effective equipment and software for filtering, monitoring and Deep Packet Inspection. The SpyFiles which WikiLeaks has published are a mine of information on the subject. The companies they use are very often western ones that have been lured by a very lucrative market.

They include the US company BlueCoat, criticized for its activities in Syria, the French company Amesys, which supplied Col. Gaddafi, and Vodafone, the target of an ANHRI suit in Egypt. The Italian company AreaSpa finally pulled out of Syria after an international campaign criticizing its cooperation with the Assad regime. The European Parliament has adopted a resolution supporting tougher regulation of exports to repressive countries. A bill with similar aims is currently before the US congress.

In her book "Consent of the Networked," journalist and Internet specialist Rebecca MacKinnon has rightly stressed the need for Internet users the world over to raise questions about the way technology is used in order to ensure that their rights and freedoms are protected.

Propaganda rules the Web

North Korea has taken its propaganda war against its southern neighbour on to the Web, establishing a presence on social networks. Cuban propaganda continues to attack bloggers who criticize the government, accusing them of being mercenaries working for the American "empire".

China has signed up "50-cents", bloggers paid to post messages endorsed by the party, ever since the disturbances that shook in Inner Mongolia after a protesting herder was killed by a truck. Propaganda messages like this one have taken root on the Internet: "Dear students and friends, it was just a road accident. Some people with an ulterior motive have interpreted as an ethnic conflict, or linked to oil and gas. The government is taking this case very seriously … We hope that students will not believe the rumours …" The government is believed to have an arsenal of 40,000 microblogs to communicate with the population.

Syria's cyber army is expert in the art of contaminating the Facebook walls of opponents and dissidents, often with the aim of discrediting them, and to drown out critical comments with a tide of praise for the government of President Bashar al-Assad. Twitter accounts have been created to exploit the #Syria hashtag, sending out hundreds of tweets with keywords that link to sports results or photos of the country.

Bahrain is spending millions to polish its image abroad and give the impression that the country has returned to normal. This has been capped by the announcement that the 2012 Bahrain Formula One Grand Prix, cancelled last year, will go ahead in April.

Cyber attacks

Cyber attacks in the form of distributed denials of service (DDoS) are widespread. Last year saw the rise of groups of hacker such as Anonymous, which were behind cyber attacks on the Tunisian, Egyptian and Syrian governments.

Governments are often behind attempts to hack news websites or independent sites. Even Eritrea was hit. Opposition sites were blocked just as the United Nations was approving sanctions against the country. Sri Lankan sites were also victims of cyber attacks. On the eve of the parliamentary election in

Russia, a series of coordinated cyber attacks and arrests of journalists and bloggers took place with the aim of stifling political discussion, which can only take place freely via the Internet.

During the demonstrations in Belarus, the Internet service provider BelTelecom redirected web users trying to connect to the Vkontakte social network to sites containing malicious software.

Besides a regular army, every country now has a cyber army, which may or may not be official. The reputation of the Chinese cyber police is well established and the Syrian and Iranian cyber armies also play a major role.

Getting rid of awkward witnesses

2011 was the deadliest year for netizens, its violence unmatched in the time that dissidents and human rights campaigners have been making widespread use of the Web. Several were killed in Bahrain, Mexico, India and Syria. Dozens of others are probably still to be identified and there will undoubtedly be still more to add to the toll, particularly in Syria.

In Mexico, drug cartels hit social network users directly. Three netizens and one journalist were shot dead in cold blood. The headless body of a Mexican Internet activist was found in Nuevo Laredo on 9 November. The victim, nicknamed "Rascatripas" (Belly-Scratcher), moderated the website "Nuevo Laredo en Vivo" which exposed organized crime. A message left beside the body proclaimed: "This happened to me for not understanding that I shouldn't report things on social networks."

On 9 April 2011, the netizen Zakariya Rashid Hassan died in custody in Bahrain, a week after he was arrested and charged with inciting hatred, disseminating false news, promoting sectarianism and calling for the overthrow of the government on online forums.

At least seven media workers had already been killed as a result of their work in Syria by the end of February this year. Netizens who also paid with their lives included Basil Al-Sayed, Ferzat Jarban and Soleiman Saleh Abazaid.

Raids and roundups

As netizen numbers grow, more and more of them are at risk. At least 199 of those engaged in informing the public were arrested in 2011, a 31-percent increase compared with the previous year. Today, at least 120 netizens are in prison because of their activities. China, followed by Vietnam and Iran, has the largest number of netizens in prison again this year.

On 16 February this year, a raid was carried out at the Syrian Centre for Media and Freedom of Expression, similarly in Turkmenistan after an explosion at an arms depot near Abadan killed many civilians. Iran and Vietnam have also used similar methods. Vietnam has attacked Catholic networks and China regularly arrests netizens and dissidents to intimidate their followers. Nobel Peace Prize laureate Liu Xiaobo remains behind bars.

Egypt jailed its first political prisoner of the post-Mubarak era, the blogger Maikel Nabil Sanad who was convicted for criticizing the armed forces.

House arrests and "fake releases" abound. China has made this a speciality, as the blogger Hu Jia and cyber-dissident Hada, who campaigns for the rights of the Mongol people, discovered. Vietnam has also used this practice.

Inhuman treatment, pressure and unfair tactics

Many Syrian and Bahraini netizens have been tortured in custody. Iranian authorities in particular favour extracting confessions from dissidents then broadcasting them on television. In Egypt bloggers have reported being subjected to degrading treatment during questioning by security forces.

The "UAE five", a group of netizens and activists accused of online subversion and jailed in the United Arab Emirates, were accused of being traitors, as were their families.

In Bahrain, the noted dissident Nabeel Rajab is regularly smeared in the media as well as being subjected to physically assault.

In Cuba, a pitched battle is in progress between pro-government bloggers and their "alternative" counterparts who criticize the government. The latter, including the blogger Yoani Sanchez, have been the target of a smear campaign in the state-run media and on foreign propaganda sites.

Chains of support

Bonds have been created between blogospheres and citizens throughout the world have started relaying calls for solidarity, as well as startling images and shocking stories. Global Voices, the international network of bloggers and citizen journalists, has played an important role in the dialogue between online communities and NGOs that campaign for freedom of expression.

In order to combat increasingly competent censors, self-styled "hacktivists" have been giving technical assistance to vulnerable netizens to help them share information in the face of pervasive censorship. The campaigns on behalf of the Egyptian blogger Maikel Nabil Sanad and Syria's Razan Ghazzawi have transcended international borders. The hashtag #OpSyria, started by Telecomix – a decentralised network of net activists committed to freedom of expression – has allowed Syrians to broadcast videos of the crackdown.

Last year also saw the development of tools to bypass censorship and blocking of Web access, such as "Internet in a suitcase" and FreedomBox. Cyber freedom activists are working flat-out to respond to increasingly effective censorship tools.

Diplomats enter the picture

Freedom of expression on the Internet is no longer the sole preserve of dissidents, geeks and censors. Diplomats have followed in their wake. Statements and joint texts issued by international organizations and coalitions of countries on Internet freedom have multiplied, from the report by Frank La Rue, the UN special rapporteur for the promotion and protection of freedom of opinion and expression, who last June acknowledged Internet access as a basic right, to the ruling by the European Court of Justice condemning Internet filtering and its adverse effects on freedom of expression.

At a meeting of the U.N. Human Rights Council in late February, the high commissioner for human rights, Navi Pillay, deplored restrictions on the Internet and the arrests of bloggers in some countries. She declared: "The Internet has transformed human rights movements. States can no longer exercise control based on the notion of monopoly over information."

The U.S. secretary of state, Hillary Clinton, urged the Organization for Security and Cooperation in Europe to approve a statement guaranteeing online freedoms, believing "rights exercised in cyberspace deserve as much protection as those exercised in real space".

For their part, China, Russia, Tajikistan and Uzbekistan defended the principle of a code of good conduct for the Internet, a concept that in reality is aimed as legitimizing censorship.

Democracies have a poor record

Some democratic countries are far from blameless. The free flow of news and information online often loses out to internal security, the war on terrorism and cyber crime, and even the protection of intellectual property.

Monitoring of the Internet has been stepped up in India since the 2008 attacks in Mumbai. Russia habitually describes sites that do no more than criticize the Kremlin as "extremist" to justify closing them down. Canada has approved repressive Internet legislation under the label of the fight against paedophilia.

The United Kingdom, whose Digital Rights Bill aimed at protecting copyright has been singled out by U.N. Commissioner La Rue, went through a difficult period during the riots last August. In a worrying development, the Canadian company Research In Motion, manufacturers of the Blackberry, made the personal details of some users available to the police without a prior court order.

Despite international condemnation and the fact that its laws are outdated, France still applies the Loppsi Internet security law, which provides for official filtering of the Web, and the Hadopi law, which allows for Web access to be cut off to prevent illegal downloading of copyright content, despite several unsuccessful cases. Decrees ordering the application of other laws show that the usual reaction of the authorities is to impose filtering. Australia has yet to scrap its national filtering system, despite waning support and the fact that the type of content it is designed to cover may change.

Speeches by U.S. officials on the importance of the fight against online censorship and their financial support for anti-censorship tools is belied by the treatment of WikiLeaks (see the Reporters Without Borders report on the United States and the Internet). Using Visa and MasterCard to cut off its access to funds has hampered the site's operations. Bradley Manning, suspected of being one of WikiLeaks' informers, has been detained for several months in dreadful conditions. The founder of WikiLeaks, Julian Assange, is the subject of "secret charges" which Reporters Without Borders urges the U.S. authorities to clarify.

Response of Internet users and netizens of the "free world"

Internet users in Western countries cut their teeth with the Occupy Wall Street movement. An even bigger number took to the streets to protest against the repressive U.S. Stop Online Piracy Act (SOPA) and Protect IP Act (PIPA), which sacrificed Internet freedom for the sake of copyright protection. The operation Stop SOPA and the 24-hour blackout observed by many websites, including Wikipedia, mobilised Web users throughout the world who were potentially affected by these bills to an unprecedented extent.

The campaign took off again with a new wave of protest against the Anti-Counterfeiting Trade Agreement (ACTA), which up till then had left most people indifferent despite campaigns by the NGOs La Quadrature du Net and Reporters Without Borders. Netizens from all sides understood that these bills could affect on their day-to-day activities.

Eastern Europe spearheaded the campaign. Several governments held off ratification. Resistance to ACTA is stronger than ever and the treaty may not see the light of day. Vigilance must be maintained. The next target for Internet activists could be the Intellectual Property Rights Enforcement Directive (IPRED), proposed by the European Union to clamp down on infringements of intellectual property law, which could potentially lead to large-scale filtering of the Internet. Another blow for Web neutrality.

Internet sovereignty and fragmentation of the Web

Internet sovereignty is an idea that is gaining ground in the minds of national leaders, whether repressive or not. Others have followed the example of the national platform created in Burma in 2010. Several times in 2011, Iranian President Mahmoud Ahmedinejad, true to his nationalist policies, announced the creation of a national Web, an Islamic "halal" version of the Internet with its own search engine and messaging service. This may mean two different types of access, one for the authorities and another for the rest of the population, similar to the way the Internet is now structured in Burma. Belarus requires commercial companies to register the websites they have set up in the country. This does not affect news and information sites for the time being.

Some countries such as North Korea, Turkmenistan, Uzbekistan and Cuba, and also Iran, censor Internet access so effectively that they restrict their populations to local intranets that bear no resemblance to the World Wide Web. The decision by Twitter among others to apply location-specific censorship confirms the tendency to fall back on national Webs.

In 2011, the fragmentation of the Internet gathered pace. Web users were granted varying access depending on where they were connected. This is contrary to the original concept of the founders of

the Web. Digital segregation is spreading and the "global village' is breaking up into a multitude of small landlocked neighbourhoods.

THE 2012 LIST OF THE ENEMIES OF THE INTERNET

Bahrain and Belarus move from "under surveillance" to "Enemies". Libya and Venezuela had been dropped from the list of countries "under surveillance" while India and Kazakhstan have been added to it.

Bahrain and Belarus, new Enemies of the Internet

Two countries, Bahrain and Belarus, have been moved from the "under surveillance" category to the "Enemies of the Internet" list, joining the ranks of the countries that restrict Internet freedom the most: Burma, China, Cuba, Iran, North Korea, Saudi Arabia, Syria, Turkmenistan, Uzbekistan and Vietnam. They combine often drastic content filtering with access restrictions, tracking of cyber-dissidents and online propaganda. Iran and China, in particular, reinforced their technical capacity in 2011 and China stepped up pressure on privately-owned Internet companies in order to secure their collaboration.

Iran has announced the launch of a national Internet. Iran and Vietnam have both launched a new wave of arrests, while the bloody crackdown on protests in Syria is hitting netizens hard and is enabling the regime to perfect its mastery of online surveillance with Iran's help. Turkmenistan has fought its first battle in the war over Information 2.0 while North Korea, which is developing its online presence for propaganda purposes, is confronted with an increase in smuggling of banned communications equipment across the Chinese border. In Cuba, bloggers supportive of the government and those critical of the regime argue online.

Saudi Arabia has continued its relentless censorship and suppressed coverage of a provincialuprising. Uzbekistan took measures to prevent Uznet from becoming a forum for discussing the Arab springs. There is one light of hope: the situation is improving in Burma, where the military have permitted the release of journalists and bloggers and the unblocking of news websites, but the legislative and technical tools for controlling and monitoring the Internet have yet to be dismantled.

Bahrain offers an example of an effective news blackout based on a remarkable array of repressive measures: keeping the international media away, harassing human rights activists, arresting bloggers and netizens (one of whom died in detention), smearing and prosecuting free speech activists, and disrupting communications, especially during the major demonstrations.

In Belarus, President Lukashenko's regime has increased his grip on the Web as the country sinks further into political isolation and economic stagnation. The Internet, a space used for circulating information and mobilizing protests, has been hit hard as the authorities have reacted to "revolution via the social media." The list of blocked websites has grown longer and the Internet was partially blocked during the "silent protests." Some Belarusian Internet users and bloggers have been arrested while others have been invited to "preventive conversations" with the police in a bid to get them to stop demonstrating or covering demonstrations. The government has used Twitter to send messages that are meant to intimidate demonstrations, and has diverted those trying to access the online social network Vkontakte to sites containing malware. And Law No. 317-3, which took effect on 6 January 2012, reinforced Internet surveillance and control measures.

Movement in "countries under surveillance" list

The countries "under surveillance" list still includes Australia, whose government clings to a dangerous content filtering system; Egypt, where the new regime has resumed old practices and has directly targeted the most outspoken bloggers; Eritrea, a police state that keeps its citizens away from the Internet and is alarmed by its diaspora's new-found militancy online and on the streets of foreign cities; France, which continues a "three-strikes-and-you're-out" policy on illégal downloading and where filtering without reference to the courts is envisaged by an internal security law and appears with increasing frequency in decrees implementing laws; and Malaysia, which continues to harass bloggers (who have more credibility that the traditional media) in the run-up to general elections.

The "under surveillance" list also includes Russia, which has used cyber-attacks and has arrested bloggers and netizens to prevent a real online political debate; South Korea, which is stepping up censorship of propaganda from its northern neighbour and keeps an array of repressive laws; Sri

Lanka, where online media and journalists continue to be blocked and physically attacked; Thailand, where the new government sends bloggers to prison and is reinforcing content filtering in the name of cracking down on lèse-majesté; Tunisia, where freedom of expression is still fragile and content filtering could be reimposed; Turkey, where thousands of websites are still inaccessible, alarming filtering initiatives have been taken and netizens and online journalists continue to be prosecuted; and the United Arab Emirates, where surveillance has been reinforced preventively in response to the Arab Spring.

Venezuela and Libya no longer under surveillance

In Libya, many challenges remain but the overthrow of the Gaddafi regime has ended an era of censorship. Before his removal and death, Col. Gaddafi had tried to impose a news blackout by cutting access to the Internet.

In Venezuela, access to the Internet continues to be unrestricted. The level of self-censorship is hard to evaluate but the adoption in 2011 of legislation that could potentially limit Internet freedom has yet to have any damaging effect in practice. Reporters Without Borders will nonetheless remain vigilant as relations between the government and critical media are tense.

India and Kazakhstan, new additions to the "under surveillance" category

Since the Mumbai bombings of 2008, the Indian authorities have stepped up Internet surveillance and pressure on technical service providers, while publicly rejecting accusations of censorship. The national security policy of the world's biggest democracy is undermining freedom of expression and the protection of Internet users' personal data.

Kazakhstan, which likes to think of itself as a regional model after holding the rotating presidency of the Organization for Security and Cooperation in Europe in 2010, nonetheless seems to be turning its back on all its fine promises in order to take the road of cyber-censorship. An unprecedented oil workers strike, a major riot, a strange wave of bombings and the president's ailing health all helped to increase government tension in 2011 and led to greater control of information, especially online information: blocking of news websites, cutting of communications around the city of Zhanaozen during the riot, and new, repressive Internet regulations.

Thailand and Burma may be about to change places

If Thailand continues down the slope of content filtering and jailing netizens on lèse-majesté charges, it could soon join the club of the world's most repressive countries as regards the Internet.

Burma could soon leave the Enemies of the Internet list if the country takes the necessary measures. It has clearly embarked on a promising period of reforms, which has included the release of journalists and bloggers and the restoration of access to blocked websites. It must now go further by abandoning censorship altogether, releasing the journalists and bloggers still held, dismantling the surveillance apparatus that was built on the national Internet platform, and repealing the Electronic Act.

Other countries to watch

Other countries have jailed netizens or established a form of Internet censorship. Even if they are not on these lists, Reporters Without Borders will continue to closely monitor online freedom of information in countries such as Azerbaijan, Morocco and Tajikistan, to name just a few.

At the time of writing, Pakistan has invited private-sector companies to bid for the creation of a national Internet filtering and blocking system. Reporters Without Borders has asked the authorities to abandon this project, which would result in the creation of an Electronic Great Wall. If they go ahead, Pakistan could be added to the Enemies of the Internet in 2013.

BAHRAIN

ENEMY OF THE INTERNET

Bahrain offers a perfect example of successful crackdowns, with an information blackout achieved through an impressive arsenal of repressive measures: exclusion of the foreign media, harassment of human rights defenders, arrests of bloggers and netizens (one of whom died behind bars), prosecutions and defamation campaigns against free expression activists, disruption of communications.

Use of filtering intensified in reaction to political unrest

Although the country has used filtering for years to target political and religious contents (see the Bahrain chapter of the 2011 "Enemies of the Internet" report), since February 14, 2011 – starting date of the rebellion – it has bolstered its censorship efforts in reaction to the unrest destabilizing the Arab world.

According to Arbor Networks, Internet traffic to and from Bahrain, as of mid-February 2011, allegedly dropped by 20% compared to the three preceding weeks, which points to increased filtering being used in response to the events occurring in the country. High-speed Internet access was slowed down to hamper the real-time uploading and circulation of videos and photos taken during protests and crackdowns. Authorities wanted to target some accounts on streaming platforms such as Bambuser and social networks, and blocked YouTube and Facebook pages posting videos of the events. A few months later, its was PalTalk's turn to be blocked. This online audio and video chat group service had a community chatroom, "Bahrain Nation," that dissidents used to send messages. The website twitcam.livestream.com designed to allow Internet users to circulate real-time information on Twitter, was also blocked.

On the eve of the first anniversary of the Bahrain uprising, in February 2012, the authorities launched a new wave of repression, blocking independent news sites and notably streaming websites, and once again slowed down bandwidth speeds. The live973.info site, which was streaming real-time footage of an opposition demonstration, was blocked, as was the "Wefaq live" page of the audio-streaming site mixlr.com. Access to the iPhone/iPad app via Live Station's website was also closed off from Bahrain. This app had made broadcasting possible for TV channels such as Lualua TV, jammed since its launch on 17 July 2011. On February 11, the site Witnessbahrain.org, which had been denouncing abuses, was blocked and its activists arrested. The few deblockings of registered political group websites, Aldemokrati.org, Alwefaq.org and Amal-islami.net, that occurred in early 2012 were nothing but a smokescreen.

Surveillance was also strengthened and expanded to include human rights activists and their close friends and relatives. Nokia Siemens Network (NSN) was accused of sharing private netizen data with the authorities.

Waves of arrests, deaths while in detention, and mock trials

In addition to taking these technical measures the number of arrests of netizens and cyberdissidents has soared since February 2011. In September 2011, Bahrain's Interior Minister announced that anyone posting online messages calling for demonstrations or inciting dissidents to take action could end up in prison. He kept his promise. Among the netizens arrested and later released in recent months are: bloggers Abbas Al-Murshid, Mohamed Al-Maskati and Ali Omid, as well as forum administrators and moderators Fadel Al-Marzouk, Hossein Abdalsjad Abdul Hossein Al-Abbas, Jaffar Abdalsjad Abdul Hossein Al-Abbas, Hamza Ahmed Youssef Al-Dairi, Ahmed Youssef Al-Dairi, Fadhel Abdulla Ali Al-Marzooq, Hani Muslim Mohamed Al-Taif, and Ali Hassan Salman Al-Satrawi. Also on the list of arrested netizens is Hussein Ali Makki, administrator of the Facebook and Twitter pages of Rasad News, a major news source on human rights violations in Bahrain, who was arrested on June 9, 2011. Not to mention blogger and activist Zainab Al-Khawaja (@angryarabiya). Blogger and human rights activist Sayid Yousif Al-Muhafdah has also been reported missing since March 19.

The crackdowns have also entered the courts: on June 22, 2011, a military court gave 21 human rights activists and opposition members harsh prison sentences, upheld on appeal on September 27 after a mass trial intended to serve as an example and impress dissidents. Among those tried was blogger **Abduljalil Al-Singace**, Director of the Al-Haq Movement's Human Rights Bureau, who received a life sentence. Well-known blogger **Ali Abdulemam**, thought of as one of Bahrain's Internet pioneers, was sentenced in absentia to 15 years behind bars.

