World day
against cyber censorship

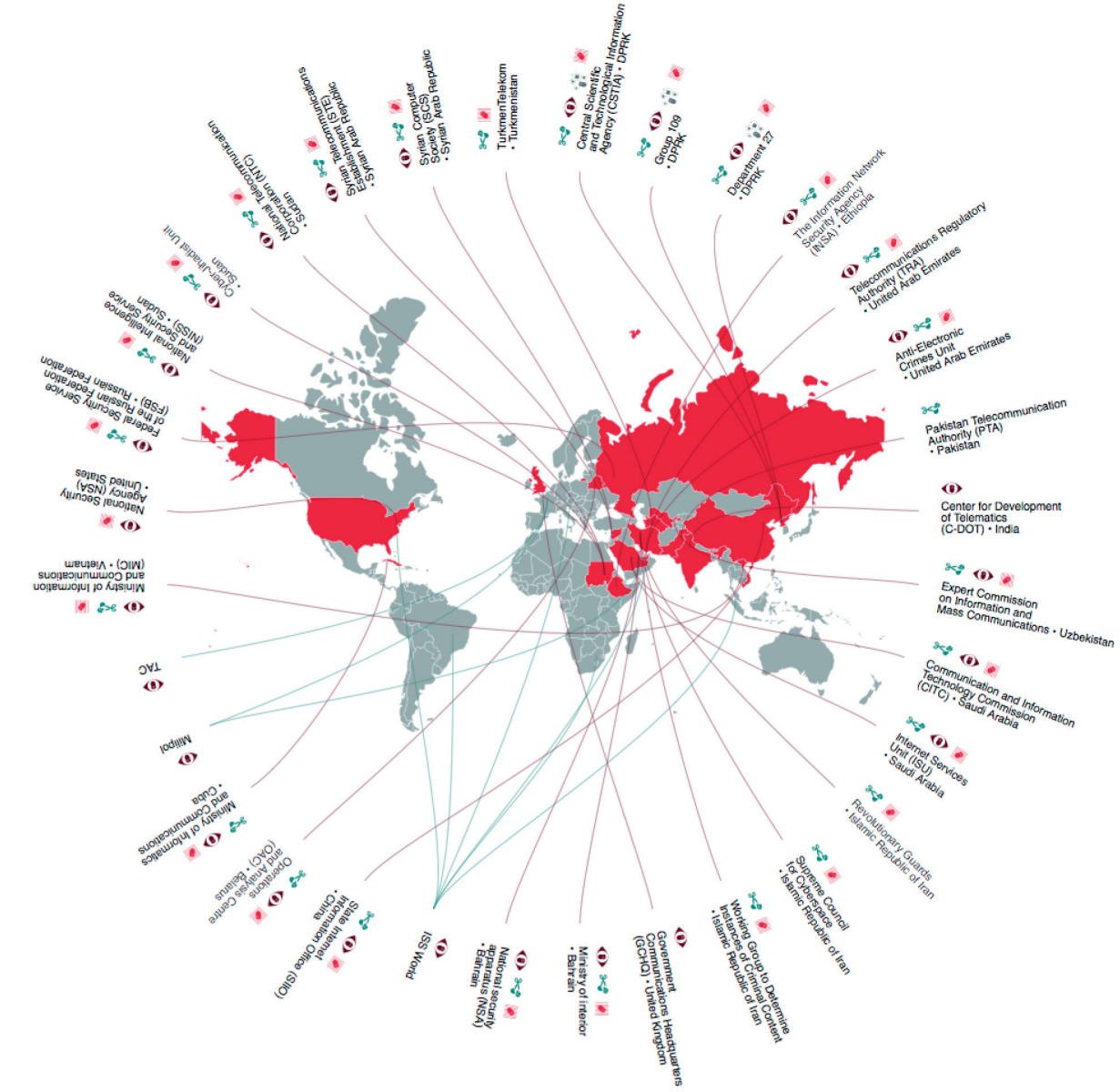
ENEMIES OF THE INTERNET

2014

REPORTERS WITHOUT BORDERS
FOR FREEDOM OF INFORMATION

INSTITUTIONS THAT ARE ENEMIES OF THE INTERNET

12 March 2014



Surveillance Censorship Imprisonment Disinformation

Get the full report at
12march.rsf.org

REPORTERS WITHOUT BORDERS
FOR FREEDOM OF INFORMATION

ENTITIES AT THE HEART OF CENSORSHIP AND SURVEILLANCE

Natalia Radzina of *Charter97*, a Belarusian news website whose criticism of the government is often censored, was attending an OSCE-organized conference in Vienna on the Internet and media freedom in February 2013 when she ran into someone she would rather not have seen: a member of the Operations and Analysis Centre, a Belarusian government unit that coordinates Internet surveillance and censorship. It is entities like this, little known but often at the heart of surveillance and censorship systems in many countries, that Reporters Without Borders is spotlighting in this year's Enemies of the Internet report, which it is releasing, as usual, on World Day Against Cyber-Censorship (12 March).

Identifying government units or agencies rather than entire governments as Enemies of the Internet allows us to draw attention to the schizophrenic attitude towards online freedoms that prevails in in some countries. Three of the government bodies designated by Reporters Without Borders as Enemies of the Internet are located in democracies that have traditionally claimed to respect fundamental freedoms: the Centre for Development of Telematics in India, the Government Communications Headquarters (GCHQ) in the United Kingdom, and the National Security Agency (NSA) in the United States.

The NSA and GCHQ have spied on the communications of millions of citizens including many journalists. They have knowingly introduced security flaws into devices and software used to transmit requests on the Internet. And they have hacked into the very heart of the Internet using programmes such as the NSA's Quantam Insert and GCHQ's Tempora. The Internet was a collective resource that the NSA and GCHQ turned into a weapon in the service of special interests, in the process flouting freedom of information, freedom of expression and the right to privacy.

The mass surveillance methods employed in these three countries, many of them exposed by NSA whistleblower Edward Snowden, are all the more intolerable because they will be used and indeed are already being used by authoritarians countries such as Iran, China, Turkmenistan, Saudi Arabia and Bahrain to justify their own violations of freedom of information. How will so-called democratic countries will able to press for the protection of journalists if they adopt the very practices they are criticizing authoritarian regimes for?

Private sector and inter-governmental cooperation

The 2014 list of Enemies of the Internet includes »surveillance dealerships« – the three arms trade fairs known as ISS World, Technology Against Crime and Milipol. These forums bring companies specializing in communications interception or online content blocking together with government officials from countries such as Iran, China and Bahrain. Here again, the contradictory behaviour of western democracies should be noted. France hosted two of these forums in 2013 – TAC and Milipol. At the same time, it issued a notice in December 2013 requiring French companies that export surveillance products outside the Europe Union to obtain permission from the General Directorate for Competition, Industry and Services (DGCIS).

The censorship and surveillance carried out by the Enemies of the Internet would not be possible without the tools developed by the private sector companies to be found at these trade fairs. Ethiopia's Information Network Security Agency has tracked down journalists in the United States thanks to spyware provided by Hacking Team, an Italian company that Reporters Without Borders designated as an Enemy of the Internet in 2013. Even the NSA has used the services of Vupen, a French company that specializes in identifying and exploiting security flaws.

Private-sector companies are not the only suppliers of surveillance technology to governments that are Enemies of the Internet. Russia has exported its SORM surveillance system to its close neighbours. In Belarus, Decree No. 60 on »measures for improving use of the national Internet network« forces Internet Service Providers to install SORM.

China has begun assisting Iran's uphill efforts to create a *Halal Internet* – a national Internet that would be disconnected from the World Wide Web and under the government's complete control. An expert in information control ever

since building its Electronic Great Wall, China is advising Iran's Revolutionary Guards, the Supreme Council for Cyberspace and the Working Group for Identifying Criminal Content. Deputy information minister Nasrolah Jahangiri announced this during a recent visit by a delegation from China's State Council Information Office.

China's pedagogic zeal has not stopped there. The *Zambian Watchdog* website reported in February 2013 that the Zambian government is working with China to install an Internet surveillance network. The blocking of the *Zambian Watchdog* and *Zambia Reports* websites in June and July 2013 showed that Zambia wants to be able control online information. China is also represented in Uzbekistan by ZTE, a Chinese company that opened an office there in 2003 and has since become the country's main supplier of modems and routers.

National security as pretext

The NSA and GCHQ, Ethiopia's Information Network Security Agency, Saudi Arabia's Internet Services Unit, Belarus' Operations and Analysis Centre, Russia's FSB and Sudan's National Intelligence and Security Service are all security agencies that have gone far beyond their core duties by censoring or spying on journalists and other information providers.

The tendency to use national security needs as grounds for riding roughshod over fundamental freedoms can also be found in agencies not named in this report. In Colombia, a digital surveillance unit that was almost certainly run by the Colombian government intercepted more than 2,600 emails between international journalists and spokesmen of the Revolutionary Armed Forces of Colombia (FARC) during recent peace talks between the FARC and Colombian government representatives.

Ignoring the objections of many human rights groups, France's parliament cavalierly adopted a Military Programming Law in December 2013 that allows the authorities to spy on phone and Internet communications in real time without asking a judge for permission. The grounds given are vague and general, ranging from the need for »intelligence affecting national security« and »safeguarding the essential elements of France's economic potential« to »preventing terrorism, criminality and organized crime«.