A series of pressures and attacks on journalists, bloggers, and activists has led to increased self-censorship. While seemingly trivial, the following reveals the true situation in the country: several dozen students were expelled from a prestigious school for liking a Facebook page. Worse still, was the intimidation campaign led against Bahraini bloggers and human rights activists. Their pictures were circulated online with the caption "traitors." **Nabeel Rajab**, Director of the Bahrain Center for Human Rights, is on the front line. Prosecuted and repeatedly assaulted, and despite intense pressure, he continues to denounce the repression that is still rife in Bahrain.

One of these cyberdissidents – yet another victim of regime repression – lost his life. On April 9, 2011, netizen **Zakariya Rashid Hassan** died while in detention, probably after having been tortured after his arrest for "inciting hatred," "disseminating false news," "promoting sectarianism," and "calling for the regime's overthrow in online forums." At first, the authorities denied their responsibility, claiming that he had died from sickle-cell anemia. Then an investigation was opened in early January 2012. Two officers accused of having beaten him to death face up to seven years behind bars.

Cynicism shown by the authorities and the international community

The way in which this crisis has been managed exemplifies the authorities' hard-line cynicism and two-sided discourse, since they are calling for national dialogue and claim to have accepted, in late November 2011, the critical conclusions of an independent investigative commission, yet they continue to wage reprehensible crackdowns on the almost daily protests troubling the Kingdom. Reporters Without Borders has been urging the international community to react by sending a United Nations' special rapporteur to Bahrain.

The money spent by the regime to improve its reputation and the reluctance of the United States to criticize this country in which it has its main Middle East military base has helped to squelch talk about the events and their repression. The Bahrain Formula 1 Grand Prix, which is scheduled to take place in April 2012, should be the highlight of the communication campaign's offensive launched by the authorities. It would be a golden opportunity for the regime to regain its prestige and make people believe in an illusory return to normal.

BELARUS

ENEMY OF THE INTERNET

While Belarus sinks into political isolation and an economic slump, President Lukashenko's regime has been strenghtening its grip on the Web. The Internet – a mobilization and information platform – has received the full brunt of the authorities' brutal crackdown on the opposition.

The Internet has played a crucial role in a climate marked by intensified censorship and a hunt for journalists. Foreign – and particularly Russian – reporters are now personae non gratae. Some 100 Belarusian journalists were interrogated in 2011 alone, and over 30 given prison terms, as were **Irina Khalip**, correspondent for the independent Russian newspaper *Novaya Gazeta*, and **Natalia Radzina**, editor of the Charter97.org website, who was forced to seek asylum in Lithuania. Pressures on netizens and the number of cyberattacks on the media have been multiplying. Surveillance has become routine.

Internet filtering, provided for by Decree 60 (see the Belarus chapter of the 2011 "Enemies of the Internet" report) has increased. The blacklist of blocked websites, which has been steadily growing since the unrest of December 2010, now includes the news website Charter97.org, the opposition website belaruspartisan.org, the human rights NGO Viasna's website, and humorist Yauhen Lipkovich's blog on LiveJournal.

Crackdown intensified in times of unrest

In December 2010, demonstrations against the re-election of Lukashenko led the regime to intensify its crackdown. A new series of destabilizing events induced it to try to impose a genuine blackout on media coverage of the Minsk metro bombing in April 2011. Journalists deemed too focused on the investigation were labeled "scoundrels" and "criminals," and were accused of "disseminating false information" and "defamation." The Charter97.org and belaruspartisan.org websites, known for their criticisms of government policy, were the target of cyberattacks. On 12 April 2011, Belarusian Prosecutor General Grigory Vasilevitch set the tone by openly declaring that he wanted "to restore order" on the Web.

In June and July 2011, peaceful anti-regime demonstrations were harshly repressed: hundreds of people were arrested, including dozens of journalists, and the Internet was partially blocked during "silent protests" without slogans or banners, which took place throughout the country. In addition to denouncing the regime itself, participants objected to deteriorating living conditions and the devaluation of their currency. The "Revolution through Social Networks" campaign, widely circulated on Twitter via hashtag #2206v1900 and on the Russian-language version of Facebook, Vkontakte, spread like wildfire.

Intimidation and "preventive conversations"

In view of the mobilization's magnitude, Belarusian authorities began to take the offensive on the Internet. The "Revolution through Social Networks" group, which boasted 216,000 members, was shut down by Vkontakte just before the 3 July 2011 protests. It reopened the next day at a new address, losing many participants in the process. The Vkontakte website was blocked for several hours on 13 July 2011 by several Internet Service Providers (ISPs), including ByFly. On 3 July, the Belarusian service website of *Radio Free Europe/Radio Liberty* was hit by a distributed denial of service attack (DDoS) that shut it down for several hours.

Under pretense of a "friendly get-together," the police invited some netizens to "preventive conversations" in order to persuade them to stop protesting and covering the protests. Despite these pressures, many blogs and online media such as euroradio.by, Babruiski Rehiyanalny Portal (in Babruisk), Silnye Novosti (in Gomel), and Ximik.info (in Novopolotsk) covered the demonstrations. Youtube actively relayed video clips of the events.

Not only did the government censor online protests, but it also used the Web to intimidate demonstrators: for example, the Interior Ministry – who created its Twitter account (@mvd_by) in April 2011, later followed by the Minsk Police Department (@GUVD_Minsk) – did not hesitate to tweet

warning messages during the demonstrations: "To all persons going to the city square (...): you will have to answer for it." In addition, the Belarus ISP BelTelecom redirected netizens trying to connect to Vkontakte to sites containing malware. From early May to early June 2011, at least seven websites were shut down at the request of the police, who had been granted new prerogatives by the Law of March 1, 2011.

The authorities pursued the offensive through legislation. Following Decree 60 of February 2010, Law 317-3, which took effect in Belarus on 8 January 2012, reaffirmed Internet surveillance and reinforced Net censorship in Belarus with a repressive arsenal. Already included among the main provisions of Decree 60 of February 2010 was the obligation of ISPs and cybercafés to collect Internet users' personal data and conduct citizen surveillance, and the option for authorities to order the blocking of any site deemed "extremist" (a vague definition which regularly leads to the overblocking and closure of opposition websites). The new law provides sanctions against those who violate such provisions. Although non-commercial entities do not seem to be directly affected by the part of the law which requires Belarusian company websites to be hosted or duly registered in the country, the authorities may still draw up a list of banned sites controlled by state bodies.

In January 2012, the European Union strengthened its sanctions against certain Belarusian individuals and entities by subjecting them to travel restrictions and a potential assets freeze. The regime cannot resolve the country's problems by sinking into a repressive hysteria that would only exacerbate tensions. It is urgent for it to hear the international community's appeals to reason and put an end to its aimless repression and war on information.

BURMA

ENEMY OF THE INTERNET

The recent and relative opening of the Burmese regime has resulted in information being more freely circulated on the Internet, despite continued close monitoring. The international community and Burmese human rights activists need to remain vigilant and keep striving for more freedom. One priority is to reform the liberticidal legislative framework. While much progress is still needed, the reforms already underway would be difficult to reverse.

The Thein Sein era is off to a troubling start for Internet freedoms

In March 2011, President Thein Sein stated in his inaugural address that the media's role must be respected. However, the already severe restrictions imposed on cybercafés (see the Burma chapter of the 2011 "Enemies of the Internet" report) were tightened in May 2011. The use of external hard drives, USB flash drives and CDs were banned, as was the use of Internet telephony services (VoIP) to make international calls – a measure apparently meant to further isolate dissidents.

Journalists and bloggers released, websites unblocked

In the last few months, a series of amnesties has allowed thousands of detainees, including hundreds of prisoners of conscience, to be released. Among them were journalists and bloggers. All journalists working for the Democratic Voice of Burma (DVB), including **Hla Hla Win, Ngwe Soe Lin, Win Maw, Sithu Zeya** and his father **U Zeya**, as well as freelance journalists **Thant Zin Aung** and **Zaw Thet Htwe** and blogger **Nay Phone Latt**, were released, the last of them in January 2002. Blogger and comedian **Zarganar** had been released in October 2011.

Several Internet news websites, including YouTube, *BBC*, *Reuters*, *The Bangkok Post*, *Straits Times, Radio Free Asia, Irrawaddy, Democratic Voice of Burma (DVB),* and the Burmese version of *Voice of America* were unblocked right after the visit of the United Nations' special rapporteur on the situation of human rights in Burma, which coincided with the International Day of Democracy.

Between optimism and vigilance

In November 2011, Reporters without Borders interviewed renowned dissident Aung San Suu Kyi during a video conference held in the United States by the Council on Foreign Relations on the status of media freedom in Burma. She stated, "The situation has gradually improved," and said that the authorities are starting to "make concessions," adding "I think that this détente applies to everyone in general." Since September 2011, her name can be published in the media.

Nay Phone Latt, who – along with Zarganar – won Reporters Without Borders' Blogger Award, said in an interview granted to Reporters Without Borders after his release in January 2012, that the new media and bloggers had helped bring political change in Burma, but also cautioned, "We are not yet free. (..) The repression is still going on." During his talk on the *France 24* TV station, he had confided: "I cannot help but find the swiftness of these changes troubling." He also recalled: "It is now possible to use Gmail, read blogs, go on Facebook, and visit news sites, but the laws governing restrictions and authorized websites still exist and must be repealed. (...) We will not be completely safe as long as there is no law to protect freedom of expression."

In fact, in order for reforms to take hold and to avoid any setback, the entire legal framework needs to be revised. One positive sign is that the authorities have promised to adopt in 2012 a media law that will put an end to censorship. They are then expected to revise or repeal the Electronic Act and emergency rule. Some individuals are still being arrested under the Unlawful Association Act, or treason charges.

Although certain key opposition figures such as Min Ko Naing and Ashin Gambira have been released, blogger **Kaung Myat Hlaing (Nat Soe)**, imprisoned since April 2010, and four other journalists remain behind bars, as do more than 450 political prisoners, according to National League for Democracy's estimates. Others, like *DVB* journalist **Sithu Zeya**, have been granted a conditional release but may be returned to prison at any time if, for example, they send a photo to the *DVB*. Some

feel that these amnesties were inadequate and that the government is using the remaining prisoners as hostages in their negotiations with the international community.

The very structure of the new Burmese Internet as modified in 2010 gives the authorities more surveillance options, while reserving the fastest and best-quality access for the government and military, according to an exclusive report issued by Reporters Without Borders and the Burma Media Association. Undetectable sniffers may be placed on the public's ISP to retrieve various confidential user information. The authorities need to show proof of transparency and authorize an independent audit of the infrastructure that would outline the needed changes in order to reassure users and rid the platform of abusive surveillance tools. They also need to explain their plans for ISPs Myanmar Post and Telecommunication (MPT) and Yatanarpon, what control the State will continue to exert on these two structures and the possibilities and conditions for privatization. Burma's use of Blue Coat technologies, observed on the Yatanarpon Teleport ISP, is raising questions about the company's filtering policy and how it might be used for Internet surveillance.

Several reports attest to a very slow bandwidth speed – so slow that the Eleven Media group recently launched a news via SMS system to better meet its readers' needs.

The regime also needs to extend Internet access to the whole population. Currently, just 1% of the latter enjoys Internet access, and the country only has about 500 cybercafés, mainly in large cities.

The streamlining of Burma's (primarily trade) relations with the West remains a key factor in accounting for the recent changes made by the Burmese regime, which is anxious to climb out of its economic slump and offset the hegemonic Chinese influence.

For many years, Burma has coveted the Association of Southeast Asian Nations (ASEAN) presidency. The reforms undertaken guarantee that it will win it for the year 2014. An easing of U.S. sanctions could take place shortly, but Congress is still highly critical of the regime and pushing for more reforms and a democratic transition. The eyes of the world are on Burma in the run-up to its April 2012 by-elections.

CHINA

ENEMY OF THE INTERNET

The soaring expansion of the "Participative Web" and related impact on social and political debates are making it harder each day for Chinese censors to do their job. Harsher controls and crackdowns on netizens and their online tools have been symptomatic of the regime's increasing concern over potential fallouts from Arab Spring and the Internet and social networks' role as sounding boards.

Obsessive controls to counter the specter of Arab Spring

China may have the world's most sophisticated online censorship and surveillance system, but it has been pushed to its limits to thwart any risk of contagion from protest movements, mainly by removing most references to Arab Spring and "Occupy Wall Street" movements from the Chinese Net (see the China chapter of the 2011 "Enemies of the Internet" report). Some blogs and microblogs have been shut down, and keywords such as "jasmine" or "Egypt" banned. It is now impossible to use the word "occupy" followed by the name of a Chinese city (ex.: "Occupy Beijing" (占领北京) in a Web search.

The Chinese Communist Party's plenary session officially devoted to "cultural reforms" was in reality an occasion for the government to legislate again on Web censorship. The CCP adopted a directive aimed at preserving "security" and expanding the Chinese culture's "influence." These repressive measures were justified by the need to maintain a "healthy Internet" for future generations. The law that prohibits the spreading of "rumors" actually serves as a pretext for the Chinese government to muzzle dissident voices and indulge in arbitrary arrests.

The regime has also required public Wi-Fi access providers to install extremely expensive Internet user tracking software. In addition to reinforcing their control of Internet traffic, the authorities are now imposing a form of economic censorship by forcing cybercafés to stop offering Wi-Fi access if they cannot afford the software.

Invited to "have tea"…

… which is actually a euphemism for being summoned to the police station, for censorship is now being combined with waves of blogger and netizen arrests. Arbitrary detentions, unfair trials, repressive regulations and harsh sentences have recently multiplied, taking special aim at cyberdissidents. Seventy-eight of them are still in jail for their online activities, making China the world's biggest prison for netizens. Its victims include:

- Nobel Peace Prize winner **Liu Xiaobo**, who is still behind bars;
- Cyberdissidents **Chen Xi** (陈西) and **Chen Wei** (陈卫), respectively sentenced to 11 and 9 years for "subversion";
- Cyberdissident **Li Tie**, who received a 10-year sentence for subversion;
- **Liu Xianbin**, sentenced to a 10-year term for "inciting subversion of the government";
- Human rights activist and cyberdissident **Govruud Huuchinhuu**, beaten while in detention;
- Lawyer **Ni Yulan** (倪玉兰) and her husband **Dong Jiqin** (董继勤), awaiting sentencing;
- Netizen **Hu Di** (**胡荻**), forcefully interned in a psychiatric ward.

Those released, such as **Ai wei wei**, **Wang Lihong** (王荔蕻), **Zheng Yichun** (郑贻春), **Ding Mao** (丁矛), **Ran Yunfei** (冉云飞), **Wang Yi**, **Chen Guangcheng** and **Hu Jia**, are often victims of persecution, subjected to constant surveillance and even placed under house arrest.

Blogger and activist **Wen Yu Chao**, based in Hong Kong, who takes courageous pro-freedom of expression stands on the Chinese Internet, has been repeatedly harassed. His Gmail account has been hacked several times and photo montages designed to destroy his reputation have been circulating on the Internet.

The family of lawyer and human rights activist Gao Zhisheng, who has been missing since April 2012, fear the worst. In early January 2012, the activist's brother Gao Zhiyi was informed by a court notice

that Zhisheng was being detained in a western Xinjiang jail. But close relatives who went to the jail were not permitted to see him.

Microblogging sites soar

According to official figures, by year-end 2011, China had 513 million Internet users; i.e., an Internet penetration rate of 38.3%. Some 356 million of them are said to access the Internet via their mobile phone, half of whom (250 million) have microblogs. The Techrice blog publishes a list of 15 of the most popular social networks, as well as their stated and likely number of users.

The microblog revolution, sharing of opinions, and increased circulation of news resulting from microblogs have led the regime to take certain measures. The police accused Chinese Twitter ("Weibo") of having a "bad influence on society." Chinese Internet leaders such as Sina Corp (which owns the Sina Weibo microblogging website), Baidu (search engine) and Tencent (owner of the QQ messaging service), agreed in November 2011 to implement the government directives on online surveillance. These businesses promised to combat online pornography, Internet fraud, and the dissemination of rumors and false reports. The microblogs had already been asked to have moderators, but that has apparently proved inadequate.

Next step**:** Chinese authorities have been targeting anonymity on microblogging websites. As of March 16, Chinese netizens registering on microblogging sites hosted in China will be required to use their real names instead of an alias. If they do not comply, they will only be allowed to consult other contributors' microblogs, but will not be able to actively participate. The terms under which this identification system (实制, "shimingzhi") will be applied to all platforms concerned are still unknown.

News blackouts thwarted by social networks

China's censorship apparatus has done its utmost to suppress reports on an uprising in the small city of Wukan, in the province of Canton. The local authorities violently repressed demonstrations against farmland seizures, and following the death of their leader, thousands of citizens took to the streets to continue protesting against the expropriations and to demand justice, while also using social networks to expose their situation. The authorities imposed a genuine offline and online news blackout of the town. They blocked the keyword "Wukan" on the Internet, closely monitored "hot tweets" and removed all images and videos showing the population's demonstrations from the Sina and Tencent Weibo microblogging websites. Since the villagers had managed to make their grievances heard and to rally public support, thanks to the Internet, Beijing had to agree to negotiate with them. Lin Zulian, who had led the insurgents, was appointed local Communist Party chief on January 16, 2012.

In July 2011, the Propaganda Department attempted to impose severe restrictions on media coverage of the high-speed train crash that occurred on the 23rd of that month in Wenzhou, leaving some 40 people dead. It ordered "*all media including newspapers, magazines and websites to give priority to reports from the authorities on the positive aftermath of the train disaster."* In reaction, critics rushed onto the Web and millions of comments on Weibo demanded explanations about train safety in China.

Online mobilization campaigns continue: Some examples

In the city of Dalian, tens of thousands of demonstrators mobilized thanks to messages distributed on Weibo opposing a chemical plant. The later was moved.

The "guardian of Lake Tai," Wu Lihong, was arrested for his activism, particularly online, in denouncing pollution. He is still under close surveillance. His Internet connection was cut off, but his efforts induced the authorities to take steps to improve the lake's water quality.

During Ran Yunfei's detention, Twitter users created a blog on which they circulated English translations of the cyberdissident's writings.

A powerful online mobilization campaign on behalf of Ai Weiwei was organized to help him pay the 15.22 million yuan (about USD 2.4 million) fine imposed on him by the authorities for tax evasion. He managed to scrape together half of it through an Internet fundraiser to which 20,000 people

contributed. Many netizens posted nude shots of themselves online when Ai Weiwei was charged with "pornography" because of a single photo.

Regional discrimination: Localized censorship

In response to the unrest in Inner Mongolia and Tibet, the regime stepped up its repression:
.
In late January 2012, a communications blackout was imposed to prevent media coverage of the authorities quashing protest movements in Tibet. The independent and foreign media were kept in the dark, while disinformation prevailed in order to hide from the world the magnitude of the protest. The Internet was a collateral victim of the crackdown, with cut-off connections, increased blockings, and removals of content related to the uprisings. Local community networks were particularly targeted in order to nip in the bud any attempt at mobilizing support online. Tibetan exile media organization websites are still inaccessible, as are Tibetan-language blogs and discussion forums such as Sangdhor.com and Rangdrol.net.

The Chinese authorities' strategy of cutting off certain provinces or regions from the media and the Internet in order to subdue them in silence is not new. Tibet has already been the target of harsh restrictions on communications. Xinjiang was cut off from the outside world for several months after interethnic riots in 2009.

In May 2011, the Internet was also a victim of the crackdown on the Inner Mongolia demonstrations, as the authorities stepped up their control following protests about the death of a Mongol herdsman on October 20, 2011. Many Mongolian websites called for demonstrations against the government's attempts to impose a news blackout on the event, and access to several sites such as Boljoo, Mongolian BBS and Medege were blocked as of October 27, 2011. Cyberdissident **Hada** and his family are still in jail, and their close relatives are being harassed.

Official strategy: Propaganda, cyberwar and refusal to accept any interference

Following the protests triggered in Mongolia by the death of a herdsman, propaganda messages likely posted by government-hired bloggers known as "50 cents" have mushroomed online. One such post read: "Dear fellow students and friends, it was just a traffic accident. Some people with their own agendas are interpreting it as an ethnic problem or saying it has something to do with oil and natural gas development. The government is taking the case very seriously (....). We hope that our fellow students will not believe the rumors (...)".

The authorities are trying to have the last word: they claim to have 40,000 micro-blogs on which to publish "approved" news and welcome netizens' comments.

The Chinese Army has set up an elite unit responsible for thwarting cyberattacks according to the daily *Global Times*, cited by *Agence France-Presse*. In August 2011, McAfee security experts exposed a series of large-scale cyberattacks that had been occurring since 2006. Once again, China is strongly suspected. It is thought to be behind attacks against Google. In mid-August 2011, after the self-immolation of a young monk, Chinese authorities may have also initiated a wave of cyberattacks against the Tibetan media.

The regime launched an offensive against censorship-circumventing software programs, which are used more and more in China, as pointed out by Global Voices. The Great Firewall is now thought to be capable of controlling the data flow from local IP addresses and simultaneously restricting the number of IPs authorized to connect to the international network. Multinational companies have supposedly sent internal communications to their employees instructing them not to use VPN and not to visit foreign websites unless they are related to their work.

On October 19, 2011, aware of the economic impact of Net censorship, the United States demanded clarifications concerning "Internet restrictions in China," which violate World Trade Organization (WTO) rules. The Chinese Foreign Affairs spokesperson, Jiang Yu, rejected the U.S. demand, stating: "We do not accept using the excuse of 'Internet freedom' to interfere in other countries' internal practices," she said, adding that "The Chinese government promotes and actively supports the Internet and safeguards its citizens' freedom of expression."

While the Chinese government is not prepared to relax its painstakingly won grip on the Internet, it is increasingly overwhelmed by the immense potential of the Participative Web, and the tension between the regime and cyberdissidents is intensifying. The transition period now underway, expected to culminate in the fall of 2012 when Hu Jintao will be replaced by his successor Xi Jinping, back from an official visit to the United States, is unlikely to usher in an era of respite and – even less likely – a Chinese spring.

CUBA

ENEMY OF THE INTERNET

A digital cold war is being played out against a backdrop of demonizing the Internet and social networks, which are accused of having a destabilising influence and being orchestrated by the American enemy. Will the arrival of the Venezuelan fiber-optic cable call into question the "rationing" of the Internet, which remains out of reach for the majority of the population? The creation of a tightly controlled Cuban Web 2.0 tends to indicate that the regime has no intention of making any concessions with regard to communications.

Pressures and defamation campaigns against critical bloggers

Pro-government bloggers are waging a non-stop battle on the Internet against "alternative" bloggers critical of the authorities. The regime is preventing most of its citizens from gaining access to the Internet and is occupying the field in order to leave no cyberspace for dissidents (see the Cuba chapter in the 2011 "Enemies of the Internet" report). However, although less than 2% of Cubans have access to the World Wide Web, a growing number of them have found creative ways to connect with the Internet and visit the social networks.

In March 2011, an official documentary programme named the "Las Razones de Cuba" ("Cuba's Reasons") TV series was broadcast which accused critical bloggers, labelled as "cybermercenaries," of being manipulated by the United States, had been countered by the publication, on Viméo, of a dissident video entitled "Citizens' Reasons," in which blogger Yoani Sanchez explained that the "demonization of the Internet" was in full throttle because the government was "frazzled" and fearful that the Internet might play a role similar to that of the Arab Spring. The dissident later stated in an interview granted on 2 January to the Peruvian daily *El Comercio* that she was very "sceptical" about the likelihood of a Cuban protest movement of the sort observed in Tunisia or Egypt, in view of how "highly fragmented" Cuban society is and the "minimal" mobilisation capacity of its social networks.

Yoani Sanchez founded a school of bloggers to break the tight grip on information imposed by official news sources. Other bloggers such as Claudia Cadelo, Laritza Diversent and Orlando Luis Pardo Lazo have also taken the initiative to defend "digital freedoms" and the Cubans' right to be informed. The coverage of dissident Juan Wilfredo Soto Garcia's death by "alternative" bloggers offended a government already displeased that its official version was being challenged.

The authorities' strategy about social networks

In November 2011, the whole world witnessed what was probably the first direct confrontation between a member of the Cuban leader's family – in this case Mariela Castro, Raul Castro's daughter – and dissident Yoani Sánchez. In a baptism by fire on Twitter, Mariela Castro lost her composure while responding to the arguments of her critics, calling them *parásitos despreciables* [despicable parasites]. During an interview for *BBC Mundo*, Yoani Sanchez later praised the social networks' role as a dialogue facilitator: "On Twitter, no one gives lessons to anyone else. Presidents don't order citizens around and neither do major personalities bully ordinary people. They all learn from each other." She was once again prevented from leaving the country in February 2012.

On 1 December 2011, Cuba's Foreign Minister, Bruno Rodríguez, urged social networks to develop a new strategy which would allow them to rid themselves of the "dictatorship of the sector's large U.S. groups". A few days later, the government accused Twitter of having spread rumours about Fidel Castro's death.

Shortly afterwards, the regime launched RedSocial, a Cuban version of Facebook accessible only via the Cuban Intranet, Red Cubana. Conceived as "a virtual meeting place for Cuban academics," it is nonetheless a surveillance tool. In order to register, the user must provide his or her e-mail's password. This "Made in Cuba" social network boasted several thousand registered users by the end of 2011.

The undersea cable from Venezuela, a new hope?

Much more is at stake now with the arrival of the undersea Alba fiber-optic cable which will link Cuba and Venezuela, multiplying by 3,000 the island's capacity to connect to the rest of the world. Initially scheduled for the summer of 2011, its implementation was postponed without further explanation. In early 2011, the regime announced that this Web access would be reserved for "social use" by institutions, universities and certain professions such as doctors and journalists. It would also make it possible to continue setting up collective access centres. Contrary to expectations, in late January 2012, the Cuban Communist Party Congress carefully set aside the issue of Internet development.

Although no one is banking on the fact that certain cable fibres will be diverted towards the Internet access black market, others believe that the cable will not create new opportunities for Cubans who wish to connect to the World Wide Web. Since the latter is rationed, as is the rest of Cuba, the cable could only enhance connection quality and bandwidth speed for those who already have access. The regime remains ready to crush any attempt to bypass censorship. In November 2011, Cuba accused the United States of bolstering parallel Internet connections on the island by unlawfully importing equipment and making satellite connections available. An American citizen accused of involvement in these clandestine activities was arrested in December 2009.

IRAN

ENEMY OF THE INTERNET

The announced launching of Iran's "National Internet" has been widely covered in the media. Meanwhile the authorities have fortified filtering and their technical capacity to closely monitor the Web. Individuals and groups alike have been arrested in order to identify and neutralize dissident networks and intimate bloggers and journalists. For the first time, four netizens have been given the death penalty, and three of them may be executed at any time. Iran's already harsh repression has become even more brutal.

Sentenced to death for their online activities

This is the first time that netizens have been sentenced to death. On January 29, 2012, the Iranian *Farsnews* agency, with close ties to the Guardians of the Revolution, confirmed the sentencing to death of Web developer Saeed Malekpour, a permanent resident of Canada, for "anti-government agitation" and "insulting Islam."

In early 2012, Iran's Supreme Court also confirmed the death sentence for IT student Saeed Malekpour and website administrator Ahmadreza Hashempour. The Revolutionary Court's Fifteenth Chamber informed Web developer and humorist Mehdi Alizadeh that he had been sentenced to death.

These four netizens, who are between 25 and 40, are victims of a plot orchestrated by the Center for the Surveillance of Organized Crime, an entity created illegally in 2008 by the Revolutionary Guards. Under torture, the accused admitted having links with websites that criticize Islam and the Iranian government, and to having intended to "mislead" Iranian youth by distributing pornographic content. They were also forced to confess to participating in a plot backed by the United States and Israel.

Waves of arrests with no end in sight

These waves of arrests sometimes coincide with anniversary dates likely to generate unrest. They may also be tied to internal tensions between the various power circles. They can occur at unpredictable moments in order to mislead dissidents, disrupt their independent publications, and create a continuous climate of suspicion. The most recent series of arrests occurred in May and June 2011 during the anniversary of Mahmoud Ahmadinejad's disputed reelection, as well as in early 2012, just before the anniversary of the Islamic Revolution and the two widespread protests of February 14 and March 1, 2012.

Reporters Without Borders counted 29 netizen arrests between March 1, 2011 and March 1, 2012. Eleven netizens received sentences ranging from three to six years. Fifteen were released on parole. They are awaiting their trial and verdict with little hope for leniency.

In February 2012, Mehdi Khazali, son of an influential conservative religious leader, was sentenced to four years in prison for regularly posting criticisms of the Iranian president on his blog.

Sakhi Righi, whose blog is balochistan-s, was arrested on June 18, 2009 in his native city of Zahedan. His prison sentence was the harshest one ever served on a blogger in Iran – 20 years – for "publishing false information" and committing "acts against national security."

To learn more, read the articles about freedom of information violations in Iran since January 1, 2012, and in 2011.

Inhuman and degrading treatments, and pressures of all kinds

Detainees are repeatedly tortured and mistreated, and further victimized by defamation campaigns and forced confessions shown on Iranian TV.

Many arbitrarily detained journalists and netizens are being denied medical treatment for illnesses despite their physical and psychological deterioration. The state of health of the following detainees is

particularly worrying: **Masoud Bastani, Issa Saharkhiz, Mohammad Sadigh Kaboudvand**, **Hossein Ronaghi Maleki**, **Saeed Matinepour, Mehdi Mahmudian**, **Kivan Samimi Behbani,** and **Arash Honarvar Shojai**. Their very lives are at stake.

The authorities have not hesitated to harass relatives or separate families. **Parvin Mokhtare**, the mother of jailed blogger **Kouhyar Goudarzi**, was sentenced to 23 months in prison by a revolutionary court in the city of Kerman.

Those who are released on bail are forced to post exorbitant amounts of money. Blogger and women's rights activist **Parastoo Dokoohaki**, and **Sahamoldin Borghani**, a journalist who writes for the news website Irdiplomacy, were released at the end of February 2012. Arrested in January, they had been held in solitary confinement in Sections 209 and 2 A of Tehran's Evin prison, which are run by the Intelligence Ministry and the Revolutionary Guards. The journalists were freed after posting bonds in the amounts of 300 and 200 million tomans, respectively (USD 19,700 and USD 15,800).

The day before their release, the Revolutionary Guards' organized crime unit, in a statement posted on the Gerdab website, accused them of "collaborating with the *BBC*, British intelligence and the foreign-based opposition." The Revolutionary Guards had announced that an operation code-named "eye of the fox" had led to the breakup of an information-gathering network that produced content for the *BBC* en Iran. The British broadcaster denied that it had employed staff in Iran. Satellite stations such as the *BBC* and *Voice of America* had been jammed at regular intervals in Iran. On March 5, 2012, confessions of this operation's victims – for the most part excerpts from their interrogations – were broadcast on national TV channels and relayed by *Press TV*, the Islamic Republic's English-language station.

In early March 2012, a few days before Iran's "International Women's Day," the regime intensified its crackdown on cyberfeminists, including **Noushin Ahmadi Khorasani**, founder of the Feminist School website, and one of the women who organized the "One Million Signatures for Equality" campaign, which calls for reforming laws that discriminate against women. Cyberfeminists are frequent victims of threats and arrests.

Another sign of the authorities' intransigence was the regime's refusal to accept a visit from Ahmed Shaheed, the United Nations Special Rapporteur on Human Rights in Iran.

New regulations are bolstering Iran's legislative arsenal

At a news conference on December 28, 2011 – the day for registering candidates for the March 2012 parliamentary elections – Abdosamad Khoramabadi, the Prosecutor-General's legal adviser, unveiled "a list of 25 election-related Internet crimes." Among the contents deemed "criminal" are: calling for an election boycott, the publication of counter-revolutionary or opposition logos or website contents, etc.

Under the new 20-point regulations for cybercafés published by the Iranian Internet police on December 28, 2011, clients are required to produce an ID. Managers must install cameras on the premises and keep the camera recordings, along with all the details of their clients and a list of the websites they visited. The use of software to circumvent content filtering, Virtual Private Networks (VPNs) and USB flash drives is banned. After raiding 43 cybercafés in Birjand (in the southern province of Khorasan), the police closed six of them for "non-compliance with security measures and the use of censorship circumvention software."

Social networks demonized

The regime continues to demonize new media, claiming that they serve foreign interests and are "means of subversion." On July 29, 2011, Intelligence Minister Heydar Moslehi stressed "society's vulnerability to social networks introduced in the country by the enemy." Two days before, Interior Minister Mostafa Najar had stated that "satellites and Facebook are the electronic means of a 'soft war' by the West intended to cause the Iranian family's collapse."

The June 2011 announcement by the United States that it is developing a "shadow Internet or "Internet in a suitcase" that will enable citizens anywhere in the world to have access to the Web – one that will

work even if a government had shut down the national Internet, caused Iran to immediately adopt a tougher line and announce that it had the means to block this new technology.

Cybercensorship under full steam

Cybercensorship constitutes a major investment for the Iranian government (read the Iran chapter of the 2011 "Enemies of the Internet" report for more information). As evidenced from the last few months, Iran's technological advances show that surveillance is spreading in an increasingly sophisticated manner from one computer to the next. Censors can match a suspicious email with the sender's IP address. While most dissidents are very well aware of what precautions to take online, the slightest error or lack of attention can be fatal.

In August 2011, Gmail users became "snoop" victims of a "man-in-the-middle attack (MTM) via a fraudulent SSL certificate originally delivered by the Dutch company DigiNotar, which finally revoked it. Computer security firm F-Secure was reported by *Agence France-Presse* to have said: "It's likely the Government of Iran is using these techniques to monitor local dissidents."

Internet access cut-offs and a general slowing down of Internet bandwidth to disrupt communications have become commonplace in periods of unrest. They are increasingly adapted to match the seriousness of the events taking place, and the authorities are now able to target those cities or districts they want to disconnect.

For several days in February 2012, censors managed to block access to the secure "https" protocol that encodes Internet communications, thus depriving millions of Iranians from being able to access their Gmail and Yahoo accounts. VPN ports were also blocked, impeding many Iranians who use such tools to circumvent censorship. The Tor network has also been very difficult to access.

Collaboration with Western companies

The repression orchestrated by the Tehran regime relies on the help it gets from foreign companies, particularly Western ones. Despite the sanctions adopted by European and U.S. bodies against Iran, Reporters Without Borders is astonished by the government's ability to circumvent these measures by means of the "dummy" companies it has created. The rules governing the export of censorship and surveillance equipment need to be revised. Procedures for tracking relevant equipment and software must be reinforced to prevent "banned" products from reaching dictators via third countries or obscure companies.

According to the *Bloomberg* news agency, Israeli computer security company Allot has for years been selling surveillance software and programs that locate mobile phone and Internet users to the Danish company RanTek, which then resold it to Iran. Irish firm AdaptiveMobile Security has just announced that it is suspending sales of its SMS filtering and blocking systems to Iran.

The frequently announced (and always postponed) national Internet

The blocking of the "https" protocol has been interpreted as a dress rehearsal before launching Iran's national Internet, cut off from the World Wide Web, already announced for the spring of 2011.

However, netizens who seized the occasion to use Iranian email accounts apparently were not impressed with the quality of service. Could the censors still have a lot more to work out?

In actuality, Iranians who cannot, or dare not, circumvent the censors' filtering system are doomed to use a regime-approved version of the Web, meaning one "cleansed" of any political, social and religious criticism. The national Internet has been a reality for years now, so the announcement of its launching primarily stems from political and nationalist motives.

Since July 2011, Communication and Information Technology Minister Reza Taqipour Anvari has been announcing the launch of the first phase of a "National Internet", also called "Clean Internet." During the first phase, the Minister claimed that consumers would initially have access to an 8 Mbps speed broadband connection scheduled to later rise to 20 Mbps. Iran is also expected to launch its own national search engine, "Ya Haq" ("Oh Just One"). The Minister recalled that the project's aim is to

"better manage national emails and information gathering within the country and to improve security." Surveillance of dissidents' email will inevitably increase.

Can the country afford such a project? Besides the related development and operation costs, Iran needs to stay connected with the World Wide Web to carry on its commercial and financial transactions. It may be recalled that a five-day cut-off in February and March 2011 had cost Egypt USD 90 million. Is the regime moving toward a two-speed Internet with access to the World Wide Web for the government, religious leaders, Revolutionary Guards and big companies on one side, and the vast majority of the population limited to a censored Intranet on the other?" If such is the case, the authorities would be guilty of grave discrimination against its own people – a genuine digital apartheid.

NORTH KOREA

ENEMY OF THE INTERNET

The world's most closed country's absolute control over the media became evident during the events surrounding the death of Kim Jong-il and the meticulous staging of his succession. Yet official and unofficial telecom markets have been booming. The new leader Kim Jong-un's policy regarding basic freedoms appears to be a continuation of his father's, which understandably worries the international community.

Kim Jong-il's death showed the full extent of the regime's tight grip on the media and information inside the country inasmuch as the news was only announced on North Korean state-controlled television after it had been kept secret for two days.

North Korea online: the digital "self-reliance" theory

Recently, North Korea officially entered the World Wide Web to wage a propaganda war against South Korea and the United States. The regime equipped itself with an army of hackers instructed to destroy websites and practice espionage. Most were trained at Mirim College, an authentic ultra-secure, and clandestine hacker training center. The regime has simultaneously been keeping the great majority of the population away from the Web, even the very limited and ultra-censored national intranet (see the North Korea chapter of the 2011 "Enemies of the Internet" report).

The development of new technologies was one objective of the latest "New Year Editorial," which set the priorities for the coming months, in keeping with the country's "self-reliance" theory, the juche. On the blog NorthKoreaTech.org, Martyn Williams discussed the publication in the official media, of a staged photo of workers inspecting computers in a factory. Mere propaganda?

Yet more and more North Korean media are launching their own Internet websites, such as *Voice of Korea*. The newspaper of the Workers' Party, *Rodong Shinmun*, appears to be adapting to new technologies by sending news to its subscribers' mobile phones. Transmissions are being made via MMS to compensate for the lack of smartphones.

The popularity of cell phones

Could economic factors be fueling the current telecommunications boom? In January 2011, Kim Jong-il's warm reception of Orascom Telecom's Chairman, Egyptian businessman Naguib Sawiris, who set up the country's 3G mobile phone network via Koryolink, was interpreted by the elites and general public as a sign that the security services would approve an expanded use of the networks – provided, of course, that doing so would not prove a threat to the regime. North Korea is allegedly planning to allow access to the Internet and mobile phones in the Mount Kumgang Special Tourist District, which had previously been the subject of a development agreement with Hyundai.

The explosion in the number of mobile phones – one million 3G subscribers as of early February 2012 out of a population of 24 million inhabitants – may constitute a factor in the opening of this market. However, the network only functions within the country and is still subject to close surveillance. The government, now incapable of monitoring everything, is setting a few examples to keep other users in line.

In addition to the official network, North Koreans living within a radius of about 12 miles of the Chinese border have the (illegal) option of connecting to the Chinese mobile network. The authorities have intensified the crackdowns and fines for simply making an international call, which can run as high as 1 million wons (about $1,100) along with one week of detention. In addition to jamming telephone networks, the North Korean regime has established a surveillance system for calls placed from North Korea. Moreover, the high cost of calls for a portion of the population, and geographical constraints, have limited the use of mobile phones among the rest of the population.

News smuggling along the Chinese border

News smuggling along the Chinese border creates a hard-to-eradicate situation, yet several special units, such as "Group 109,"have been set up – some by Kim Jong-un himself before assuming leadership of the country – to thwart these clandestine activities. The government is also monitoring citizens who travel to China. Any person who criticizes the regime or engages in reprehensible activities such as using the Chinese Internet – which is by no means free – can be denounced.

Despite harsher crackdowns and the illegal nature of such markets, they are extremely active and their use is spreading. They are the place of transit for Korean and U.S. series DVDs and CDs, as well as USB flash drives. Korean associations also distribute, through other channels, stealth USBs containing news about democracy and human rights, and designed to appeal to the country's dissidents, students and intellectual elites.

Many questions concerning the country's future and its communications system remain unanswered. Will Kim Jong-un be a more open-minded successor? Or just a front for a regime actually led by a military junta? His past experience as head of a unit responsible for using terror tactics to control the smuggling of "impure" media is raising concern. Yet one thing is certain: the development of an underground economy and the permeability of the Sino-Korean border, combined with an expansion of regime-approved mobile telephony, are key factors for the prospect of a gradual opening up of North Korea.

SAUDI ARABIA

ENEMY OF THE INTERNET

In 2011, the regime did everything possible to dissuade the population from supporting the arab revolutionary movement. Its rigid opposition to the simmering unrest on the Web caused it to tighten its Internet stranglehold even more to stifle all political and social protests.

Harsh censorship

Intolerant of criticism, in the last few years the government has been enforcing harsh censorship through the use of extended filtering bolstered by repressive legislation and widespread online surveillance (see the Saudi Arabia chapter of the 2011 "Enemies of the Internet" report).

The authorities resorted to blocking websites created in the aftermath of the demonstrations in Tunisia and Egypt which relay the protestors' demands, such as Dawlaty.info and Saudireform.com. An online petition was circulated to openly call for the King to initiate political reform. Despite the censorship, it was signed by several hundred people – activists, writers and academics – and posted on Twitter, thanks to the hashtag #saudimataleb.

The authorities **intensified their crackdown on forums and social networks**, anticipating demonstrations held in several of the Kingdom's cities on 11 March, redubbed the "Day of Rage." Facebook's "Revolutionary Nostalgia" page, which echoes the calls for reform, was added to the long list of URLs rendered inaccessible in the country. NGO Amnesty International's website was blocked after publication of an anti-terrorist draft law aimed at repressing even more severely criticisms of the royal family.

Attempt to impose a blackout on protests in eastern Saudi Arabia

The authorities tried **to impose a total media blackout on protests in the governorate of Al-Qatif** in eastern Saudi Arabia, which has a majority Shiite population, raising the spectre of religious unrest to justify the repression. Several demonstrators were shot and killed. Even foreign journalists with visas were stopped and questioned while covering protests in the town of Hofuf, also in the eastern part of the country. It was netizens – sometimes at the risk of life – who circulated news about these events online. Bloggers **Mustafa Al-Mubarak** and **Hussein Al-Hashim**, known for their Web-based activities, were arrested in April 2011 and their computers confiscated. They were later released. However, writer **Nazir Al-Majid**, who in April had published an article entitled "I protest, therefore I am a human being" on the news website rashid.com, is still in prison. So are **Fadil Al-Manasef** and **Hussein Al-Youssef**, as well as writer and reformer Sheikh Mekhlef bin Dahham Al-Shammari. Detained since June 2010, he may be facing "terrorism" charges. His state of health has grown considerably worse.

Avoid any risk of "social destabilisation"

Special measures have been taken to avoid any risk of "social destabilisation" in a troubled regional conjuncture, despite promises made by the King in March 2011 to grant billions of dollars in subsidies to improve the Saudis' working and housing conditions, as well as their health coverage. Three online TV journalists were arrested in October 2011 and held for several days after the "Malub Aleyna" show broadcast a report on the living conditions of the poorest inhabitants of the Saudi capital. The programme's online video has been viewed over 500,000 times. Radio Nederland's Internet website was blocked after it featured an article on the poor treatment of immigrants in Saudi Arabia.