In Tunisia, the government gazette announced the creation of a Technical Agency for Telecommunications (ATT) on 12 November 2013 for the purpose of monitoring communications in order to assist judicial investigations into »information and communication crimes«. Its sudden creation by decree without any consultation with civil society triggered immediate concern, as it revived memories of the Tunisian Internet Agency (ATI), the symbol of online censorship under ousted President Zine el-Abine Ben Ali. The lack of any safeguards and mechanism for controlling its activities is particularly alarming.

Dangerous monopoly of infrastructure

In countries such as Turkmenistan, Syria, Vietnam and Bahrain, the government's control of Internet infrastructure facilitates control of online information. In Syria and Iran, Internet speed is often reduced drastically during demonstrations to prevent the circulation of images of the protests.

More radical measures are sometimes used. In November 2012, the Syrian authorities cut the Internet and phone networks for more than 48 hours. In China, the authorities disconnected the Internet for several hours on 22 January 2014 to stop the circulation of reports about the use of offshore tax havens by members of the Chinese elite. In Sudan, the authorities disconnected the Internet throughout the country for 24 hours on 25 September 2013 to prevent social networks being used to organize protests.

Censors enlist Internet Service Providers

Internet Service Providers, website hosting companies and other technical intermediaries find themselves being asked with increasing frequency to act as Internet cops.

Some cases border on the ridiculous. In **Somalia**, for example, the Islamist militia Al-Shabaab banned using the Internet in January 2014. As it did not have the required skills or technical ability to disconnect the Internet, it ordered ISPs to terminate their services within 15 days. Ironically, to ensure that the public knew of the ban, it was posted on websites sympathetic to Al-Shabaab.

More insidiously, gender equality and anti-prostitution laws in France have increased the burden of responsibility on technical intermediaries for blocking content after being notified of it. Article 17 of the law on gender equality requires ISPs and hosting companies to identify and report any content inciting or causing hatred that is sexist, homophobic or anti-disability in nature.

In **Venezuela**, President Nicolás Maduro has forced ISPs to filter content of a sensitive nature. The authorities ordered them to block about 50 websites covering exchange rates and soaring inflation on the grounds that they were fuelling an »economic war« against Venezuela. This did not prevent a wave of protests against shortages and the high crime rate. On 24 February, when many photos of the protests were circulating on Twitter, the authorities ordered ISPs to block all images on Twitter.

In **Turkey**, the latest amendments to Law 5651 on the Internet, voted on 5 February 2014, turn ISPs into instruments of censorship and surveillance, forcing them to join a new organization that centralizes requests for content blocking or removal. If they do not join and install the surveillance tools demanded by the authorities, they will lose their licence. Law 5651 also requires ISPs and other technical intermediaries to keep user connection data for one to two years and be ready to surrender them to the authorities on demand. The law does not specify what kinds of data must be surrendered, in what form or what use will be made of them. Experts think the required data will be the history of sites and social networks visited, searches carried out, IP addresses and possibly email subjects.

Draconian legislation

Legislation is often the main tool for gagging online information. Vietnam already has penal code articles 79 and 88 on »crimes infringing upon national security« and »propaganda against the Socialist Republic of Vietnam« but the information and communications ministry decided to go one step further with Decree 72. In effect since September 2013, this decree restricts the use of blogs and social networks to the »dissemination« or »sharing« of »personal« information, effectively banning the sharing of news-related or general interest content.

In **Gambia**, the government gave itself a new legislative weapon in July 2013 by getting the national assembly to pass amendments to the Information and Communications Act – the main law limiting freedom of information. The amendments make the »spreading of false news against the government or public officials« punishable by up to 15 years in prison or a fine of 3 million dalasis (64,000 euros).

In **Bangladesh**, four bloggers and the secretary of the human rights NGO Odhika were arrested in 2013 under the 2006 Information and Communication Technology Act, which was rendered even more draconian by amendments adopted in August. Its definition of digital crimes is extremely broad and vague, and includes »publishing fake, obscene or defaming information in electronic form«.

The Electronic Crimes Act that **Grenada** adopted in 2013 prohibits use of »an electronic system or an electronic device« to send »information that is grossly offensive or has a menacing character«. Here again, vaguely-worded legislation is posing a real threat to freedom of information.

Permission to publish

The creation of a licencing system for news websites serves as an administrative and sometimes economic barrier and is a widely-used method for controlling online information.

In **Singapore**, the authorities have created a major economic barrier for online news media. Under a measure that took effect in June 2013, news websites that post more than one article a week about Singapore and have more than 50,000 Singaporean visitors a month need a licence that requires depositing »a performance bond« of 50,000 Singaporean dollars (39,500 US dollars). The licence has to be renewed every year.

Since 2007, news websites in **Uzbekistan** have had to register with the authorities just as radio, TV and print media already did. The registration procedure is arbitrary and accreditation depends on an inspection of content. In **Saudi Arabia**, the websites of traditional media have had to obtain a licence from the information and culture ministry since 2001. The licence has to be renewed every three years.

This overview of censorship and surveillance is far from exhaustive. During the coming months, we will probably learn about more surveillance practices from Edward Snowden's files, which Glenn Greenwald and other journalists have been serializing since June 2013. The latest and perhaps most outrageous practice to come to light so far is GCHQ's »Optic Nerve« programme, used to capture the personal images of millions of Yahoo webcam users. It suggests that there are no limits to what the intelligence agencies are ready to do.

What forms of response are possible in order to preserve online freedom of information? We think it is essential to:

- press international bodies to reinforce the legislative framework regulating Internet surveillance, data protection and the export of surveillance devices and software. Read Reporters Without Borders' recommendations;
- train journalists, bloggers and other information providers in how to protect their data and communications. Reporters Without Borders has been doing this in the field for several years. It has organized workshops in many countries including France, Switzerland, Egypt, Tunisia, Turkey, Afghanistan and Tajikistan;
- continue to provide information about surveillance and censorship practices. That is the purpose of this report.

EUROPE AND CENTRAL ASIA

BELARUS: OPERATIONS AND ANALYSIS CENTRE

APPARATUS OF REPRESSION

The Internet is the last bastion of freedom of information in Belarus, where censorship and self-censorship are the rule among traditional news outlets. Since 2008, the authorities have had an armoury of technological, administrative and legal weapons at their disposal to exert their control over the Web.

Operations and Analysis Centre (OAC)

Lukashenko.by

The **Operations and Analysis Centre (OAC)** was established in 2008 and reports directly to President Alexander Lukashenko. It ensures data collected by Internet service providers complies with the law. The centre can impose sanctions if any are required. More generally, it responsible for administering the national domain .by and coordinates Internet surveillance operations. Surveillance is carried out by several government agencies including the State Control Committee, the State Telecommunications Inspection and the Public Prosecutor's Office. The ministry of information and information technology completes the repressive regulatory apparatus of used by the Belarus government.

Faced with the rapid development of information technology, the authorities in the first instance used existing legislation to penalise libel, defamation of the president and insults including those directed at the president or anyone in an official position. This legislation does not refer specifically to cyberspace, but allegations of discrediting the republic and hooliganism are among those most frequently made against netizens.

Decree 60

It was not until 2008 that legislation specifically aimed at online information made its appearance. A series of media laws were passed in 2008 and entered into force in February 2009, severely undermining Internet freedom. News sites were classified as media outlets and had to register in order to have legal status. Any that received more than 30 percent of the funding from abroad were banned from receiving this official stamp of approval, necessary to be able to publish any foreign content. The cabinet was meant to set out the criteria allowing a website to be classified as a news outlet, but no decisions have yet been made in this regard.

The real legislative turning point came in 2009 with the enactment of Decree 60, »on measures for improving use of the national Internet network«, which boosted control over the Internet. It introduced the Russian SORM surveillance system, requiring ISPs to pay for its installation and to keep the harvested data for a year.

Internet service providers must block access to any illegal site or content, such as those containing pornography or inciting violence. To do so, they must to refer to two lists of sites that are banned from being accessed from official institutions or Internet cafes. One is publicly available but empty, the other is accessible only by ISPs and the authorities themselves.

In February last year, the authorities announced that the second list contained 119 sites, including the online newspapers charter97.org and belaruspartisan.org, and the websites of the Belarus Association of Journalists and the Human Rights Centre »Viasna«.

Decree 60 brings Internet café owners into the Belarussian censorship and surveillance system, making them responsible for recording the identities of customers and keeping a record of their online activities for a year, making them available to the authorities if required. An amendment was approved in 2012 requiring Internet users to provide their passports only when accessing the Web via a wifi hotspot. However, Internet café owners are now also obliged to photograph or film their customers.

Websites providing services to the public must register using the national .by domain and be hosted on Belarussian territory. Since 2012, any breach of this regulation is liable to severe fines.

Defamation as a control mechanism

Examples abound of journalists accused of defamation as a result of what they have published online.

In July 2011, **Andrzej Poczobut**, a correspondent of the Polish newspaper Gazeta Wyborcza, was given a three-year suspended prison sentence for publishing online stories about the Belarussian president that were ruled defamatory.