Another evidence of Saudi Arabia's implacable intolerance of freedom of expression : **Hamza Kashgari**, a young journalist, was arrested after expressing his personal views online. He is facing a possible death sentence for three tweets which the Saudi authorities regard as blasphemous.

In the last few months, the fight for women's rights has been waged mainly online – the only news and mobilisation platform for such issues – from the "Women2Drive" campaign promoting the right of women to drive launched on Facebook, Twitter and YouTube (one of its organizers was arrested for filming herself while driving), to the Baladi campaign for women's right to vote. The latter ended in

triumph: women have won the right to vote in the 2015 elections. This victory is all the more significant in that it occurred at a time of widespread loss of individual freedoms.

SYRIA

ENEMY OF THE INTERNET

Bashar Al-Assad's regime responded with violence when Syrians, inspired by the mass uprisings in the Arab world, took to the streets in March 2011 to demand democratic change. In the weeks that followed, the regime stepped up control of the means of communication and surveillance of dissidents. With the help of its cyber-army, it engaged in a battle of disinformation. Syria's netizens, the only witnesses still present in the worst-hit areas, continue heroically to risk their lives to inform the world. Like Syrian and foreign journalists, these unwanted witnesses are now seen as enemies of the state.

Syria was already known for its censorship of the Internet before the start of the Syrian revolution (read the Syria chapter in the 2011 Enemies of the Internet report). In response to the protests, a violent crackdown in the streets was accompanied by unrelenting online repression.

Citizens and netizens combat the news blackout

Outraged by the regime's reaction, bloggers and netizens took it upon themselves to provide news and information once the foreign media has been expelled shortly after the start of the uprising. As the death toll mounted, ordinary citizens got involved, becoming activists and journalists at the same time, documenting what was happening as journalists would have done, but from the perspective of those who are clearly committed. Already seen during the Tunisian and Egyptian revolutions, this trend is much more pronounced in Syria. Activism and reporting have become one.

Simultaneously citizens, activists and reporters, they use their imagination to get the information out. Video is filmed with mobile phones and sent straight to video-streaming websites. Or it is filmed with video cameras and the video files are copied on to USB flash drives and passed from hand to hand until they can finally be posted online. Much use is made of Skype and Mumble. Syrians who live the near border use Lebanese or Turkish servers to access the Internet or mobile phone networks and thereby escape surveillance.

As the regime reinforces its censorship, the media center created by local coordination committees has formed a network of contributors throughout the country to help disseminate information. They have managed to post videos directly on YouTube, above all via *LCCSyria TV*, and have helped to transmit content to foreign media. Other networks such as Sham News Network and Avaaz have contributed to circulate information.

Members of the Syrian diaspora play a key role in relaying information to journalists and politicians in the countries where they live. Human rights activists throughout the world have also joined this chain of international solidarity. Participative initiatives such as Syria Tracker are trying to document the crimes being committed in Syria.

"Hactivists" have helped to get video footage out of Syria. Telecomix, for example, executed a major operation called #OpSyria on the night of 4 September to help Syrians to dodge the government's censorship. It succeeded in diverting all Syrian Internet traffic to a special page with advice on circumventing censorship, including how to install the Tor software and use a secured https connection. More and more people have since then connected to the Telecomix channel using the protected instant messaging system IRC and have been given help with circulating videos, photos and eye-witness accounts.

Indiscriminate violence against population and news sources

The toll from the repression since March 2011 is damning. Amnesty International cites the figures provided by the London-based Strategic Research and Communication Centre, which specializes in following Syria. According to the centre, the toll on 4 March 2012 stood at 10,207 dead (including 710 children), 65,000 disappeared and more than 212,000 arrests.

At least seven journalists had been killed in connection with their work in Syria by the end of February 2012. Netizens have also paid with their lives for disseminating information. Citizen journalist Basil Al-Sayed was killed in Homs on 29 December while filming a bloodbath in the district of Baba Amr. He

had been filming demonstrations and the brutal crackdowns by the security forces since the start of the uprising (watch his last video). Photographer and video-reporter **Ferzat Jarban** was murdered on 20 November after being arrested in Homs. **Soleiman Saleh Abazaid**, who ran the "Liberated people of Horan" Facebook page, was killed by a shot to the head in July. Writer and activist **Hussein Issou**'s fate is not known but the worst is feared.

Many Syrian journalists and bloggers have been arrested or kidnapped and many have been tortured while detained. A total of 16 people – employees and visitors – were arrested during a raid on the Syrian Centre for Media and Freedom of Expression in Damascus at midday on 16 February. The centre's director, **Mazen Darwish**, was one of those arrested. The others were **Yara Badr**, **Razan Ghazzawi**, **Hanadi Zahlout**, **Hussein Greir**, **Hani Z'itani**, **Sana Z'itani**, **Rita Dayoub**, **Joan Farso**, **Bassam Al-Ahmad**, **Mayada Al-Khalil**, **Maha Al-Assablani**, **Mansour Hamid**, **Abdelrahman Hamadah**, **Ayham Ghazzoul** and **Shady Yazbek**. The women were released two days later but were told to report daily to intelligence services while an investigation continues. Nine men are still detained. The raid was condemned by four UN experts.

Ahmed Hadifa, a 28-year old blogger better known by the blog name of **Ahmad Abu Al-Kheir**, was arrested in Damascus on 24 March 2011 "because of his activities on Facebook in support of the protests in Deraa" and was held for three weeks. It was his second arrest.

The many others who have been arrested include cyber-activists **Alaa Shueiti** and **Qais Abatili**, and the Kurdish activist **Shabal Ibrahim**. **Anas Al-Ma'arawi**, a journalist, blogger and founder of the first Arab website to specialize in the Android system, was arrested in a Damascus suburb on 1 July and was held for two months. **Mohamed Ghazi Kannass**, a journalist who was active on Facebook and kept his own blog called Kalemah Insan ("A man's word"), was arrested in Damascus in January 2012. **Jehad Jamal**, a blogger known as "**Milan**," was arrested in October and was released at the end of December while the Arab League observers were in Syria. The blogger **Othman Mohamed Issa** was arrested at his Damascus home on 21 November.

Filmmaker and cyber-activist **Firas Fayyad** was arrested on 1 December at Damascus airport on charges of spreading false information and belonging to an opposition movement. He was finally released in February. (See a partial list of bloggers held on 14 January.)

Student and blogger **Tal Al-Mallouhi** has been detained since December 2009. She was brought before a state security court in Damascus for the second time on 17 January 2011. Reportedly accused of spying for the United States, she is being held in Duma prison, near Damascus. Internet users all over the world have called for her release.

Reporters Without Borders knows of dozens of Syrians who have been arrested and tortured after giving interviews to foreign media about the repression in their country. Others have been arrested for working for journalists. The Syrian security agencies make every effort to identify those who help foreign reporters or talk to them. Reporters Without Borders has urged the international media to use the utmost prudence in their contacts with Syrians.

Disrupting communications

At the start of June 2011, the government temporarily imposed an almost complete stop on the Internet. It was subsequently lifted but Internet connections are now slowed right down regularly, almost every Friday, when the big weekly protests are staged. This is especially so in areas that are opposition strongholds. The aim is to prevent people from sending and receiving video footage of demonstrations and the ensuing violent response from the security forces. There have been reports of the Internet and mobile phone communication being disconnected in Homs at the height of the offensive against the district of Baba Amr.

In an attempt to limit the size of the protests and the transmission of photos and videos, the authorities often temporarily suspend Internet and mobile phone services in the localities where protests are taking place. News media and NGOs have responded by distributing satellite phones in cities that are often targeted by such cuts or are hard to access. Risks of geolocalization are involved. Border checks have been stepped up and it is now very difficult to bring such hi-tech equipment into the country.

Charging batteries is also a problem. The authorities often cut power supplies to restrict the dissemination of information.

Access to Bambuser, a Swedish website that allows users to post video footage shot with a mobile phone, has been blocked in Syria since 16 February. Confirming this on 17 February, the head of the site said "dictators don't like Bambuser" and that the Assad regime regarded it as a "serious threat." The Syrian opposition has been using Bambuser to circulate video footage of the government's brutal repression. Video of the bombardment of Homs that had been posted on Bambuser was recently broadcast by leading international TV stations. Bambuser was blocked in Egypt in January 2011 and is still blocked in Bahrain.

Surveillance and propaganda

The government's cyber-army, which tracks dissidents on online social networks, seems to have stepped up its activities since June. Web pages that support the demonstrations were flooded with pro-Assad messages. To disrupt information on the #Syria hashtag, Twitter accounts were created to send hundreds of tweets with keywords that switched the reader to sports results or tourist photos of Syria. And to discredit the uprising, messages calling for violence were posted on the pages of government opponents to give the impression that they were the authors.

The cyber-army claimed its efforts were designed to make up for the shortcomings of the official media and to wage an information war targeted at Syrians both at home and abroad.

In order to better monitor dissidents, the authorities used phishing and "man-in-the-middle" methods to obtain their personal data. The Electronic Frontier Foundation (EFF) warned Syrian Facebook users on 5 May that fake security certificates planted by Syria's telecommunications ministry were being used to trick them into providing their personal data and thereby allowing their communications can be monitored. The fake security certificates caused warnings to pop up in browsers, but people tended to ignore them. The EFF urged Syrian users to use proxy connections to access Facebook, or to login via Tor. The EFF subsequently reported that Syrian ISPs were blocking access to Tor. Another option is to use a Virtual Private Network (VPN).

The Syrian authorities have reportedly used Iran's expertise in online surveillance as well as filtering equipment provided by the US company Bluecoat. Syria is subject to US trade sanctions but Bluecoat insists that any equipment that may have ended up in Syrian hands was in fact supposed to be sent to Iraq. The case highlights the paramount importance of monitoring the export of Internet censorship and surveillance equipment.

Legislative farce

In an example of the regime's macabre and schizophrenic attitude towards all those who provide news and information, President Assad issued a decree on 3 December creating a National Information Council to regulate the broadcast media and Internet. It followed a 28 August decree that included a call for "respect for the fundamental freedoms contained in the Universal Declaration of Human Rights and in international conventions." Article 11 said that "any attack on a journalist will be treated as an attack on a Syrian government official." No one was fooled.

The latest videos from Baba Amr in Homs are evidence of the regime's crimes against humanity. The risks being taken by journalists and bloggers and the sacrifices that ordinary citizens are making to ensure that information continues to circulate testify to the greatest fear of Syria's dissidents, that the massacres will take place without the outside world knowing what is going on.

UZBEKISTAN

ENEMY OF THE INTERNET

In intensifying censorship and surveillance, and making a pretence of promoting freedom, the Uzbek regime has been attempting to strictly monitor Internet users in order to offset the fallout from Arab Spring, while taking the offensive by exporting its model on a worldwide scale.

Cynical official rhetoric

On the occasion of "Media Workers' Day" on 27 June 2011, President Karimov asserted that the government "...fully supports the desire of our fellow citizens to increasingly use the Internet. [...]" He further stated: "We absolutely do not accept the establishment of any walls, [or] limitations in the information world leading to isolation," and denounced the "destructive forces" which "tend to mislead young people."

The official rhetoric is very remote from the contemptible reality: Uzbekistan is one of the region's most Internet-repressive countries (see the Uzbekistan chapter of the 2011 "Enemies of the Internet" report).

Arab Spring: The censors' latest scapegoat

Uzbek censorship and online monitoring were bolstered in 2011 in reaction to Arab Spring. The first step consisted of intensifying Web filtering:

- The Institute for War and Peace Reporting (IWPR) website, and that of Russian investigative magazine Russky Reporter, one of the last sources of independent information still accessible in the country, are now blocked.
- On 9 August 2011, on the eve of the Internet Festival of the national domain UZ, marking the 20th anniversary of Uzbekistan's independence, more than 50 major websites, including such foreign news portals as those of *The New York Times*, *Reuters*, *Bloomberg* and *Lenta.ru*, as well as the Google research engine, Reporters Without Borders' website, etc., were blocked for several days.
- Uzbek discussion forums on events in Egypt, Tunisia, and Bahrain such as arbuz.com have been blocked and contributors arrested.
- Articles and news about demonstrations and protest movements have been blocked,particularly the controversy surrounding the United Nations' resolutions on Syria. The *BBC* website was unblocked in late 2011, but since January 2012, specific pages dealing with the Arab Spring have been inaccessible.

The authorities are increasingly cracking down on technical intermediaries. ISPs and mobile phone operators are now required to report mass mailings of "suspicious content," and to disconnect their networks at the authorities' simple request. The objective is clear: to prevent any mass distributions and rallies.

All-out surveillance

In August 2011, the already well-developed Internet surveillance apparatus was reinforced with the creation of a "Committee of Experts on Information and Mass Communication." Exclusively made up of government employees, this new structure was apparently created to analyze and interpret data collected by the Center for Monitoring Mass Communications in the aim of monitoring the media and formulating new laws.

Phishing attempts have been detected. A mirror website of the Uzbek *Radio Free Europe/Radio Liberty* service, ozod.orca.uz, allegedly has been set up to collect the personal data of netizens consulting the site.

On 1 September 2011, the regime launched a national social networking site – Muloqot ("Dialogue"), with drastic Terms of Use – which some observers interpreted as a prelude to blocking Facebook, or at least as indicating their desire to restrict its influence. According to *Radio Free Europe/Radio Liberty*: "Colleagues in *RFE/RL*'s Uzbek Service managed to register on the first day and post RFE/RL content (blocked in Uzbekistan) to a general Wall (at that point there were only about 400 users).

Within 15 minutes, however, their profiles were deleted. Another RFE/RL staffer posted some comments praising the president's daughter, Gulnara Karimova, and their profile has remained active."

Two human rights activists, Saida Kurbanova and Gulbahor Turaeva, were harassed and intimidated after the former denounced online issues concerning government credit cards, and the latter criticized the unhappy fate of the country's elderly and the defects of the waste collection system.

Between uncertain reform and exporting a control model

Media legislation reform is underway. However, the official pro-media freedom discourse may be an omen of more obstacles to the free flow of information. By integrating new technologies, according to the OSCE, "it must result in more, and not less media freedom".

Uzbekistan has been exporting its repressive practices. The country has globally positioned itself as the champion of tighter Web controls. Not content to warn his Collective Security Treaty Organization (CSTO) allies against online "terrorism" and "revolutionary contagion," the Tachkent government also signed, notably with China and Russia, an International Code of Conduct for Information Security aimed at guaranteeing "cybersecurity," which it would like to see adopted by the United Nations.

TURKMENISTAN

ENEMY OF THE INTERNET

For the first time, netizens have managed to breach the censorship wall of one of the world's most closed countries. In response, the regime has targeted them for harsh crackdowns, ready to do whatever it takes to retain its absolute power, even to the point of viewing people with satellite dishes and mobile phones as potential enemies.

Hopes that the country would open up with the coming to power of President Gurbanguly Berdymukhamedov in 2007 have come to nothing.

Turkmenistan, one of the countries most hostile to freedom of expression, is still technologically and financially blocking the growth of the Internet and imposing drastic censorship, resulting in a "Turkmenet" purged of any political or social topic (see the Turkmenistan chapter of the 2011 "Enemies of the Internet" report). In fact, only 2.2% of Turkmen are connected. Yet for those not using a software circumvention tool, social networks – particularly *Facebook, Twitter* and *YouTube*, considered to be troublemakers – are blocked. This censorship was extended to Gmail in February 2012.

Abadan: Start of the Information War 2.0

A deadly explosion at an arms depot in the Ashgabat suburb of Abadan in July 2011 marked the start of the first online information war in Turkmenistan. For the first time, netizens managed to breach the wall of silence imposed by the regime by posting on the Internet amateur videos taken with their mobile phones. Most of the videos were sent by emails to contacts abroad who could publish them online easilier.

After initially covering up this incident, the authorities were eventually obliged to acknowledge it, though they tried to minimize it. But they quickly reacted by launching a wave of seizures, interrogations and incarcerations, though how many is still unknown.

It is thought that dozens of netizens were arrested, at least temporarily. According to the Institute for War and Peace Reporting, one policeman allegedly stated that anyone possessing a mobile phone or Internet account with the state-owned operator Altyn Asyr was being monitored. Dovletmyrat Yazkuliyev, a *Radio Free Europe/Radio Liberty (RFE/RL)* correspondent, and one of the first to cover this incident, was sentenced to five years in prison, then pardoned in response to international pressure. The independent news website Khronika Turkmenistana, hosted abroad, experienced several cyberattacks. Hackers pirated the subscribers' data, and posted the identity of contributors and commentators in lieu of the site.

Mobile phones and satellite dishes under close surveillance

Connection speed has declined since Russian telecom company MTS was ousted from Turkmenistan. The "Central Asia: Censorship and Control of the Internet and Other New Media" briefing paper written by several NGOs claims that the regime, dissatisfied with national operator Altyn Asyr, which had become a monopoly once its only competitor was eliminated, signed a contract with Huawei Technologies (China) and the Finnish-German company Nokia Siemens Networks to increase network capacity and offer new services. It remains to be seen what these companies can achieve in a country whose government routinely monitors netizens.

According to the state TV network, President Gurbanguly Berdymukhamedov, who in 2008 had already declared war on satellite dishes, announced in May 2011 that their number would be limited, complaining that they "spoil the appearance of buildings." The main reason for this initiative was to prevent the population from escaping the state-controlled media's relentless propaganda by tuning into Russian, Turkish and Arabic satellite television channels.

Technological ambitions up against the censorship wall

During a speech made in January 2012 just before his programmed "reelection," Turkmenistan's President apparently stated his desire to form "a new generation of specialists who have mastered all

the modern communications and multi-media technologies" in a future "highly developed information society" who will advance civilization "by the unrestrained flight of human thought." The President apparently grasped the country's need to modernize, but refuses to question the censorship system that keeps him in power, even as he strives to bolster his own personality cult. The Eurasianet website sums up the situation as: "Berdymukhamedov's Failed Internetization."

VIETNAM

ENEMY OF THE INTERNET

The regime's attention is focused on the Arab world and its protest movements. Paranoid Vietnamese authorities have stepped up repression and control to stave off any possibility of a regime collapse, favoring surveillance over increased filtering. Bloggers have been the target off a new wave of arrests.

The authorities, aware they cannot impose a complete control of the news, are afraid of an increasingly connected population. Cybercafes are full, smartphones very popular. More than 111 cell phones are in service in the country for a population of 86 millions.

Netizens help defeat censorship

Citizen journalists have continued to fill the void left by the heavily censored official media. The bauxite mining activities undertaken by China and their disastrous impact on the environment are still such a controversial topic that the Central Highland region has been closed off. The few visitors allowed to enter the site are prohibited to bring camcorders, smartphones or cameras to prevent the circulation of embarrassing images. Despite all this, the Bauxitevietnam.info website has managed to obtain information and is doing its best to cover the situation on-site.

Another popular subject for Vietnamese Internet users is police brutality. One officer was suspended after a video was posted on YouTube showing him using violence against a demonstrator. The authorities initially denied the facts, but the concrete evidence provided by the video clip forced them to take action.

The regime has learned how to tolerate, and even exploit, online mobilization campaigns as long as they serve its interests. For several weeks following June 2011, calls for protests against the Chinese presence in southern Vietnam (disputed territories of the Paracels and Spratly islands) were circulated on Facebook, leading to public rallies – several hundred in Hanoi, and several thousand in Saigon. Although initially tolerated, these protest movements against "China's violation of Vietnam's maritime sovereignty" were first confined, then repressed.

Although filtering remains severe (see the Vietnam chapter of the 2011 "Enemies of the Internet" report), it has not been drastically intensified. The number of cyberattacks against sensitive websites seems to be holding steady. The government is more interested in monitoring than in blocking websites. Facebook is still occasionally inaccessible, but has not been permanently blocked from its two million users in Vietnam. This is another way for the authorities to monitor Vietnamese netizens' activities and networks.

In order to meet the threat that the Web's collaborative nature poses for Vietnamese censorship, the regime decided to regain control of social networks by launching its own national version of Facebook in May 2010. To open an account, the site requires users to identify themselves by their real names, as well as by their ID card number. According to *The Wall Street Journal*, Minister of Information and Communications Le Doan Hop is using his blog to encourage Vietnamese teenagers to visit the site to find out about its "culture, values and benefits." The objective is to attract over 40 million members (almost half of the population) by 2015. To accomplish this, the network is mainly relying on making available video games popular with Internet users. By mid-2011, the site had about three million registered users

Waves of arrests

Another component of Vietnam's strategy to control the Internet consists of the arrest of bloggers, netizens and journalists. One revealing sign of the authorities' intransigence is that out of the more than 10,000 prisoners amnestied by the government to mark the 66th anniversary of Vietnam's independence celebrated on September 2, 2011, there was just a handful of political prisoners. Blogger Nguyen Van Tinh and poet Tran Duc Thach, sentenced in 2009 to three and one-half and three years in prison, respectively, for "propaganda against the socialist state of Vietnam," were released, but this rare piece of good news conceals a sad reality: netizen arrests have soared in the last few months in the world's second biggest prison for netizens after China.

Several bloggers and activists linked with the Vietnamese Catholic networks were caught in a wide-scale operation carried out by the authorities between late July and mid-August 2011. Blogger **Paulus Lê Son** was arrested on August 3, 2011 in Hanoi as part of a genuine "police-engineered kidnapping." All indications are that his arrest was linked to his attempt to cover the trial of the well-known cyberdissident **Cu Huy Ha Vu**. The Catholic priest **Nguyen Van Ly** was returned to jail despite his age and poor health. Blogger **Lu Van Bay** received a four-year prison sentence in September 2011. The announcement that lawyer Le Cong Dinh may be deported to the United States has not been acted upon to date. Franco-Vietnamese blogger **Pham Minh Hoang** was released from prison after serving his 17-month sentence, but remains under a three-year house arrest.