More recently, **Dzianis Dashkevich**, the editor of the online newspaper vrogacheve.ru, has been subjected to numerous intimidation attempts. On 19 November last year, police searched his house, seizing two computers and a modem. The operation was launched after a local government official, Vasil Karalchuk, lodged a complaint that the site had insulted a representative of the state.

It followed the publication of an investigation into the alleged large-scale theft of gasoline by the official while he held office in the town of Zhlobin.

Those working in the media are not the only ones to be targeted – any netizen who criticizes the government falls foul of the law sooner or later.

Ruslan Mirzoev made a name for himself on the Internet in 2012 when he uploaded videos showing the daily lives of workers at the Minsk Automobile Plant where he worked. As a result of the reports, he was fired in July 2013 then imprisoned for seven days on 9 August for hooliganism. However, these abuses did not deter him from continuing with his project to post documentary footage about the grim reality of life in his home city. He was sentenced to a year in prison for violating house arrest.

Finally, the blogger **Aleh Zhalnou** of Babruysk has been the target of persecution by the authorities. Well-known for his exposures of police misconduct in his hometown, he has been picked up by the police at least 40 times in recent months. He has been the subject of legal proceedings 14 times, as well as being searched several times and having computer equipment seized. He has also been forced to undergo numerous psychiatric examinations.

Not all the legal actions have been heard, but in early February the public prosecutor opened yet another criminal case against him. He is accused of insulting a representative of the state arising from postings on his blog in which he criticized the behaviour of the local police force. In early November, he was given a fine of 200 euros. The judges upheld a complaint accusing him of disobeying the police on 4 September last year, when he and his eldest son were manhandled and detained briefly for trying to film police vehicles parked illegally on a pedestrian crossing.

RUSSIA: FEDERAL SECURITY SERVICE

REPRESSION FROM THE TOP DOWN

With great fanfare, the Russian authorities announced the creation of a new surveillance system known as SORM-3 in the run-up to the 2014 Winter Olympics in Sochi. Ever since Vladimir Putin came to power in 2000, the authorities have exploited the issue of security to boost Internet censorship and surveillance. This trend became more pronounced in the wake of mass protests in late 2011 and early 2012 against Putin's return to the Kremlin.

The Federal Security Service of the Russian Federation (FSB), the successor to the KGB, lies at the heart of the surveillance system. Work on SORM began in the mid-1980s. SORM-1 focused on intercepting telephone communications. SORM-2 allowed for the interception of data sent via the Internet. SORM-3 is able to intercept any form of communication – telephone, mobile communications and Internet – and includes long-term storage.

Direct access for the FSB

In most Western countries, intelligence agencies must obtain an order from a judge or a court and present it to the target Internet service provider (ISP) or telephone operator, which then must provide the requested information. In Russia, FSB officers must seek a court order but once they have obtained it, they need only show it to their superior officer.

When an ISP or telephone operator receives a request from the FSB, they are not given any legal documentation. Worse than that, in order to comply with FSB orders they must install the equipment necessary to implement SORM-3, codenamed *Omega*, meeting the costs themselves. Any ISP that fails to install the equipment on time is subject to heavy fines.

Once *Omega* has been installed, the FSB has direct access to the information, bypassing the technical staff of the ISP or the phone operator. It's a process that works well. According to documents obtained by the secret services watchdog website Agentura.ru, the number of intercepted emails and phone conversations has doubled in six years, to 539,864 in 2012 from 265,937 in 2007. These figures do not include wiretaps carried out abroad.

Self-censorship encouraged

When the Russian journalists Irina Borogan and Andrei Soldatov published an investigation in The Guardian on 6 October last year into the monitoring and wiretapping measures being prepared for the Sochi Games, the authorities did not bother to deny the extent of the system – quite the opposite. In reply to the investigation, the Russian government's international broadcasting service *Voice of Russia* published an article headlined *Don't be scared of phone tapping during Sochi. It's for your own safety*, saying the measures were necessary as part of the fight against terrorism.

A month later, on 8 November, Prime Minister Dmitri Medvedev signed a decree authorising the FSB to intercept and retain for three years all data relating to the telephone and Internet communications of the organizers, athletes and journalists attending the Sochi Games.

The Russian authorities and the FSB hope that the announcement of these draconian measures will drive journalists to exercise self-censorship. The data gathered at Sochi will allow the FSB to identify journalists who are critical of the government and their sources.

More broadly, the export by Moscow of its surveillance system to its ex-Soviet neighbours such as Belarus and Uzbekistan provides substantial support for their autocratic leaders.

Blacklist grows longer and longer

Russia has adopted dangerous legislation governing the flow of news and information and freedom of expression online. Since 2012 it has had a veritable legal armoury allowing any site to be placed on a blacklist and blocked without a court decision.

The Duma, Russia's parliament, passed a law in 2012 allowing the authorities to compile a blacklist of websites without a court order, ostensibly to protect children. The blacklist includes sites »containing pornography or extremist ideas, or promoting suicide or the use of drugs«.

Once a site is on the list, the hosting service must notify the owner within 24 hours. If the owner fails to remove the incriminating content, the web hosting service must close down the entire site. If the host fails to do so, it is in turn added to the blacklist and ISPs must cut off access to its platform.

Since then, the list of criteria used to block access to a site has continued to grow. In late 2013, a new law extended the grounds for blocking websites to include the publication of content regarded as extremist, such as inciting hatred or acts of terrorism, but including urging people to participate in unauthorized protests.

The creation of the blacklist and the gradual extension of the grounds for blocking sites are typical of the draconian legislation passed by the Russian parliament. There is an obvious risk of over-blocking online content when the reasons given are vague, there is a lack of clarity in decision-making and the technical procedures are unsound.

Earlier this month, the site rublacklist.net listed 35,000 sites that had been blocked by mistake because they shared an IP address with those containing »harmful« content. YouTube, Google and Russia's first social network site Vkontakte have all been blocked temporarily several times for »technical reasons«. The same thing happened to the country's most popular blog platform, LiveJournal.

News and information providers are fair game

The list of bloggers and netizens who suffer harassment continues to lengthen, especially those who write on sensitive subjects that are in the public interest.

The well-known journalist and blogger **Sergei Reznik**, 37, has criticized the local authorities and highlighted widespread corruption in the southern city of Rostov-on-Don in his blog and in articles for the newspaper *Yuzhny Federalny* and *Novaya Gazeta's* regional online supplement, *Yuzhnom Federalnom*.

Last November, a local court sentenced him to 18 months in a labour camp. At the same time, he was found guilty of insulting a magistrate in his blog, of fabricating telephone threats even though he was later brutally assaulted, and of offering 2,000 roubles to a garage mechanic to obtain a roadworthiness certificate for his car.

Suren Gazaryan, an environmental activist and popular blogger, is well known for his investigations into environmental problems and corruption linked to this year's Winter Olympics in Sochi.

In June last year, he and another activist each received a conditional prison sentence of three years in a trial without due process, after he reported that a dacha belonging to the governor of the Krasnodar region, Aleksandr Tkachev, had been built illegally in the middle of a protected nature reserve.

The two men were found guilty of causing serious damage to private property over minor damage to a metal fence that was carried out by other activists, despite offering to pay for repairs themselves.

In November 2012, more trumped-up charges were brought against Gazaryan and, fearing imminent arrest as a result of his previous conviction, he fled the country and received political asylum in Estonia.

Maxim Efimov is a blogger and human rights activist from the Karelia region on the Finnish border. He is the head of the Karelian branch of the non-governmental organisation Youth Human Rights Group and editor of the anti-fascist newspaper Chas Nol . He also has several blogs, such as http://maxim-efimov.livejournal.com. In April last year, an investigation was opened against him for inciting religious hatred after he published an article in December 2011 entitled »Karelia is tired of priests«.

On the night of 10 April, the FSB raided his home and seized his computer. On 12 May, a regional court ordered him to be committed to a psychiatric hospital. On 20 May, he fled Russia and was given political asylum in Estonia.

TURKMENISTAN: TURKMENTELECOM

A NEWS BLACK HOLE

The extent of Internet censorship in Turkmenistan confirms the regime's extremely despotic and paranoid nature. President Gurbanguly Berdimukhammedov has yet to keep his promises to develop the Internet and there still has not been any improvement in online freedoms.

Online censorship begins before you connect to the Internet in Turkmenistan because the cost of access is prohibitive for most of the population. And those who can afford it find that TurkmenTelekom, the country's main telecommunications company, blocks many independent and foreign news websites. The minority with a connection has access to only a highly censored version of the World Wide Web, dubbed »Turkmenet«.

More than 30,000 dollars for a home Internet connection

Despite a slight increase, the percentage of the population with Internet access continues to be very low (barely 7% in 2012). Local governments have no access. In ministries and government agencies in the capital, there are rarely more than three or four computers connected to the Internet. These outrageously low figures are largely the result of the exorbitant tariffs charged by access providers. In 2013, for example, TurkmenTelekom was charging 96,023 manats (33,700 US dollars) a month for an unlimited 34 Mbps connection. The new »home Internet« plan offers a 2048 Kbps connection with a 4Gb data limit for 321 manats (112 dollars) a month. And to top it all, the connection quality is deplorable.