Relatives of blogger **Dieu Cay** have had no news of him for months, leading to widespread alarmist rumors. Whether or not they are well-founded, concerns about his fate and health remain justified as long as the authorities refuse to grant his family visiting rights.

The government's priority is to remain in power, even at the cost of tarnishing the country's image. International influence is dwindling except for that of an increasingly restrictive China, whose relations with Vietnam are highly complex. The U.S. Congress could play a key role in protecting Vietnamese freedoms. In early 2012, members of Congress are scheduled to examine a bill that could tie the non-"humanitarian" part of its financial aid and military cooperation between the two countries to expected improvements in the status of human rights in Vietnam, particularly freedoms of expression and religion. The U.S. Agency for International Development (USAID) granted USD 134 million to Vietnam in 2010.

AUSTRALIA

COUNTRY UNDER SURVEILLANCE

The government has not abandoned its efforts to win approval for its mandatory national Web filtering system and has persuaded Internet service providers to create a voluntary system. It has just received the recommendations of the Law Reform Commission which may put in question the type of content involved and enforce its application to all media. In parallel, the conclusions of an inquiry into the media, such as the creation of a "News Media Council" could turn out to be dangerous for freedom of information in the blogosphere.

Privatisation of censorship

In the Australia chapter of the 2011 report on Internet Enemies, Reporters Without Borders expressed concern at the government's readiness to create a repressive Internet filtering system which would be managed in a non-transparent manner by a government agency based on very broad criteria.

Mandatory filtering appears still to be the government's goal but it does not yet have the necessary political support. To bypass the political status quo, members of the Internet Industry Association introduced a voluntary system in July last year, based on Interpol's blacklist rather than the one compiled by the Australian Communications and Media Authority (ACMA), the official body responsible for censorship.

The voluntary system, already applied by the ISPs Telstra, Optus and Primus, blocks domain names and URLs. Like the proposed national filtering system, it blocks access to content deemed inappropriate by the government such as child pornography and sexual abuse. According to Senator Stephen Conroy, the minister for broadband, communications and the digital economy, the proposal has been rejected by only one ISP, with which the government is still negotiating.

This is the first time in Australia that, as a result of cooperation from technical providers, the federal police are able to invoke section 313 of the Telecommunications Act to block domain names and URLs by identifying and collating online content for censoring. In this way it compels ISPs to remove the content concerned, effectively applying mandatory censorship.

The Australian branch of the NGO Electronic Frontier Foundation, which campaigns against censorship of the Web, has asked the authorities for greater transparency in the way that the blacklists of domain names, URLs and websites are drawn up.

According to Enterprise Features, a website that specializes in business computing, Australia spends 2.7 million dollars a year on Internet censorship. However, most of this is used to settle complaints by blacklisted sites.

Classification of filtered content to be reviewed

Officially, the application of the filtering system has been suspended since July 2010 while the Australian Law Reform Commission conducts a review of the criteria for the "refused classification" (RC) category.

The justice minister, Robert McClelland, ordered the ALRC to review this category, while also conducting public consultation and evaluating the practices and codes of companies in the sector.

The ALRC's report, submitted at the end of last month, contains recommendations that the type of content targeted by the filtering rules should be restricted to that linked to paedophilia. It suggests that other types of content should be blocked by ISPs only when it is defined as "prohibited".

The Commission has recommended that the government review prohibitions on "the depiction of sexual fetishes in films and detailed instruction in the use of proscribed drugs" and to refine its ban on content that "promotes, incites or instructs in matters of crime" to be limited only to serious crime.

A new media content classification act should cover the classification of all media in Australia on any platform, and spell out how those responsible for content, including Internet service providers, should rank prohibited content.

The ALRC, said that, because of the large number of online media organizations, it would not be possible to classify everything and ISPs should "take reasonable steps" to identify prohibited content, including allowing users to report such content online.

Reporters Without Borders is opposed to all mandatory and comprehensive filtering systems. The European Court of Justice has ruled that Internet filtering undermines freedom of information. In its ruling, the court states clearly that measures that oblige an ISP to carry out general monitoring of information that it transmits via its network were contrary to European law and infringe basic rights.

Frank La Rue, the UN special rapporteur for the promotion and protection of freedom of opinion and expression, recommended in his report published in June 2011: "There should be as little restriction as possible to the flow of information via the Internet, except in few, exceptional, and limited circumstances prescribed by international human rights law." He also said: "The right to freedom of expression must be the norm, and any limitation considered as an exception."

Media inquiry and judicial harassment of bloggers

The report of the Inquiry into Media and Media Regulation by former Federal Court judge Ray Finkelstein and Professor Matthew Ricketson published on 4 March includes a basic recommendation that is fraught with danger for freedom of information in the blogosphere.

Its proposed creation of an independent News Media Council, at a cost to the government of least 2 million dollars a year, represents a danger for the most financially vulnerable organizations and individuals. The council would have the power to order changes to published content, publication of a right of reply by anyone or any organization that makes a complaint, and the publication of an apology. Refusal to comply could result in the author, media organization or blogger being accused of contempt of the Council and tried by a court with the power to impose prison sentences.

The impact of the News of the World scandal in the United Kingdom has strengthened the idea among those in favour of the new council that there is a need for an authority to regulate the media, given that the latter tend to abuse their power.

For any Internet user who wants to appeal, once the case has been referred to court, the financial cost could remove any possibility of a fair defence by the author of content that is the subject of a complaint.

Mark Pearson, professor of journalism at Bond University, commented: "And what if such a Council orders a leading environmental news site or magazine to publish an apology to a mining magnate for the ethical breach of publishing a 'biased' and inaccurate report about the company's waste disposal practices, based on sensitive material from confidential sources? Where would the power and resources rest in a court appeals process in that situation?"

This proposal amounts to converting the code of ethics of the Media Entertainment and Arts Alliance (MEAA), the union covering Australian media, into laws enforceable by the courts.

Small publishers and bloggers could well feel coerced into publishing corrections or apologies because they may not have the time, energy or resources to defend themselves in court against a contempt charge.

EGYPT

COUNTRY UNDER SURVEILLANCE

The first anniversary of Egypt's revolution was celebrated in a climate of uncertainty and tension between a contested military power, a protest movement attempting to get its second wind, and triumphant Islamists. Bloggers and netizens critical of the army have been harassed, threatened, and sometimes arrested. Blogger ***Maikel Nabil Sanad*** *was the first prisoner of conscience of the post-Mubarak era.*

See the Egypt chapter of the 2011 "Enemies of the Internet" report.

The Supreme Council of the Armed Forces (SCAF), which has been leading the country since Hosmi Mubarak February 2011 departure and his reluctant relinquishment of power to newly forces, has not kept its promises. It was not until the eve of the 25 January 25 festivities that the state of emergency in effect since 1981 was partially lifted. Untouchable in Egypt, the army still practices the same censorship and intimidation. The Council has not only perpetuated Hosni Mubarak's ways of controlling information, but has strengthened them. Numerous journalists and bloggers seeking to expose the abuses committed during the pro-democratic uprising by certain elements of the Army or the military police have been prosecuted before military courts, and sometimes jailed for several months. The SCAF has affirmed that it will show "no tolerance for insults [against itself]."

Multiple assaults, threats of prosecution, and still more political prisoners

One striking example is blogger Maikel Nabil Sanad, the first prisoner of conscience of the post-Mubarak era. This conscientious objector was sentenced by a military court to a three-year prison term in April 2011 for "insulting the armed forces." He was accused of having published a report on his blog questioning the alleged neutrality of the army during the January and February 2011 demonstrations. Held incommunicado, he began a hunger strike that raised concern about his health. The judge had even decided to have him transferred to a psychiatric hospital. Along with close to 2,000 other detainees, he was granted a pardon on January 21, and finally released on January 24, 2012 after spending ten months behind bars. Immediately after his release, he once more began to challenge the legitimacy of the armed forces and criticizing their record on the eve of the first anniversary of Egypt's revolution.

Australian journalist **Austin Mackell**, who relates Egyptian revolution events in his articles and in his blog "The Moon under water," was arrested while covering a general strike in Mahalla on February 11, 2012, the first anniversary of former president Hosni Mubarak's departure. His arrest confirms the Egyptian authorities' anxiety about the strikes that began one year ago. The military government, which has been running the country since the ousting of the former *rais* [president], is fearful that the unrest may spread even as anger continues to escalate in the streets.

Blogger **Asmaa Mahfouz** was also interrogated and warned that she would be prosecuted for insulting the SCAF. The army finally decided not to pursue the case after a particularly aggressive online campaign that led Egyptian netizens to say that she had been "released with a hashtag."

On May 15, 2011 blogger **Botheina Kamel** was summoned for questioning by the national military court shortly after she criticized the army on the *Nile TV* station.

Blogger and activist **Alaa Abdel Fattah**, who was incarcerated in late October 2011 for refusing to respond to charges of "incitement to violence," "theft of a weapon," "assaulting army personnel," "destruction of military property," "premeditated murder" and "intent to commit a terrorist act" during riots in Maspero, was indicted toward the end of November by the Egyptian High National Security Court, and then released in late December 2011. Reporters Without Borders asked that the charges against him be dropped. The army showed that it was still capable of violence during these confrontations between Coptic protesters and police forces in Cairo's Maspero district: it has directly targeted the media and journalists and has also temporarily cut off electricity, phone lines, and Internet connections in newspaper *Al-Shorooq* offices.

On October 22, 2011, Ayman Youssef Mansour was sentenced to three years of forced labor for "deliberately insulting, attacking and mocking the dignity of the Islamic religion" on Facebook. The netizen was arrested last August.

Assaults and mistreatments of bloggers and information professionals have been multiplying. Among the victimized bloggers are Mona Eltahawy, Maged Butter, and Malek Mostafa, who lost an eye during the Tahrir Square "cleansing" in late November 2011.

Is the SCAF still tampering with bandwidth speeds?

Near the end of November 2011, while the country was in the throes of a new revolutionary episode in the run-up to the legislative elections, several independent sources alerted Reporters Without Borders that Internet connection speeds had slowed down several times during the demonstrations. Internet access from Vodafone mobile phones and other digital devices had also been impeded.

Did the army give the green light to cutting off Internet services at the height of the revolution? Former president Hosni Mubarak accused Egyptian Marshal Tantawi of being behind this decision, which the SCAF allegedly denied.

Justice for Khaled Said?

The trial of policemen Mahmoud Salah Amin and Awad Ismail Souleiman, the alleged murderers of Egyptian blogger Khaled Said killed on 6 June 2010 in front of an Alexandria cybercafé, resulted in each receiving a seven-year jail sentence. According to the medical examiner's report, the netizen was apparently beaten unconscious before being suffocated, contradicting the two suspects' claim that the young man had died after intentionally ingesting some drug at the time of his arrest.

Many netizens felt that the verdict was too lenient. Khaled Said's death triggered such an outcry in the Egyptian blogosphere that he became one of the symbols of the Revolution on the Facebook page "We are all Khaled Said."

A still-mobilized blogosphere

Egyptian society remains divided between those who believe that the Revolution is over, those who want to continue to fight for democracy, and the largest group: the undecided. In a country undergoing a difficult transition, most bloggers have no intention of giving up their keyboards. They say they are determined to pursue their "mission to inform" despite the challenges facing Egypt, particularly in view of the presidential elections scheduled to be held there near the end of June 2012.

ERITREA

COUNTRY UNDER SURVEILLANCE

The Arab Spring has given new impetus to an increasingly active online diaspora's hope for change. The regime, which has totally cordoned off the country and continues its indiscriminate repression of the population, is somewhat overwhelmed by the Net's influence on Eritreans based abroad. It is now waging its propaganda war on social networks. Pro-opposition websites have been targeted for cyberattacks on an unprecedented scale.

Self-censorship, difficult Web access, and limitless terror

In this totally freedom-deprived country whose privately owned media were shut down in September 2001, the Internet remains the only space left where Eritreans are free to voice their opinions. Its use, however, is still very limited. Dictator Isaias Afewerki has imposed a climate of terror that has led the few Eritreans brave enough to connect despite technical obstacles and surveillance in the cybercafés to rely on self-censorship (Read the Eritrea chapter of the 2011 "Enemies of the Internet" report).

Leading diaspora websites such as Assenna.com, Asmarino.com and Awate.com are inaccessible mainly because of the slow bandwidth speed. No independent site is currently operated from Eritrea. Those living abroad who post writings on "banned" websites often have to do so anonymously as a security measure.

Not just content to terrorize his country's population, the President is trying to target exiled dissidents with the assistance of certain friendly foreign governments. Sudan-based Eritrean editorial writer and journalist Jamal Osman Hamad, editor of the Internet website *adoulis.com*, was released by the Sudanese security forces in Khartoum on December 16, 2011 after being detained more than eight weeks. Known for his criticisms of his country's leader, he was arrested on October 24, 2011, less than a week after Eritrean President Isaias Afewerki paid an official visit to Sudan – a visit during which the latter and his Sudanese counterpart inaugurated the opening of a road linking their two countries. On October 17, 300 Eritreans had been expelled to their native country without their cases being referred to the Office of the United Nations High Commissioner for Refugees.

Are the new media generating an Eritrean Spring?

The regime took a very dim view of the Arab uprising and the fall of presidents Hosni Mubarak and Mouammar Kadhafi, whom it supported. It forced the state-owned media to ignore these events and was prepared to cut off Internet access, just as the Egyptian regime had done during the height of the Revolution, in the event of domestic unrest. The regime also has been concerned about the social networks' potential as a rallying tool for diaspora Eritreans. Unlike their fellow citizens who remained in the country, diaspora Eritreans are much more up-to-date on the latest Arab revolution developments, which is reviving hopes for a political change in Africa's "North Korea." The movements organized by the opposition in the last few months in streets around the globe, and in diplomatic channels, are a new phenomenon.

From March to May 2011 in particular, exiled Eritrean communities held peace rallies to commemorate the 20th anniversary of the country's independence and to protest against the dictatorial regime. In Australia, Great Britain, the United States, Egypt, and Ethiopia, the slogan was "ENOUGH!" These demonstrations were coordinated primarily by the Facebook group "Ashab Yourid Isqat Isaias Afewerki" ("The People Want Isaias Afewerki to Step Down").

Opposition Eritreans living abroad have also decided to involve Eritreans who had remained at home in a special way. Youth groups such as *Eritrean Youth for Change (EYC)* and *Eritrean Youth Solidarity for Change (EYSC)* called upon Eritreans in the homeland to "empty the streets" of Asmara as part of the "Arbi Harnet" (Freedom Friday) campaign launched in early February 2012.

Daniel Gebremichael, one of the campaign organizers, stressed on Awate.com: "We also needed a channel of communication between diaspora activists and the people back home to begin to open up a bit. So you can say that [this movement] was inspired by the Arab Spring, but was heavily influenced by the political culture in Eritrea." He added that hundreds of phone calls were made by volunteers to

Asmara and other cities in the country, and text messages and emails were sent to inform Eritreans about this campaign and invite them to rally. The 10,000 plus subscribers of the EYSC and EYC Facebook pages were contacted. YouTube video clips were uploaded to convince people to take part in this call for democratic changes in the country. Daniel Gebremichael believes that the effort produced positive results. The initiative apparently received messages of support from people contacted on-site. Most of them who could be reached were so frightened that they just listened. But the important thing is that the message got through. The announced goal was to call 5% of Eritrea's more than 230,000 telephone lines.

Yemane Gebreab, the President's top political advisor, and leader of the incumbent party, was cornered after being spotted in a Manhattan pub by young Eritreans who wanted to question him about people gone missing in the country, and who criticized his support of the dictator. The event was filmed, posted on YouTube, and – to the authorities' consternation – relayed by thousands of members. According to Awate.com, various forms of the video have been viewed tens of thousands of times: a hard blow for the regime's propaganda machine.

Start of a cyberwar?

The government is still waging an online offensive against such criticisms. Eritrean Information Minister Ali Abdu, and Yemane Gebreab, are coordinating online propaganda, disinformation initiatives on the Internet, cyberattacks against opposition sites, and crackdowns and pressure on the regime's opponents. They have decided to occupy the social networks' terrain and to confront their opponents there by disseminating their own pro-regime messages. One of the Facebook pages concerned is Eritrea First, which, as of early March 2012, boasts 2,500 friends and whose motto is "The nation always comes first."

An unprecedented wave of cyberattacks struck several websites critical of the regime in early December 2011. Most of the opposition sites, including Assenna.com, Awate.com, Asmarino.com, were blocked for several days. Hackers allegedly attacked these sites' databases in a vain attempt to delete their archives, but pro-government sites such as Meskerem.net, Alenalki.com, and Dehai.org were spared – a new censorship episode with which it would be difficult not to connect the Asmaran regime.

These attacks were perfectly timed, when the targeted sites were speculating on the President's end-of-year speech, and the UN Security Council was broadening the sanctions imposed on Eritrea for its presumed support of Somalia's Islamist insurgents.

FRANCE

COUNTRY UNDER SURVEILLANCE

The government has taken the exact opposite course from the one laid out in recent court rulings and international recommendations that condemn filtering and cut off Internet access, and has done so in a context of increased pressure on journalists to reveal sources. France must not sacrifice online freedom of expression and Net neutrality for reasons related to security or copyright protection. In a country aspiring to become an Internet leader, the legislative straitjacket that is being deployed will impede innovation.

When online information topples

The France chapter of the 2011 "Enemies of the Internet" report, the first year France was added to the list of countries "under surveillance," began with the observation that 2010 had been a difficult year for online journalists and their sources. The year 2011 has proved just as challenging, mainly because of escalating lawsuits against journalistic sources. Two *Rue89* journalists and one from *France Inter* were indicted on August 30, 2011 based on a complaint filed by the Bolloré Group concerning information they released about this group's activities in Cameroon. French Minister of the Interior Claude Guéant withdrew his complaint against Mediapart, according to which French intelligence services were spying on its journalists. Death threats were made against a Mediapart journalist who was covering the Karachi case. Read the "La tentation du contrôle" report published by Reporters Without Borders on February 27, 2012.

Another embarrassing example is the decision of the French High Council for Broadcasting (CSA) regarding the on-the-air mention of social networks such as Facebook and Twitter. In June 2011, the CSA found that "redirecting [people] to pages by naming the social networks concerned is a form of publicity that violates the provisions of Article 9 of the March 27, 1992 decree prohibiting surreptitious advertising." However, "redirecting TV viewers or radio listeners to the broadcast's page on social networks without mentioning them has an informational purpose." The CSA therefore called on TV and radio stations to find creative ways to mention their Facebook and Twitter pages without naming them.

The Public Prosecutor's Office sometimes shows its ignorance about new technologies by basing its decisions on a narrow interpretation of the role of information. The proceedings underway against Mikael Chambru, a volunteer journalist with news website La Voix des Allobroges, after he covered a demonstration, prove that. He was found to be a protestor on the grounds that he did not have a press card. The journalist would have faced a jail term of up to six months and a fine of USD 1,980, had the judge not dismissed the case in October 2011.

Meanwhile, in October 2011, the Court of Cassation recalled that the 1881 Press Law also applies to bloggers. The trial judges (of the Tribunaux de Grande Instance (TGI) – specifically the 17th chamber of the Paris TGI – are already applying this law by considering the specificity of the author of the incriminating article if he(she) is a blogger, notably in terms of good faith.

HADOPI law meets growing criticism

Aside from its omissions and shortcomings, the HADOPI law violates basic freedoms by making it possible to cut off people's Internet access. Reporters Without Borders continues to call for its repeal.

In his report released in June 2011, Frank La Rue, the United Nations' Special rapporteur on the promotion and protection of the right to freedom of opinion and expression stressed that "cutting off users from Internet access, regardless of the justification provided, including on the grounds of violating intellectual property rights law [is] disproportionate and thus a violation of Article 19, paragraph 3, of the International Covenant on Civil and Political Rights." In his report, the UN rapporteur specifically denounces France's "three-strikes [gradual response] law."

Yet the country is still enforcing its repressive approach to copyright protection. At a July 11, 2011 press conference, HADOPI [the French digital rights authority] announced that 18 million reports from digital rights holders (out of 22 million French Internet accounts in France!), 1 million IP address identifications, 470,000 initial warning letters, and 20,598 second warnings, had been made. HADOPI

said that it planned to hear 10 subscribers who had passed the "three-strikes" limit, and that it might transfer their case to the prosecutors. If convicted, they could be fined up to USD 1,980, and their Internet access could be suspended. Read the exclusive interviews of Jérôme Bourreau-Guggenheim, co-founder of SOS Hadopi and of Robert Thollot, an Internet user prosecuted by HADOPI for "blatant negligence," since he allegedly failed to adequately secure his FreeWiFi Internet access.

On October 19, 2011, the French Council of State rejected the action for cancellation filed by the French Data Network (FDN) and Apple objecting to the HADOPI law's decrees. The Commission nationale de l'informatique et des libertés (CNIL) withdrew its formal demand made to Trident Media Guard (TMG), a company that collects the IP addresses of alleged violators for HADOPI. Accused of having "inadequate security measures" following personal data leaks, TMG implemented certain procedures that seem to have satisfied CNIL, which closed the case. However, its litigation continues against TMG's designated representatives, the rights holders.

Reckless filtering?

Internet filtering is a violation of freedom of information, according to the Court of Justice of the European Union. The CJEU ruled that generalized Internet filtering violates the fundamental rights of European citizens, including the right to the free flow of information online. It also found that the protection of copyright cannot be assured at the expense of other basic freedoms such as freedom of information and privacy. The Court's decision clearly states that "measures which would require an ISP to carry out general monitoring of the information that it transmits on its network" are contrary to European law and violate fundamental rights.

Loppsi: French law on guidelines and programming for the performance of internal security

France nonetheless has continued to expand its abusive filtering methods. Loppsi had already provided for some administrative filtering that had been implemented in 2011. Other provisions have since been added.