These prohibitive tariffs are made possible by the state-owned TurkmenTelekom's near monopoly of telecommunications in Turkmenistan. After banning the Russian telephone giant MTS for more than a year and a half, the authorities gave it a new licence to offer services to Turkmen citizens in August 2012. But it has not managed to break TurkmenTelekom's monopoly or offer better services.

The position that TurkmenTelekom enjoys ensures that the authorities have complete control over the Internet. Anyone wanting to sign up for an ADSL Internet connection or a mobile Internet connection has to provide their passport details. Similarly, ID has to be shown in order to use one of the country's Internet cafés, which have become very popular.

Mass blocking and avatars

TurkmenTelekom's monopoly also allows the authorities to control and filter data coming from abroad because it is the only point of connection with the international Internet. The government is able to supervise the entire system carefully thanks to the regular reports its gets from TurkmenTelekom's CEO.

This highly centralized system simplifies blocking procedures. The government decides which websites should be censored and TurkmenTelekom then blocks access to them. The grounds for blocking a site, if they exist, are kept secret. The large number of sites blocked suggests that the criteria are very strict. They include the sites of many foreign NGOs, government opponents and human rights defenders. Most independent and foreign news sites and the main blog platforms such as *Ferghana, Khronika Turkmenistana*, the Turkmen service of *Radio Free Europe / Radio Liberty*, *EurasiaNet*, *CNN*, LiveJournal and WordPress are also inaccessible. Facebook, Twitter, WhatsApp, YouTube, Gmail, Viber and many other sites and online services are often blocked. TurkmenTelekom has created Turkmen equivalents that can usually only be accessed from inside Turkmenistan.

Any content that reflects badly on the regime or the president is systematically banned. The censorship is so extreme that it often borders on the ridiculous. When the president's horse fell at the end of a race on 28 April 2013, a vast operation was immediately launched to eliminate all visual, oral or written records. The police went so far as to check the equipment of all the journalists at the event, and the digital devices of all passengers leaving on flights from Ashgabad airport.

Death under torture

The absence of legislation specifically regulating the flow of news and information on the Internet does not limit the harassment of online journalists and netizens. The courts can use provisions of a general nature, such as those that criminalize defaming or insulting the government or president (articles 132 and 133 of the penal code) to convict those posting online. But in most cases they resort to trumped-up charges, as in the case of *RFE/RL* correspondent **Dovletmyrat Yazgulyev**, who was sentenced to five years in prison in 2011 for »inciting his sister-in-law's suicide« and was then pardoned a few weeks later.

Arrests are so arbitrary that they sometimes lack any legal basis, as in the case of another *RFE/RL* correspondent, **Rovshen Yazmuhamedov**, who was detained from 6 to 22 May 2013 with no explanation from the authorities. His arrest was probably linked to stories he had posted online about potentially sensitive social issues. Shortly before his arrest, he wrote a by-lined report about a young girl who had been banned from school for wearing a headscarf.

Prison conditions in Turkmenistan are appalling. The journalists who have been jailed in connection with their online activities include *RFE/RL* correspondent **Ogulsapar Muradova**, who died under torture at the Ovodan Depe high security prison on 10 September 2006.