LCEN's implementing decree

The draft decree implementing Art. 18 of the 2004 Law for Trust in the Digital Economy (LCEN) was denounced by the French National Digital Council in June 2011. It makes it legal to implement an administrative Internet filtering system according to very broad and vague criteria. The procedure provides for three steps based on the "notice-and-take-down" principle. Any blockings or content removals must be strictly limited and carried out within a legal proceeding framework. Reporters Without Borders is calling for the repeal of this decree.

The order to filter or remove content may be issued by several ministries, as well as by the National Authority for the Defense of Information Systems, an agency responsible for cyberdefense in France. Filtering is ordered without judicial review, and no recourse has been stipulated.

Consumer Protection Law

The draft Consumer Protection Law, aims to extend filtering and blocking to the violation of consumer rights. Its Article 10 includes a provision giving the DGCCRF (Directorate General for Competition, Consumer Affairs, and Repression of Fraud) the power to refer to a judge in order to block Internet websites that violate regulations governing consumer rights. Not only does this open the door to the overblocking of legitimate content, but the legal procedure is too expeditious to guarantee freedom of information.

During their review of the Law on October 4, 2011, the MPs rejected the amendment introduced by Socialist MP Corinne Erhel, who was advocating for a "moratorium on Internet blocking and filtering measures."

Unauthorized online gambling

Decree no. 2011-2012 of December 30, 2011 "on regulations for blocking an unauthorized online betting or gambling activity" requires "Internet service providers and website hosting companies" "to

stop this activity by using the Domain Name System (DNS) blocking protocol," an ineffective and dangerous mechanism.

The Copwatch saga

The way the Copwatch website case was handled perfectly exemplifies the fact that filtering is taking the course indicated by the authorities in charge of monitoring potentially illegal online content, even when that involves taking abusive measures. On February 10, 2011, the Paris Tribunal de Grande Instance (TGI) ordered the blocking of the Copwatch site (copwatchnord-idf.eu.org), which was charged with defaming policemen and disseminating personal information likely to endanger their lives. Full blocking was ordered, not just that of a few incriminating pages, as the Minister of the Interior was requesting. On the other hand, the latter was denied its request to block 34 "mirror sites" which it claimed reproduced the content, or to block "future websites." At the Minister's request, the Paris Tribunal had already ordered that the website be totally blocked. It had resurfaced in the meantime. Reporters Without Borders published a "Handbook for Bloggers and Cyber-Dissidents" outlining netizens' rights, as well as their duties.

Internet neutrality in jeopardy

Filtering is becoming commonplace, even without adequate judicial supervision. The networks' increasing privatization and their potentially arbitrary and discriminatory management are also impeding Internet neutrality. News website Owni revealed in November 2011 that unlimited household Internet access may be prohibited, while the daily newspaper *Les Echos* objected to the slower Web browsing speeds some mobile phone users are experiencing.

The "Telecoms Package," a set of European Union measures transposed into French law in August 2011, has proved disappointing in terms of Internet neutrality, which it partially challenges. No parliamentary debate was held despite what was at stake in this legislation – which changes the concept and vision of the Internet in France – thus displaying the government's flagrant lack of real commitment to consumers.

The order remains highly permissive in terms of Internet neutrality. Article 3, which states that the minister responsible for electronic communications, together with the Electronic Communications and Posts Authority (ARCEP), "promote the capacity of end users to access and disseminate the information of their choice and to access the applications and services of their choice," has no binding value. Article 33, which describes the information that should appear on an Internet subscription contract also does not guarantee Net neutrality, and instead just refers to the principle and demands more transparency on the subject. The contract must inform consumers about the procedures that can be used "to measure and direct traffic so as to avoid saturating or over-saturating a network line and the consequences as regards the quality of service." The effect of this is to endorse practices that violate Net neutrality, and it suggests that ISPs can reduce broadband capacity in accordance with consumer volume, a point already raised by certain ISPs.

Other points remain particularly problematic: the lack of binding measures as regards the protection of personal data, the obligation imposed on ISPs to inform their clients about risky Web activity and its legal consequences, and the state's use of electronic communications for security and public order purposes. Even more serious, especially after the recent riots in the United Kingdom, is the provision that allows the government to be able to disrupt communications.

French corporate responsibility

Last August, *The Wall Street Journal* visited a telecommunications surveillance centre in Tripoli and confirmed by means of a photo of the Amesys logo, that this French company belonging to the Bull Group had in fact supplied Libya with its Eagle massive Internet surveillance system, to be used mainly for intercepting emails on Hotmail, Gmail and Yahoo! messaging services, and for monitoring the MSN and AIM instant messaging services. Among individuals spied upon were Libyan journalist Khaled Mehiri and several opposition activists. France Telecom allegedly holds a 10% share of Amesys' stock. French Defense Minister Gérard Longuet denied any responsibility on the part of the French government, and stated that no ministerial committee had ever been solicited to (or to not) authorize the sale by French companies of Internet surveillance systems to Libya and Syria. The Sherpa

association filed a complaint in hopes that an investigation will be conducted to shed light on this transaction and eventually identify those responsible.

The firms Alcatel-Lucent, Eutelsat and Thalès were also slammed by some NGOs, including Reporters Without Borders, for their respective activities, mainly in Burma and China. WikiLeaks' Spy Files highlight, as shown by the map posted by the Owni website, the respective surveillance market segments held by the companies Alcatel, Qosmos, Amesys, Vupen, Septier, Scan & Target, and Aqsacom. Reporters Without Borders is urging French authorities to demonstrate transparency about their relations with these companies and to take concrete national, European, and international measures (see "General Introduction"), to prevent French companies from exporting surveillance equipment to countries that violate human rights.

France's Internet position in the global arena: A series of missed opportunities.

France has chosen to stray from the line taken by some 40 countries with regard to basic Internet freedoms. French Foreign Minister, Alain Juppé, has in fact refused to endorse the UN declaration recognizing Internet access as a fundamental right, conditioning his signature on the recognition of intellectual property as a right equivalent to freedom of expression.

In such a climate, the eG8 conference held in May 2011 in Deauville was bound to be a missed opportunity. Civil society voiced its concerns, and denounced abusive attempts to regulate the Net. Official discourse ranged from the notion of a "civilized" Internet to that of a "responsible" Internet. Priority must be given to defending a free Internet accessible to all.

In late February, Reporters Without Borders asked the 2012 French presidential candidates to sign the "Pact 2012 for press freedom in France," and notably commit to "ensure free Internet access, guarantee neutrality and abandon the use of administrative filtering by favoring solutions mutually worked out with host companies in order to facilitate the free flow information online."

INDIA

NEW COUNTRY UNDER SURVEILLANCE

Ever since the 2008 Bombay attacks, the authorities have been intensifying their Internet surveillance and pressure on technical service providers while publicly denying censorship accusations. The national security policy of the world's largest democracy is undermining online freedom of expression and Internet users' privacy.

An increasingly connected population

The Internet is experiencing impressive growth in India. By 2014, the country should have nearly 300 million netizens, as compared to about 100 million in late 2011. Wireless Internet, especially mobile phone Internet, is spreading as quickly as the price of smartphones is dropping.

This trend has led authorities to more closely monitor what is happening on the Web. According to the Google Transparency website, which logs the Internet content removal requests that Google receives from governments, Indian officials have asked Google multiple times (67 to be exact, between July and December 2010) to remove 282 content items (namely videos critical of politicians) from YouTube and several blogs. Google allegedly complied with 22% of the requests.

Netizen loses her life

Even the most influential netizens are not safe from a physical attack. On August 16, Shehla Masood, a Right to Information (RTI) blogger and activist, was shot dead in front of her home in Bhopal (in central India) while on her way to a demonstration in support of Anna Hazare, a civil society leader and anti-corruption campaigner who had been arrested earlier that day. Reporters Without Borders has asked the Indian authorities not to let this crime go unpunished.

Authorities pressure Web hosting service providers

Several meetings were held throughout 2011 between Indian Information Technology Minister Kapil Sibal and sector representatives. The New York Times reported that the Minister wanted hosting companies and Internet service providers to prescreen user content conveyed by their services and banish those that "threaten India's unity, integrity, defense, security and sovereignty, its relations with foreign governments or the public order." Apparently the companies flatly refused to comply because of the volume of data that would have to be processed. Later, in an interview granted to the *NDTV* network, Kapil Sibal denied having ever made such a request.

The authorities have already clamped down on several mainly file-sharing and streaming websites without any ruling on the illegality of such actions. Anti-corruption cartoonist Aseem Trivedi saw his website, "Cartoons Against Corruption," which features humorous anti-corruption drawings suspended by his hosting company in late 2011. The cartoonist has since transferred his drawings to a new site.

Weary of trying to convince companies to self-regulate, the Indian government decided to resort to legislative and legal means to achieve its goals.

Dangerous legislation

The "IT Rules 2011," which pose a threat to online free expression, were adopted in April 2011 as a supplement to the 2000 Information Technology Act (ITA) amended in 2008. These regulations notably require Internet companies to remove any content that is deemed objectionable, particularly if its nature is "defamatory," "hateful," "harmful to minors," or "infringes copyright" within 36 hours of being notified by the authorities, or face prosecution. This has turned technical intermediaries into Web censorship police informants.

Also, although some content categories are justifiably objectionable, other more vague or subjective definitions could jeopardize informational content.

The companies concerned have strongly criticized the rules. The Internet and Mobile Association of India (IAMAI) found that these would impede the development of India's social networks: "The rules seem to step on the statutory side, biased towards the complainant. Even before a case is filed in court, the website has to take down the content. It might harm freedom of speech on the Internet." Some sector companies have pointed out the risks of self-censorship and reduced the free flow of information.

The IT Rules also impose on cybercafé owners drastic regulations that violate personal data privacy and place a presumption-of-guilt burden on all Indian netizens: they must photograph their customers, follow instructions on how their cafés should be set up so that all computer screens are in plain sight, keep copies of client IDs and their browsing histories for one year, and forward these data to the government every month.

This new legislation has allowed individuals to institute civil and criminal proceedings against some 20 Web companies.

Legal proceedings likely to create dangerous precedents

Within the context of such legal proceedings, Reporters Without Borders has called on the judiciary not to hold ISPs liable for content published by third parties on Web platforms.

One of the first civil proceedings concerns 21 Internet firms (including Google, Yahoo!, Facebook, Youtube, Blogspot, the social network Orkut and the Exbii forum) accused of hosting "offensive" content. It was initiated by Mufti Aizaz Arshad Kazmi on grounds that these companies hosted content disrespectful of religious beliefs. On December 23, 2011, a New Delhi civil court had ordered that all "obscene" content be removed by February 6, 2012. At the hearing, Justice Suresh Kait had even threatened to block, "like in China," any recalcitrant Web platforms that refused to install a content-screening system.

The Indian affiliates of Google and Facebook complied with the Indian court's injunctions and removed the incriminating content from their Indian Internet domains. Facebook's parent company, on the other hand, stated that it could not comply with the Indian court's demands since its servers are based in the United States. Yahoo!, Microsoft and Google also asked that the allegations against their services be withdrawn since they are not liable for content hosted on their Indian servers. On February 6, the judge asked the 22 firms to submit within 15 days a report detailing what steps they had taken to block "offensive" content.

In addition to this civil case, criminal charges were filed on December 23, 2011 by journalist Vinay Rai against the directors of these same Internet companies. He alleges that these companies are hosting content critical of religion and politicians that is "offensive" and likely to disrupt law and order. The New Delhi High Court, to which Google and Facebook had appealed the case, refused to dismiss the charges. Google India argued that as a Google Inc. distributor and subsidiary, it cannot control all content posted on Google, Youtube, Orkut, and Blogger in India. During arguments, Google pointed out that controlling or filtering the massive number of documents passing through its servers would be humanly impossible. For example, 48 hours of video is posted on YouTube every minute.

During the February 14 and 15 hearings, the defense raised several thorny points that weakened the charges brought against the Internet companies. The "notice-and-take-down" process provided for under IT Rules, according to which the hosting company must remove the content as soon as it is notified to do so by the authorities, had not been complied with. The accused Internet companies had received no request from the competent authorities to remove the content since the plaintiff, Vinay Rai, had submitted the matter directly to a criminal court. The companies' lawyers also invoked Section 79 of the IT Act, which stipulates that no ISP can be held liable for objectionable content posted via its servers by third parties if the former can prove that it had no knowledge of such content, or that it had taken the necessary steps to prevent such infraction. However, the lawyer representing the New Delhi police argued that since the companies had been informed by the government's Department of Information Technology that some content on their servers was "offensive," the exemption under Section 79 did not apply. The judge called on the Department to provide documentary proof of this allegation.

Lawyers for Google and Facebook objected that the Indian government could not constitute a civil party in litigation between private parties. Reporters Without Borders is concerned about the impact of such an intrusion by the state into legal proceedings, which threatens the independence of the courts.

Is this purely a coincidence? On February 13, 2012, *The Wall Street Journal* revealed that an investigation had been opened to determine whether the Indian affiliates of Google and Yahoo! had violated India's foreign exchange laws.

Ongoing arm-wrestling between the government and Internet companies

Since platforms and technical intermediaries are claiming that they cannot comply because their servers are not based in India, the authorities have announced that they would require them to have a physical location on Indian soil. Foreign companies offering email services, including Yahoo! and Gmail, are now expected to route all emails exchanged through their websites via local servers. The Indian press reported that during a meeting in the office of India's Minister of the Interior, the Department of Information Technologies was instructed to notify these firms of the new directive as soon as possible.

For the moment, Yahoo! is routing emails via servers based in India only for online accounts registered in India. Emails sent by accounts registered abroad (addresses ending in yahoo.fr, for example), however, are routed through servers based abroad, which means that Indian security services cannot inspect them without first making a formal request to the government of the country concerned.

Indian security services also supposedly contacted mobile phone operators to ask them to set up a client surveillance system, according to *The Economic Times of India*. Some mobile phone operators are also suspected of having collaborated with these services. The United States government is looking into the alleged hacking of email accounts belonging to U.S. Congress committee members.

Smartphones and VoIP under close surveillance?

For months, the authorities have been pressuring BlackBerry smartphone manufacturer RIM (Research In Motion), as well as Google and Skype, to give them access to communications exchanged by their users. India's Ministry of the Interior, which is responsible for national security, is trying to gain real-time access to all communications routed through the Indian network, including Internet telephony (VoIP) services.

During a January 2012 meeting at the Telecommunications Ministry, the security services voiced their desire to gain access to the encrypted communications exchanged via the BlackBerry Enterprise Service (BES). RIM insists that it does not have access to the encryption keys used by BES clients. To accomplish this, the authorities plan to negotiate directly with the 5,000 companies using BES in India, so that they can contact the companies concerned and demand their own encryption key.

In view of its treatment of Internet sector – particularly foreign – companies, India seems engaged on a course of increasingly tight surveillance, which constitutes a threat not only to individual liberties, but also to innovation and trade. India's Minister of Communications and IT Kapil Sibal affirmed in February 2012 that India will never censor social media. It is to be hoped that these promises will be kept.

KAZAKHSTAN

NEW COUNTRY UNDER SURVEILLANCE

Kazakhstan, which considers itself a regional model after holding the rotating presidency of the Organization for Security and Cooperation in Europe (OSCE) in 2010, seems to be straying from its fine promises to embark without detours on the road to cybercensorship. In 2011, a unprecedented social protest movement prolonged by a violent uprising, a wave of odd attacks and the Head of State's health problems made the authorities even more nervous, causing them to tighten their control over information, especially online.

Website filtering and blacklists

Some twenty websites deemed "extremist" were blocked on August 20, 2011 by order of a district court in Astana (the capital), which ruled that the sites were helping to promote "terrorism and religious extremism" and contained "calls commit acts of terrorism and to manufacture explosive devices." Unexpectedly, those blocked sites include the highly popular Russian-language blog platforms LiveJournal and LiveInternet. The blockage of these platforms seems totally unfounded, since much of the banned content has nothing to do with the terms of the decision. The latter was denounced by bloggers, notably by means of an online petition.

According to the report "Central Asia: Censorship and Control of the Internet and Other New Media" by the International Partnership for Human Rights coalition, Net filtering is carried out with the assistance of the leading ISP Kazakh Telecom, which controls most of the bandwidth.

The report stresses the lack of transparency of the work done by the "Center for Computer Incidents," which involves drawing up blacklists of "destructive" websites. A presidential Security Council is already compiling lists of websites that should be blocked. According to this body, 125 websites containing "extremist" elements had been blocked by October 1, 2011. Measures are underway to block 168 more.

News websites in the authorities' line of sight

The pretext of the fight against terrorism is frequently used by the authorities to justify temporary or long-term blocking of independent news sites such as eurasia.org.ru, respublika-kaz.info, kplustv.net and krasnoetv.kz, which provide alternative insight into the struggle to replace ailing Head of State Nursultan Nazarbayev, and into the most publicized and longest wave of protests in Kazakhstan's history and subsequent unrest. Censorship gained ground the country last year. Its main thrust was an attempt to impose a blackout on news about the strikes in the oil sector, and debates over the assertion of a "terrorist" threat in a country previously spared by this phenomenon. Bombings in the western city of Aktobe in May 2011, and later in the northern town of Taraz in November, fueled speculations that they could be attributed to an organized crime plot involving Islamist insurgents or Kazakh secret service forces.

News website guljan.org, which is highly critical of the authorities' abuses and corruption, is blocked on a regular basis, and sustained massive cyberattacks shortly after it was launched. The site and its editor, Guljan Ergalieva, were fined 5 million tenge (about USD 33,800) in damages for "attacking the honor and reputation" of senior official Sarybay Kalmurzaev in January 2012.

News website *Stan TV* has been constantly hounded by the authorities, with "inspections" of all kinds, attempted bribery, threats, attacks, and court orders aimed at closing the offices. The website produces reports that are regularly broadcast *K+*, an independent satellite station devoted to Central Asian news, which is very critical of Kazakh authorities. *Stan TV* is a popular leading source of news on the conflict that has been going on for several months between the regime and striking employees of the Karajanbasmunay and Uzenmunaygaz companies in the western province of Mangystau. Two *Stan TV* journalists were violently assaulted while covering these events.

Clampdown on dissent: A region cut off from the world

On December 16, 2011, the celebration of Kazakhstan's 20th anniversary of independence was disrupted by workers who had been on strike for several months in Zhanaozen (in Mangystau). Under what are as yet unclear circumstances, the police fired real bullets into the crowd and the rebellion spread throughout the city, where most of the official buildings were burned. The official toll is at least 15 dead, but alternative sources claim the number is higher. The authorities responded by declaring a state of emergency and imposing a news and communications blackout, preventing any accurate assessment of the situation. The protest's epicenter – Zhanaozen and surrounding cities within a radius of at least 39 miles – have been totally cut off from the world and deprived of Internet connections and telecommunications. Elsewhere in the region, and particularly in the city of Aktau (the provincial capital) where tense demonstrations persisted for several days, it was very difficult, if not impossible, to exchange SMS messages or access the Internet from a mobile phone.

In the absence of updates from the state press agency, preoccupied with independence festivities, Twitter, Facebook, and *K+* labeled videos on Youtube have become the only sources of information – or disinformation – as reported by Global Voices. On December 16 and 17, on Twitter, the key word #Zhanaozen produced countless alarming tweets about "massacres" and "the civil war in Zhanaozen." The uncertainty grew when Twitter, along with a number of Russian and Kirghiz media, were blocked in the evening of December 16. Heated debates about a possible propaganda or counter-propaganda operation filled the Kazakh Web.

Although Twitter was soon accessible again, several leading news websites remain blocked, including Guljan.org, the Russian citizen news agency Ridus.ru, and the site of the opposition newspaper *Respublika*. For several days, the security services first prevented journalists from accessing the offices of these media by blocking their entry or even stopping them for questioning them on their way there. Then they let them through, but tried to interfere with their work as much as they could by imposing an escort or preventing them from meeting certain people. In several cases, the content of their computers, USB flash drives and audio recorders were closely examined. Blogger Murat Tungishbayev was brutally assaulted while filming a police check.

On January 26, 2012, the Public Prosecutor's office announced charges against the organizers of the social protest movement that degenerated into riots, the opposition leaders who supported them, and journalist Igor Vinyavsky, editor-in-chief of the newspaper *Vzglyad*. The authorities also pledged to pursue the policemen accused of killing demonstrators, allegedly corrupt high-ranking officials (including Zhanaozen's mayor), and executives of the oil companies employing the strikers. These latest measures are viewed as a gesture to calm a population who is becoming increasingly unwilling to put up with the rampant corruption of its bureaucrats. Meanwhile, a genuine manhunt was initiated to identify those who took the videos proving that policemen had fired into the crowd. The *Stan TV* staff members who had broadcast them have had to endure even greater pressure. On January 13, 2012, the National Security Committee (KNB) called in most of the news staff for questioning.

Repressive regulations

A 2009 Internet Law puts bloggers in the same penal category as journalists and holds Internet website administrators and their ISPs responsible for any content posted by others on their platforms, obliging them to hire moderators.

Criminializing defamation has consequences for online freedom of expression, yet officials are entitled to special treatment. Media and journalists critical of the government often pay for it, as shown recently in the Guljan.org case (see above).

Within the framework of a policy that centralizes all news sources inside the country, a September 2010 decree forced websites using the suffix .kz to channel all their traffic through servers based in Kazakhstan. Originally implemented for newly created sites, it gradually was applied retroactively. In May 2011, the government had insisted that Google use only servers located in Kazakhstan so that it would be easier for the authorities to monitor searches. It reversed its decision after Google announced in June 2011 that it was leaving the country and suspending google.kz.

On December 30, 2011, new repressive regulations on Internet access were adopted. A decree made video surveillance and filtering equipment mandatory in cybercafés. Visitors are now required to present an ID and managers must maintain a log of the websites visited. Most importantly, cybercafé owners are required to provide the security forces, simply upon request, access to their visitor register, the log of sites accessed, and the video surveillance recordings. They must also keep a record of security services' requests. In addition, owners must install a program allowing access to banned websites to be blocked. The use of proxies is prohibited, and the sanctions for such violations are not yet known. They will undoubtedly be the subject of a forthcoming application order. These new rules are a severe blow to cybercafés, which are already closing one after the other while the number of individual Internet and mobile phone accounts keeps on growing.

The authorities' agitation vs. the international community's silence

The increased use of cybercensorship is symptomatic of the harsher repression being waged by a regime worried about the end of the "Kazakh stability" myth. Yet Astana leaders are still strong. Despite the many frauds attested to by OSCE observers during the last elections, people did not riot in the streets. The international community remains discreet about human rights issues. Nursultan Nazarbayev can count on Kazakhstan's vast natural resources to lessen global criticism. One recent example is the recent USD 3 billion partnership agreement concluded in February 2012 between Kazakhstan and Germany.

MALAYSIA

COUNTRY UNDER SURVEILLANCE

Malaysian emulators of Arab Spring caught Kuala Lumpur authorities off guard, but they are using all means possible to quash the Bersih 2.0 protest movement. Preventive arrests, pressures on bloggers and the media, and website blockings during local elections are omens of worse yet to come for the general elections. The campaign is expected to play out primarily on the Internet, which remains a favorite space for expression in a country where the traditional press is regularly muzzled by the regime.

See the Malaysia chapter of the 2011 "Enemies of the Internet" report.

High-risk general elections?

Political campaigning and freedom of information are not compatible in Malaysia. In the run-up to the local elections in Sarawak (on the island of Borneo), in April 2011, many opposition and news websites were the target of DDoS-type cyberattacks, including those of Sarawak Report, Radio Free Sarawak, Dayak Baru Blog and Malaysiakini. This use of cyberattacks to regulate Internet content does not bode well for the general elections expected in 2012, at a time when online bloggers and journalists will have the crucial role to play of informing the population. Some bloggers such as Wong Chin Huat (researcher), Sivarasa (lawyer and MP), and Haris Ibrahim (lawyer) were denied entry to the island.

In July 2011, 30,000 Malaysians representing all strata of the population, rallied in the streets in response to Bersih 2.0's call for transparent elections. A general election should take place by March 2013. Both before and during the protest rally, which united Malaysia's entire civil society, the authorities arrested hundreds of opposition and human rights activists and threatened to prosecute those media that denounced police violence. The capital, Kuala Lumpur, was literally closed down on the eve of July 9, 2011 by police roadblocks set up to systematically search all vehicles, and T-shirts with a Bersih logo, or even yellow T-shirts (the organization's logo color) were banned. The anti-government Malaysiakini website was then subjected to a new wave of cyberattacks.

Bloggers and netizens under pressure

A dangerous precedent was set for journalists and bloggers who cover political scandals: blogger Amizudin Ahmat was sentenced to pay exorbitant damages and costs of up to 300,000 Malaysian ringgits (approximately USD 100,000) to the Minister of Information, Communications and Culture, Rais Yatim, for an article judged defamatory, despite his apologies and the retraction of the offending article.

A defamation suit was launched against another blogger, Ahmad Sofian Yahya (Sekupangdua) who exposed a misuse of power, accusing deputy Nga Kor Ming of arranging for a contract with the State of Perak to be awarded to his wife's company. The blogger retaliated by filing a countersuit against the politician.

The charges against satirical blogger Irwan Abdul Raman, who blogs under the name Hassan Skodeng, were dropped in March 2011. He had been charged with disseminating false news after posting a humorous message about "State warming." He thanked the blogger community for their support. His lawyer stated that he hoped such cases would not "kill satirical talent in the country."

Political cartoonist Zunar, charged with "sedition" for having posted satiric drawings about his country's political and social situation, whose books are still banned from publication in Malaysia, presented a solo exhibit of 80 of his cartoons in London entitled "To Fight through Cartoon."

Real legislative reform or empty promises?

In an effort to bolster his image as a reformer, Prime Minister Najib Tun Razak announced in September 2011 a repeal of the draconian Internal Security Act (ISA), which had been used until then by the authorities to arbitrarily pursue and detain journalists, bloggers and opposition leaders in order

to serve their political ends. One year earlier, peaceful vigils had been held to ask for such that repeal. Although this announcement was welcomed by the traditional media and by certain international media, the opposition and online media are recommending vigilance, for just a few months earlier, in December 2010, a cyber sedition bill had been introduced in the Council of Ministers.

Social media "junkies"?

According to comScore, a leading online audience measurement company, one-third of the time spent online in Malaysia is devoted to using social networks. Facebook now exceeds 12 million users vs. 470,000 for Twitter.

The new media appear to be the most effective remedy to compensate for self-censorship. Election forecasts, as well as corruption cases, or negotiations on the installation of the next nuclear power plant can be broached there more freely than anywhere else. Genuine political debates are held online, not in the traditional media, which leaves the Internet and bloggers particularly vulnerable in a pre-general election climate.

RUSSIA

COUNTRY UNDER SURVEILLANCE

The authorities have used the issue of national security to expand Web monitoring and censorship – even while continuing to promote and develop Internet access for the population at large. The Web has played a key role in the political debate prompted by legislative and presidential elections and in the post-election mobilization of the opposition and civil society. These developments provoked a strong official response. The blogosphere has grown stronger and better organized in the face of state attacks.

Government anti-"extremism" campaign hits Internet content and access

Prime Minister (now President-elect) Vladimir Putin said on 9 February 2012: "Negative phenomena exist everywhere, including on the Internet, and should not be used as a pretext to limit Internet freedom." However, the authorities have used the justification of preventing violence to reinforce their control of the Internet, with the Federal Security Service (FSB) taking steps to close a number of online organizations in late 2011. Most of these groups have clearly called on their members to respect the law and not to let themselves be provoked into violence.

The government list of "extremist" content, as well as the boundaries of the category itself, keep growing. It now includes everything touching on religion and issues of ethnicity, which have become taboo subjects on RuNet – as the Russian Internet is known. That list is the basis of official demands to take down content, and of actions to block site access (see the Russia chapter in the 2011 report on Enemies of the Internet).

The process of domain name registration could affect freedom of expression online by leading to closure of more sites. New rules promulgated by Nic.ru, the biggest Russian domain name-registration company, allow the cancellation of domain names for inciting violence, "extremist" activity, advocating overthrow of the government, activity in conflict with human dignity or religious beliefs. The rules reflected new official regulations. Domain name-registration companies are authorized to suspend names in the .ru and .rf (pΦ) domains upon written notification from "agencies conducting an investigation." That provision would potentially authorize prosecutors, the FSB, the police, or the drug enforcement agency (FSKN) to order such a move.

In Tomsk, Siberia, the broadcast arm of Roskomnadzor, the federal mass communications supervisory agency, has recently pressured the regional television network *TV-2* to stop transmitting two news programs by *Dozhd*, the first Internet TV network in Russia, whose content is critical of the government.

Anatoly Baranov, owner of the forum.msk.ru discussion platform, states that the Yandex search engine filtered out news items from his site on Yandex.News searches.

Danger of the spread of online monitoring and censorship

Roskomnadzor, whose regulatory authority extends to information technology and mass communications, has announced that it has installed online software to detect "extremist" material. The sites identified through this process will be given three days to take down content that meets this ill-defined standard. If a site does not comply, two additional warnings will be sent. The site will then be shut down.

The software was to go into operation in test mode in December, 2011. Its full deployment has been postponed indefinitely. Nevertheless, it carries the risk of system-wide monitoring of the Russian Web and could lead eventually to the taking down of all content that displeases the authorities.

The justice ministry, for its part, has invited bids to create its own monitoring system of content on the Internet. Such a system would allow close examination of all content touching on Russian government and justice systems, and any European Union statement concerning Russia.

Bloggers under pressure

Prison sentences and violent attacks were less frequent in 2011, except during the election campaign period. Yet legal proceedings and pressures of all kind continue – above all when the activities of netizens focus on sensitive topics and powerful interest groups.

Maj. Igor Matveev of the interior ministry garrison in Vladivostok has been prosecuted on charges that seem to have been prompted by his revelations last June of practices in the military region where he served. He reported that troops were served dog food in cans falsely labelled as containing beef stew. He faces a possible 10-year sentence.

Yuri Yegorov, a former employee of the regional government of Tatarstan's human rights ombudsman's office, received a six-month suspended sentence last June, as well as two years of probation, for defamation. He had revealed a case of alleged corruption in the ombudsman's office, headed by Rashit Vagiov, that took place from February to July 2007.

Leonid Kaganov, a prominent blogger, was forced last May to house his site abroad. In 2009, the FSB had demanded, through his hosting service, the removal of an anti-Semitic poem that was on his site because he had mocked it.

Roman Hoseyev is the target of administrative action for having quoted from "Mein Kampf" on a site in 2005, before the 2010 banning of the book in Russia. He had drawn comparisons between statements by US President George W. Bush and Hitler.

No information has been received about the fate of a Navy conscript who blogged under the name Vasily, publishing on Twitter under the name Sosigusyan. He denounced hazing and poor living conditions in his unit. His Twitter account was hacked and the content about the military taken down, except for the last three posts, which were written by another person.

Propaganda and cyber-attacks

In addition to mounting a campaign of repression against online oppositionists, the Kremlin deploys its own cyber-weapons. Several thousand Twitter accounts were hacked at the end of 2011 in order to flood social media with pro-government messages, using hashtags popular with oppositionists (notably, #navalny, from the name of the well-known political activist and anti-corruption blogger Alexei Navalny, and #триумфалънпая, from Triumfalnaya Square in Moscow).

Many Russian bloggers have pointed to a wave of "bots" unleashed against the LiveJournal social media platform. Oleg Kozyrev, an opposition blogger, has counted more than 2,000 of these software weapons.

Oppositionist Navalny's e-mail inbox has been hacked, with the contents displayed on a site called navalnymail.kz. According to several bloggers, this action could be part of a government-organized campaign to discredit Navalny.

The wave of cyber-attacks peaked at the time of the legislative elections last December. A series of Distributed Denial of Service attacks paralyzed sites critical of the government before and during the vote, apparently to silence the dissidents. Access to LiveJournal, which hosts blogs critical of the Kremlin, was blocked for three days, starting on 1 December 2011. The site had already suffered a DDoS attack the month before.

Among other Web targets are:
- *Echo of Moscow* radio's site, Echo.msk.ru
- The independent daily *Kommersant*'s site, komersant.ru
- The election-monitoring NGO's site, golos.org
- KartaNarusheniy.ru, an interactive map created by Golos to track reports of election fraud
- Gazeta.ru, an independent news site
- Lenizdat.ru, a Saint Petersburg-based independent news site
- Slonl.ru and Newtimes.ru, opposition sites which posted the Golos map after Gazeta.ru took it down
- Ridus.ru, a citizen-journalism site
- Doshdu.ru, the site of *Dosh*, an independent news magazine about the Russian Caucasus

- Zaks.ru, a news site on the northwest region.

Some media organizations and opposition groups, having anticipated these developments, migrated to social networks and called on their readers to follow them on Twitter and Facebook in the event that their sites went down.

Disputed elections, attempted control of online political debate

Most traditional media organizations, notably television networks, are under Kremlin control, genuine political discussions have been possible only online. Any measure deemed necessary to uphold the country's strongman, Putin, has been considered appropriate.

Even before and during the legislative elections, debates had been hindered by cyber-attacks and by the arrests of journalists and bloggers. Those detained included Alexey Sochnev, the editor of the independent news site Besttoday.ru; Maria Plieva, a prominent blogger in Ossetia; and the president of Golos, Lilia Chibanova.

Golos' interactive election-fraud monitoring map proved to be a great success as the elections unfolded. Thousands of videos showing irregularities at voting places were posted to the site, prompting Russians to take to the streets in great numbers to denounce election fraud. Navalny and many journalists were arrested during these post-election demonstrations,

The great majority of traditional media organizations – especially television networks – ignored these events. Instead, they provided largely favourable coverage of Putin's party, United Russia, which swept the legislative elections.

The social media site Vkontakte, which has more than 5 million members in Russia, found itself in the government spotlight. The FSB told the site's founder and director, Pavel Durov, to shut down seven groups calling for demonstrations last December (including a group rallying to defend the ruling party). A Russian blogger estimated that up to 185,000 netizens subscribed to protest-organizing groups. A spokesman for Vkontakte said publicly that the site would not practice censorship and would not carry out the FSB order. Following the statement, Durov was summoned to appear before prosecutors in Saint Petersburg on 9 December.

Regional discussion forums, very popular at the provincial level, with most participants anonymous, have become a favourite resource for political debate among Russian netizens, and a nightmare for the authorities. However, these sites are less powerful than the national media and easy to censor, though that has not prevented netizens from migrating to other sites, hosted abroad. At least three forums were closed or suspended during the months leading up to the early December elections.

One of these sites is the Kostroma Jedis regional forum, which was targeted following the posting of two satirical videos criticizing Igor Slyunyaev, governor of the Kostroma region, some 300 km northwest of Moscow. In November, other forums were shut down or purged of all political content by their administrators. One such case occurred in the Arzamas, a city 410 km east of Moscow, affecting the mcn.nnov.ru site. Another took place in the west-central city of Miass, 95 km west of Chelyabinsk, affecting the forum.miass.ru site. It is not clear if these were cases of official action or self-censorship. In either case, the closing of these forums signifies a narrowing of the possibilities for political debate on the Russian Web.

In the run-up to the presidential election in March, Golos, the election-monitoring NGO, put up a new version of its interactive map to track election fraud, with stronger defences against cyber-attack. Navalny, the activist and blogger, mounted a site, Rosvybory.org, to assist citizens in becoming presidential election observers.

The campaign of repression mounted for the legislative elections illustrated the official attitude toward protest. And the official response was designed to create a deterrent to popular action in the presidential election period. Tensions grew during the months between the two elections. On 17 February, Reporters Without Borders denounced a wave of intimidation aimed at national independent media. Major targets included *Echo of Moscow*, *Novaya Gazeta*, an independent newspaper, and *Dozhd*, the online television operation. The latter organization received a fax on 16 February from the

Moscow prosecutor's office, demanding detailed information on the "network's financing for coverage of mass demonstrations on 10 and 24 December."

These barely veiled accusations against *Dozhd* track precisely with statements by Prime Minister Putin, who had publicly accused demonstrators of having acted at the encouragement of the US state department. Roskomnadzor, the mass communications authority, had already required *Dozhd* to defend its coverage of the December protests. After examining in detail the images that the network had transmitted, the agency finally concluded that they contained nothing objectionable.

Journalists were again arrested and beaten during the post-election demonstrations of 5 March 2012. The clear goal was to prevent coverage of the demonstrations. However, contrary to what was seen in December, cyber-attacks seem to have been set aside – for now.

Export of the Russian model of Web control?

Russia has played a leading role on the international scene in promoting its vision of the Internet and exporting its Web control strategy. Moscow has proposed to the UN, together with China, Uzbekistan and Tajikistan, an Internet conduct code designed to provide "information security."

The impact of the Kremlin's policy is all the greater because the RuNet sphere of influence extends throughout the region, influencing countries such as Belarus and Kazakhstan in their Internet monitoring and censorship programs.

SOUTH KOREA

COUNTRY UNDER SURVEILLANCE

While the world's eyes were riveted on Pyongyang during the transfer of power in North Korea, South Korea clamped down even more on online content related to its neighbor, which continues to expand its Net presence for propaganda purposes. Censorship is also focused on political opinions expressed online – a critical topic in this electoral year. The National Security Law must be reformed without delay.

Content removals soaring

Under the conservative government of Lee Myung Bak, who has been in power since 2009, the number of content removal requests issued by the Korean Communications Standards Commission (KCSC) has been soaring. According to the blog NorthKoreaTech, they rose from about 1,500 per year before 2009 to 80,449 in 2010. The procedure lacks transparency due to the typically unclear way in which the Commission functions. Similarly, the number of investigations climbed from 58 before 2009 to 91 in 2010. There were already 150 cases as of August 2011. According to the Public Prosecutor's Office, 122 pro-North Korean websites were investigated between August 2010 and September 2011. It is estimated that 78 of them have been shut down.

North Korean censorship

North Korean information censorship, which has been intensifying, has taken on a special meaning in the context of the recent transition of power in Pyonyang. Social networks are the new battlefield between the two Koreas which, in the absence of a peace treaty, are officially still at war.

In late 2011, the KCSC, whose job is to regulate Internet content, was instructed to set the standards for Facebook and Twitter users and smartphone owners. These users will be required to delete any "harmful or illegal" content related to pornography, gambling, drug use, or disseminating false information, libelous statements, or pro-North Korean comments. The Commission's President told Agence France-Presse: "We also target posts and sites that support North Korea or praise its leaders, because their number has been rapidly increasing this year."

More than a reaction to many dramatic current events, this measure is in keeping with the North Korean regime's Internet charm offensive. The regime began using social networks in 2010 to more effectively wage its propaganda war. However, the vast majority of the population does not even know the Web exists (see the North Korea chapter of the 2011 "Enemies of the Internet" report). The Internet website uriminzokkiri.com symbolizes the country's official presence on the Web. However, in late 2011, it began posting anti-South Korean and anti-U.S. visuals, urging its supporters to circulate them on the social networks (see the North Korean chapter of the 2012 "Enemies of the Internet" report).

South Korea's counterattack has not been restricted to online initiatives, but includes the arrest and intimidation of pro-North netizens, thanks to the legal means provided for under the 1948 National Security Law.

The most recent example of the obsolete and arbitrary nature of this Law and its application is Park Jeong-geun, who was arrested in January 2011 for retweeting messages such as "Long live Kim Jong-il," and now faces up to seven years in prison. The young man claims that these were just sarcastic messages meant to poke fun at North Korean leaders.

Another South Korean, Kim Myung-soo, who was arrested in 2007 and later released on bail, is still fighting the charge of "aiding the enemy" by selling "pro-North Korean" books online. The army is also investigating some 70 officers who allegedly subscribed to a pro-North Korean community website. The Defense Ministry claims that seven or eight of them engaged in "questionable" conduct by posting messages on this site and plans to investigate them more thoroughly. The others may have joined out of mere curiosity.

Politics and the Internet: "A complicated relationship"

A KCSC member who was testing the limits of censorship was himself censored. He was using his blog to instruct Internet users on the type of content targeted by censors. Pressured by other KCSC members and the threat of seeing his blog shut down, he was forced to remove what was deemed to be "sensitive" content.

Political comments are considered highly sensitive and are closely monitored in South Korea. On January 13, 2012, the National Electoral Commission lifted the ban on using Twitter and social networks to discuss politics. This ban had been judged "unconstitutional." Two elections are scheduled in 2012. Over 100 people are charged with violating election laws.

One of the country's most influential political commentators, Kim Eo-jun, editor of the online newspaper *Ddanzi Ilbo*, along with several others, are currently involved in legal proceedings for spreading false news about Na Kyung-won, the Grand National Party's (GNP) losing candidate in the 2011 Seoul municipal elections.. In his podcast "I'm a Ggomsu" ("I'm a cheater") – one of the most popular of its kind in the world, followed by millions of people – he and other commentators criticize and ridicule GNP figures, including President Lee Myung-bak.

On the other hand, the popular blogger "Minerva," whose real name is Park Dae-sung, has filed lawsuits against the State, whom he is suing for damages related to his incarceration in 2009 for criticizing the government's economic policy (see the South Korea chapter of the 2011 "Enemies of the Internet" report).

In May 2011, Frank La Rue, the United Nations' special rapporteur for the protection of free expression, called South Korean Internet regulations a "subject of great concern."

The National Security Law in particular, which is now too outdated to deal with the extent to which South Korean has evolved since then and embraced democratic ideals, should be revised or abolished as soon as possible so that the most connected country in the world can stop engaging in outdated and ineffective censorship and allow its citizens to form their own opinions about the futility of North Korean propaganda and freely criticize their political leaders online.

SRI LANKA

COUNTRY UNDER SURVEILLANCE

2011 was marked by violence, threats and propaganda aimed at journalists and media defenders seen as government critics. Resorting to censorship and disinformation, authorities have blocked access to websites considered unfavourable to the government, claiming legal justifications.

Media registration – a tool for increased monitoring?

On 5 November, the information and media ministry ordered news sites to register with the government, yet another restriction on the free flow of information – and a step toward heavier government control of the media. Kusal Perera, director of the Centre for Social Democracy, called the order legally invalid. "There is enough room under the normal law to prevent obscene and unethical publications," he said.

Since the beginning of 2012, some 70 sites have begun the registration process; only 27 have been authorized. Those who have withheld from registering cite the risks of divulging sensitive information to the government.

Critical news prompts site blockages

One day after the registration order, the ministry blocked access to four major independent news sites critical of the government – Sri Lanka Mirror, Sri Lanka Guardian, paparacigossip9 and lankawaynews. The ministry justified this arbitrary action on the grounds that the sites had carried insults of political leaders. Government officials have been implicated in numerous corruption scandals, which the government is trying to cover up by increasing its control of media.

The supreme court has ordered access restored to SriLankaMirror. But otherwise censorship has been expanding in recent months. Several other sites, including SriLankaGuardian and TamilNet, have had access permanently blocked. Groundviews and its partner site, vikalpa, were blocked temporarily last June, along with the Transparency International site.

Lanka-e-News, scapegoat?

The Lanka-e-News site has been blocked since late October by state-owned Sri Lanka Telecom and by privately owned Internet service provider Dialog Axiata PLC without any explanation to the site's management (read the website's editor interview with Reporters Without Borders). A court order on 8 November upheld the blockage.

Lanka-e-News had been the only site to publish news on 15 October of a shootout involving members of parliament close to defence minister Gotabaya Rajapaksa, the brother of President Mahinda Rajapaksa. Pressure on Lanka-e-News has been increasing since its office was set on fire in January of last year. On 7 April, a threatening message was left on the door of the site's new office after its editor, Bennet Rupashinghe, was arrested (he was released on bail). Meanwhile, a cartoonist and political journalist for the site, Prageeth Eknaligoda, has been missing since 24 January 2010.

Devastating cyber-attacks

On 25 February, the TamilNet news site was hit by Distributed Denial-of-Service attacks. The site's personnel are trying to keep it on line. Lanka News Web and Lanka-e-News faced similar attacks last year.

International pressure urged

At the 19th session of the UN Human Rights Council in Geneva last February, Reporters Without Borders called for adoption of a resolution condemning Sri Lankan government attacks on freedom of information. The organization demanded an end to violence and threats against media organizations and human rights activists in Sri Lanka.

THAILAND

COUNTRY UNDER SURVEILLANCE

The status of Thailand's online freedom of expression began to deteriorate from the moment the new Prime Minister Yingluck Shinawatra assumed power in July 2011. Abusive recourse to the politically exploited lèse-majesté law has led to an increase in litigations and strict censorship. The sentencing of Ampon Tangnoppakul, known as "Uncle SMS" set off a chain of heated reactions in the country and abroad. Apparently the government has forgotten its promises to amend Article 112 of the Thailand Penal Code.

New government's gloomy record in terms of Internet freedom

When she took her oath of office on August 10, 2011, Prime Minister Yingluck Shinawatra vowed that "the lèse-majesté laws [should] not [be] used inappropriately." This statement was contradicted on August 26, 2011 by Vice Prime Minister Chalerm Yubamrung, who has made the fight against lèse-majesté crimes his priority.

Since taking office, Prime Minister Yingluck Shinawatra's government has shown itself to be worse than its predecessor in terms of Web filtering. After assuming his position as Thailand's Minister of Information and Communications Technology, Anudith Nakornthap ordered the blocking of 60,000 Web pages in less than three months, as opposed to 70,000 in the preceding three years. In his view, this was proof of the government's loyalty to the King. According to the *Bangkok Post*, the rising number of blocked URLs is tied to the increasingly common use of social networks and to their capacity for disseminating information. The Minister claims that, unlike when previous officials in his Ministry asked ISPs to block sites on court order, he now directly asks ISPs and administrators of websites hosted abroad to close sites or block them so that "objectionable" content can no longer be accessible to those living abroad. The Minister made his statements in the context of December 1, 2011 inauguration of the Cyber Security Operations Center (CSOC).

Based on photocopies of official documents shared by Mahidol University's Kwanravee Wangudom Institute of Human Rights and Peace Studies between January and October 2011, 122 lèse-majesté cases (which may or may not have been prosecuted) were reviewed by courts of first instance, eight reviewed by appeal courts, and three by the Supreme Court.

Deputy Prime Minister Chalerm Yubamrung has announced that Net surveillance will be strengthened in the name ofhttp://www.bangkokpost.com/breakingnews/271898/ict-to-monitor-websites-24-7 lèse-majesté laws, in order to enforce such control 24/ hours/day. The government plans to invest about USD 13 million in Net filtering to block sites guilty of lèse-majesté.

Another example of the abusive use of lèse-majesté laws and their consequences is the announcement by the authorities that if netizens visiting Facebook merely click on the buttons "like" or "share" linked to content that potentially violates lèse-majesté laws, they could be prosecuted.

Countless legal proceedings against netizens for lèse-majesté crimes

On December 8, 2011, blogger **Joe Gordon** was sentenced by a Bangkok court to two and one-half years in prison on lèse-majesté charges for translating on his blog excerpts of King Bhumibol Adulyadej's banned biography by Paul Handley, entitled "The King never smiles." This Thai-born American pleaded guilty in the hopes of a royal pardon.

Ampon Tangnoppakul, also known as "Uncle SMS," received a 20-year sentence on November 23, 2011 for sending text messages deemed to be "insulting the monarchy," but he denied having sent them. His case aroused strong reactions in the country. It was the first time that the Thai media covered this topic in-depth. Angry international criticism also arose, mainly from the United States and the Office of the High Commissioner for Human Rights claiming that the lèse-majesté law had a "chilling effect" on freedom of expression.

The trial of the *Prachatai* news website editor **Chiranuch Premchaiporn**, better know by her pen name **Jiew**, resumed in Bangkok on February 14, 2012. The five witnesses presented by the defense

were heard by the capital's court of assizes, which announced on February 16 that the verdict would be rendered on April 30, 2012. Charged with violating Article 15 of the Computer Crimes Act and paragraph 112 of the Thailand Penal Code, Chiranuch faces a possible 20-year jail sentence for not removing comments "insulting to the monarchy" posted on the *Prachatai* site quickly enough. (Read Reporters Without Borders' previous press releases about this case.)

This trial has helped to clarify the responsibility of technical intermediaries. The first witnesses for the defense helped Jiew's case, according to her lawyer. At the conclusion of the February 14 hearing, *Prachatai*'s editor shared her satisfaction with Reporters Without Borders over the fact that the court had heard the defense witnesses.

Somyos Prueksakasemsuk, former editor of the magazine *Voice of Thaksin*, banned since 2010, has been held on remand for seven months for "insulting the monarchy."

Several netizens are still incarcerated for lèse-majesté crimes. **Surapak Phuchaisaeng** is still awaiting a verdict in his prosecution for messages he posted on Facebook. **Thanthawut Thaweewarodomkul** was sentenced on March 15, 2011 to 13 years in prison for articles he published on a website linked to the "Red Shirts": Nor Por Chor USA. Student blogger **Norawase Yotpiyasathien**, who was arrested on August 5, 2011, was finally released on bail three days later. **Akechai Hongkangwarn** and **Wiphat Raksakunthai** were released on probation while awaiting their trial.

Lèse-majesté debate more bitter over "Campaign 112"

The Truth and Reconciliation Commission (TRCT), set up under the previous government advocated a lèse-majesté law reform in January 2012, deeming the existing one "too harsh." Thailand's powerful army Commander-in-Chief General Prayut Chan-ocha judged such reform unnecessary and induced the critics to leave the country.

An academic initiative to revise the lèse-majesté law caused a political uproar. Ignoring pressure, the Nitirat Group composed of seven law scholars from Thammasat began to collect signatures three weeks ago in order to submit a petition to relax the laws protecting the monarchy – which angered the army's Commander. The university had prohibited the group from using its offices to work on this project, citing the risk of violence, but then reconsidered. This ban had created considerable tension, with student groups demonstrating for and against the group's activities.

Early in 2012, 224 scholars from all over the world, including Noam Chomsky and Paul Handley, published an open letter supporting the proposal of an amendment to the lèse-majesté law (Article 112 of the Thailand Penal Code) and the Nitirat Group spearheading the reform. Article 112 was denounced as "a powerful way to silence political dissidence."

The Thai government has distanced itself from this initiative, stating that it does not want to modify Article 112. The House of Representatives could block the debate, even if the required number of signatures has been reached.

Localized censorship

Thailand was the first country to express satisfaction over Twitter's adoption of new rules making it legal to block content on a nationwide scale. The Minister of Information and Communications Technology declared that he would work with Twitter to make certain that tweets disseminated in Thailand comply with local laws. Twitter's executives be prepared to receive many requests for tweets to be removed.

Other than for monarchy-related issues, the media are relatively free in Thailand. Yet there is a persistent and growing threat of litigation for lèse-majesté crimes and related self-censorship. Any form of dissidence can now be interpreted as disloyalty to the monarchy. The country seems set on an endless course to purge the Web of any content closely or remotely linked to lèse-majesté. This repressive and doomed approach can only further divide the population and erode national cohesion.

TUNISIA

COUNTRY UNDER SURVEILLANCE

Dictator Ben Ali's fall from power had raised hopes that Ammar 404, the censorship system set up by the former regime, would be dismantled. But the latter might rise again from its ashes in the wake of a series of court orders on filtering, while the status of freedom of information remains precarious.

Fragile freedom of information worth protecting

The Arab Spring, which began in Tunisia, has brought drastic changes throughout the region. However, much remains to be done in order to protect the benefits of these revolutions, notably those involving freedoms of expression and information, specifically online. Case in point: the film "Persépolis" and the attacks on the Nessma TV station's offices, the arrest of newspaper *Attounissia*'s editor for publishing the photo of a nude woman, and police assaults on journalists covering the demonstrations.

While the progress in freedom is real, new red lines – outlined in the Tunisia chapter of the 2011 "Enemies of the Internet" report (acts of violence committed by the police and the army, corruption, government hurdles) – seem to be emerging. The Nawaat blog deplored the fact that justice is the new spearhead of censorship, and stressed that political censorship is shifting toward moral and religious censorship.

In Medenine, lawyer Mabrouk Korchide filed three complaints against a blogger and two Tunisian citizens following their posts and comments on the rally against his nomination to the position of advisor to the governor. Blogger Riadh Sahli was charged with "defamation" on the Internet just for sharing a press release sent by the demonstrators on his page Facebook Medenine informative. Mabrouk Korchide also accused Youssef Fillali, a citizen who merely commented on this post, of "defamation." The trial, which will be the post-Ben Ali era's first defamation trial, scheduled for February 22, has been continued until March 14. Furthermore, the lawyer also filed a complaint against another blogger from Medenine, Marwane Athemna, for "defamation" and "distributing leaflets" attacking his reputation.

The Riadh Sahli case shows that the law is mute on the subject of online media responsibility, and that setting up a Web-specific legal liability framework has become mandatory.

A dangerous gap in the law?

The Decree-Law No. 115 of November 2, 2011 on Freedom of the Press, Printing and Publishing will no doubt be extended to certain online content. Even though Article 1 recognizes that freedom of expression is the basis of cybercitizen protection, the Web as a whole does not fall within the law's scope of application.

As stipulated by Article 7, which uses the notion of "*creating electronic information,*" and Article 2, which refers to "*digital works*," the decree will apply to the online media. Nevertheless, no liability framework has yet been assigned to the Internet. Such liability takes on special meaning in a context of reader comments, discussion forums, etc. The "short prescription" principle must be applied in the same way to articles published online, with the starting point being the date of the posting.

Is Internet filtering coming back?

The first alarm sounded in May 2011, when the Tunis Permanent Military Tribunal ordered that five pages on Facebook be censored. The Tunisian Internet Agency (ATI) decided to play the transparency card and released the list of sites concerned.

On May 26, 2011, the Tunis Court of First Instance ordered ATI to block access to pornographic websites after a complaint was filed by lawyers on grounds that they were posing a threat to minors and the country's Muslim values – a decision that ATI pledged to oppose. In June 2011, Reporters Without Borders met with ATI President Moez Chakchouk, who reaffirmed that ATI wishes to act in a neutral and transparent manner and refuses to engage in filtering.

When its appeal was rejected in August 2011, ATI took its case to the highest appeal court. On February 22, 2012, the Court of Cassation overturned the judgement on the filtering of pornographic Web content and referred the case back to appeal. In the meantime, ATI has had to begin Internet filtering in compliance with the court's decision. It has provided information about the measures taken to comply with the order and warned the public that the reactivation of filtering would cause service quality to deteriorate, mainly due to network maintenance problems. While filtering errors can be reported by email to filtrage@ati.tn, ATI states in its notices that it will not assume responsibility for them.

However, filtering was not implemented as smoothly as expected. On February 27, 2012, Moez Chakchouk told Reporters Without Borders that "our technical services were only able to apply it for state-owned companies and public community networks. As for the five Internet service providers, all attempts resulted in serious declines in performance (Internet traffic fluidity at the transit node level)." He explained that such problems were due to "exponential growth" (+60% in 2011 vs. 2010) of the international bandwidth" – "a growth that ATI can no longer handle for lack of the financial resources (formerly provided by the Tunisian government) needed to put the filtering system back into operation."

Reporters Without Borders denounced the potential resumption of filtering as a way of resorting to the former repressive measures and listed the technical, legal, and financial risks that this would entail, including overblocking, exorbitant costs and the privatization of censorship, which would be delegated to a technical intermediary. Reporters Without Borders is concerned about a return to Ben Ali era practices and fears that filtering of one kind of content may be a prelude to the censoring of other types of content. Widespread filtering is totally inconsistent with Internet neutrality and the freedom of expression values advocated by the Higher Authority for the Realization of Revolutionary Objectives, Political Reform, and Democratic Transition.

E-governance and the growth of free software?

One positive sign: according to Global Voices, is that the political class is now using, in sending out its messages to the population, the very tools that the state previously repressed: "Twitter is also the arena in which Tunisian politicians express their frustrations about their own parties' lack of organization or the slow pace of the current government." "Political leaders in Tunisia are eager to have more transparent relations with their electorate, and that now seems to mean making use of the social media."

The ATI has just officially launched tor.mirror.tn, a mirror of the TOR website featuring its popular circumvention and anonymity software, previously used by cyberdissidents against Ammar 404. Through TOR, Moez Chakchouk told the webdo.tn website that he "wants to encourage the use of free software platforms, as well as offer a product that guarantees better navigation security against malware scripts." Installation of the TOR mirror site in Tunisia is a first in the Arab world, in Africa and even in Asia, according to Mr. Chakchouk. Many Internet users view this initiative as a way to measure the success of the Tunisian Revolution, which in the past was an arena for censorship software tests.

Future of the Tunisian Internet: Projects and debates

The restructuring of the Tunisian Internet Agency under the auspices of the Ministry of Information and Communication Technologies is one of the items that the transition government is working on. In Moez Chakchouk's opinion, "The ATI will be able to operate in accordance with international good practices as an Internet exchange point." He believes that the ATI is a candidate for membership in the European Internet Exchange Association (EuroIX) that connects ISP networks and permits the exchange of Internet traffic at the European level.

Liberalizing the Internet market is still a key objective, along with fighting against the re-emergence of filtering techniques, which should remain in the past. Including Internet access as a fundamental right in Tunisia's new Constitution would further anchor Tunisia on a steady course leading to Internet freedom.

TURKEY

COUNTRY UNDER SURVEILLANCE

Intense debate has raged around several plans to control the Internet, ranging from an outrageous list of banned keywords to a mandatory centralized filtering system that ended up being optional. Despite relentless pressure, netizens have been mobilizing against the implementation of backdoor censorship on the Web.

Continuous filtering

As of February 10, 2012, the website engelliweb.com had tallied 15,596 sites suspended by the authorities, either by court order, or by decision of Turkey's Information Technologies and Communications Authority (BTK) – a number double what it was last year (see the Turkey chapter of the 2011 "Enemies of the Internet" report). Most of these are betting, pornographic, or pedophile content websites.

However, some 15 supposedly pro-Kurd news websites were banned by court order in 2011, including Firat News (new URL: www.firatnews.ws), gundem-online.net and welat.org. Among the topics considered taboo and therefore censored are Atatürk and the minorities' (notably Kurd) issue. The filtering of the Blogger platform was lifted on March 14, 2011 after two weeks of blocking and strong mobilizations both on and offline.

Net censorship and the legal status of the debate

Controversy over the 5651 Law has abated. Its main focus has been optional filtering and a list of banned keywords.

In April 2011, the BTK forwarded to web-hosting companies and Internet service providers a list of 138 keywords to be banned from Turkish domain names as part of the fight against pornography. Already laughable because it included words like "skirt" (*etek*), "sister-in-law" (*baldiz*) and "animals" (*hayvan*), this list posed serious Internet information access problems: since it prohibited the words "free" and "pic," it may have eliminated from the Turkish Net countless references to freedoms and the latest news photos. When the media began covering this issue, the BTK stated that the list had been cited within the context of an internal communication urging state bodies responsible for suppressing online content to be on the alert. For now, it would appear that no further action has been taken regarding this list.

The new centralized filtering system "for the safe use of the Internet" launched by Turkey's Information Technologies and Communications Authority (BTK) on November 22, has also raised strong reactions both in the country and abroad. Its introduction, initially planned for August 22, 2011, was postponed three months so it could be submitted to public consultation. The initial project required Internet users to install a filtering software on their computers in order to protect them (particularly minors), from any "objectionable" content. Since then, plans have been changed and the installation is no longer required. The number of filtering options has also been reduced from four to two: "family" and "child." Pornographic sites previously blocked by court order, like other "suspect" portals, will now be automatically filtered for netizens who have adopted the system, according to an as yet unclear procedure, about which Reporters Without Borders has requested more information. As of early December 2011, only 22,000 of the country's 11.5 million Internet users had signed up for it.

On November 4, a complaint was filed with the Turkish State Council to request the elimination of the system, which, although optional, remains a threat to freedom. Tests conducted by Reporters Without Borders have shown that certain websites were abusively blocked, such as those of evolutionist Richard Dawkins (richarddawkins.net) and of Yasam Radyo ("Radio Life," which broadcasts cultural programs on minorities). The "child" option does not provide access to Youtube or Facebook, and these social networks are only accessible under the "family" option if the user requests it. The filtering solution is inappropriate and a threat to online freedom of expression as the European Union Court of Justice recently affirmed, since it increases overblocking risks. The decision as to what is, or is not, "objectionable" must be left to families, not to the State.

Status of lawsuits against Internet website contributors

Online journalist **Baris Yarkadas**, sued for a "personal insult" by Nur Birgen, Chair of the Institute for Forensic Medicine's Third Specialization Board, was discharged in September 2011. His legal troubles are not over, however, since a deputy is currently suing him for damages for having offended him during a televised debate.

Halil Savda, administrator of the website for pacifists and conscientious objectors www.savaskarsitlari.org, was sentenced to five months in jail at the end of February because of his criticism of the army.

A writer for the eksisozluk (Eksi Sözlük, or "sour dictionary") website was charged with "contempt for religious values'' for writing an article on August 10, 2011, entitled "Stupidity of religion." The lawsuit brought against Forensics Medicine expert and Chair of the Turkish Human Rights Foundation **Sebnem Korur Fincanci** and the editor of the taraf.com.tr (Camps) website, **Adnan Demir,** will resume on April 10.

Journalist Serdar Tuncer filed a complaint against a Twitter user and its 200,000 subscribers on the grounds that the owner of the satirical account @allah (cc), and his readers, mocked Islam and other religions and humiliated believers.

Online mobilization continues and international pressures show results

Demonstrations against online censorship were held on May 15, 2011 in 31 Turkish cities. Several sites that had supported the anti-censorship protests sustained cyberattacks. The magnitude of the mobilization, as well as the reactions of the OSCE and the European Union, compelled the authorities to make certain concessions (see above).

The most impressive online initiatives were the website 'Hands Off My Internet" (http://internetimedokunma.com/), which made Internet users aware of the risks associated with the filtering system and the Senin Yüzünden ("Because of You") site, which invited netizens to post photos of blindfolded people.

UNITED ARAB EMIRATES

COUNTRY UNDER SURVEILLANCE

The UAE government has taken advantage of the region's tense political climate to tighten its control over information and communications in the country. Netizen members of the "UAE 5" group, incarcerated for several months, learned the hard way that the authorities' priority is to maintain the regime's stability, and, if necessary, is fully prepared to set a few harsh examples.

Widespread surveillance

The Emirates were spared the demonstrations which rocked the political life of some of its neighboring countries in 2011. The regime did not hesitate to increase salaries in order to divert any threat of social unrest. Determined to take whatever action necessary to monitor the population's mood, it publicly took charge of the Internet surveillance system.

Colonel Abdul Rahim bin Shafi, director of the Interior Ministry's organised crime department, told Reuters in August 2011 that the police are keeping a close watch on social networks such as Twitter and Facebook: "All media are being monitored, including social media. People can express their opinion without violating (social) norms," he said. He further added: "Twitter and Facebook were invented to make the world easier but if they were used adversely, the perpetrators will be punished by law." The authorities' target is clear: "whoever spreads false or malicious news or statements or spreading propaganda which could upset public security could spend between one month to three years in jail." The senior official admitted that the large community of foreign workers who have already gone on strike to demand better working conditions is under particularly close scrutiny.

Arbitrary arrests to indimidate potential dissidents

To discourage potential dissidents from relaying calls for political reform, the regime arrested five netizens nicknamed the "UAE 5" in April 2011. They include the well-known blogger **Ahmed Mansour**, administrator of the pro-democracy discussion forum Al-Hewar ("the Dialogue"), blogger **Farhad Salem Al-Shehh**, co-administrator of this forum, **Nasser bin Ghaith**, a writer and professor at Abu Dhabi's Université Paris-Sorbonne, and human rights activists **Hassan Ali Al-Khamis** and **Ahmed Abdul Khaleq**. All of them expressed their opinions freely online and had also signed a petition bearing a hundred or so signatures which urged the authorities to enact some reforms. Ahmed Mansour was arrested after he granted an interview to the *Al Hurra TV* channel.

Bloggers and their families have been the focus of particularly violent death threats and smear campaigns orchestrated by the authorities in the media and on the Internet. Those who tried to defend them incurred, in turn, the regime's wrath. Twitter user **Rowda Hamed** was threatened and summoned for supporting their views.

These netizens' trial was such a travesty of justice that they refused to appear in court. They went on a hunger strike to protest against the bad treatment and poor conditions of their detention. On 27 November 2011, they were finally given a two-year prison sentence for "insulting Emirate leaders" and "calling for anti-government demonstrations," except for Ahmed Mansour, who received a three-year prison sentence. They were pardoned the very next day by the Head of State, Sheikh Khalifa bin Zayed Al-Nahyan, and later released. A coalition of NGOs continues to demand that their convictions be expunged from their records and that their equipment and passports be returned to them.

At the same time, the BlackBerry saga took a new turn. New restrictions were imposed in May 2011 on smartphones manufactured by Research in Motion (RIM). The authorities decided to limit access to the highly secure BlackBerry Enterprise Server (BES) to only a few companies which can account for over 20 users – a decision likely to irritate some CEOs because it discriminates against small companies. The entrepreneurs' view of the country's prospects has been tainted by the regime's intensified control over society in reaction to Arab Spring.