UNITED KINGDOM: GOVERNMENT COMMUNICATIONS HEADQUARTERS

WORLD CHAMPION OF SURVEILLANCE

»They are worse than the U.S.« – Edward Snowden

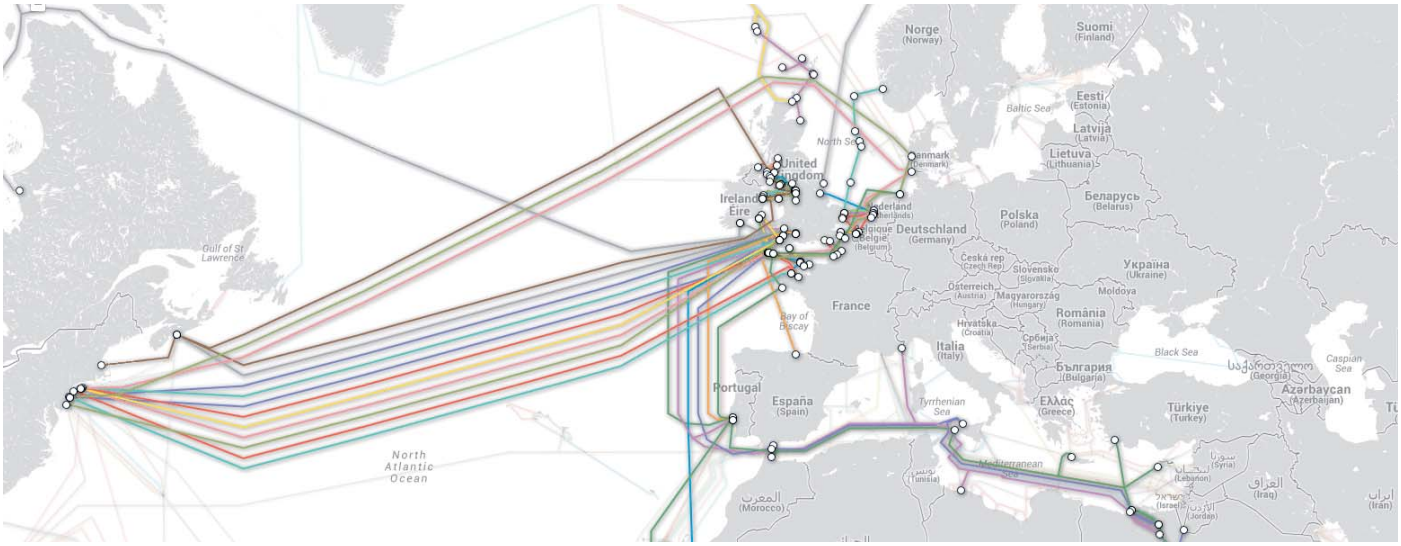
The widespread surveillance practices of the British and U.S. governments, unveiled by Edward Snowden in June last year, put Britain's Government Communications Headquarters (GCHQ) and its U.S. equivalent, the National Security Agency (NSA), at the centre of a worldwide scandal. As part of its project »Mastering the Internet«, GCHQ has developed the world's biggest data monitoring system. Supported by the NSA and with the prospect of sharing data, the British agency brushed aside all legal obstacles and embarked on mass surveillance of nearly a quarter of the world's communications.

Tempora: interception of source data

The UK lies in a geographically advantageous position to access the hardware »backbone« of the Internet. This consists of 263 submarine cables that criss-cross the world and are owned by the big names of the World Wide Web, such as Verizon, Orange and Alcatel-Lucent. Most of the world's telecommunications are carried on this network. Some of these cables – 49 to be precise – run under British beaches. Thus the United Kingdom is an unparalleled transit point for telecommunications between Europe and North America.

There are a number of landing stations for these submarine cables around the British coast. The best-known is at Bude in Cornwall, which host seven cables including Apollo North which links the UK and the United States, and more particularly TAT-14, which connects the United States and Europe. The latter showed up in one of the U.S. diplomatic cables disclosed by WikiLeaks in a list of »essential resources«. Bude is no ordinary small coastal town. It hosts a satellite monitoring station built in the 1960s, known as GCHQ Bude.

The NSA has been particularly interested in it, since the proximity of a monitoring facility and a submarine cable landing station provides a unique opportunity to monitor vast quantities of data. It even provided a budget of £15.5m for its technical redevelopment.



http://www.submarinecablemap.com/#/country/united-kingdom

According to *The Guardian*, the Tempora program was launched in 2011. The Bude monitoring station became a pilot scheme for the mass interception of data carried by the submarine cables. Seven terabytes of data per day transit via Bude, 10 percent of global Internet traffic.

The Guardian understands that 300 analysts sift through the data. However, the success of the Tempora project is mainly thanks to assistance from the telecoms companies that manage the cables. Among them are British Telecom, Global Crossing, Interoute, Level 3, Verizon, Viatel and Vodafone Cable, all of which are known to have links with the British intelligence service.

Some of these companies have made their infrastructure available to GCHQ, allowing it to place hundreds of wiretaps in submarine cable landing stations.

GCHQ thus gathers an unprecedented quantity of information including data on British and foreign citizens whose exchanges have transited, for example, via servers based in the United States.

Millions of emails, telephone calls, browsing histories and all types of digital content have thus been intercepted by GCHQ and shared with the NSA. Documents disclosed by Snowden explain that the British agency keeps the content, including the contents of emails and telephone conversations, for three days and the metadata, such as login times, telephone numbers, originators and addressees and email subjects, are kept for 30 days, a boon for both GCHQ and the NSA.

EdgeHill: decryption on a vast scale

There are several methods of encrypting Internet traffic. The simplest is to use the protocol https, which works by using digital certificates supplied by companies known as *certification authorities*. The certificates guarantee the confidentiality of online exchanges. Documents published by Edward Snowden showed that GCHQ has a program, known as EdgeHill, designed to break the encryption provided by the three main certification authorities.

The use of a Virtual Private Network (VPN) is another method of encrypting Internet data. EdgeHill's other objective is to target the encryption keys of some 30 VPN providers.

As part of the same program, GCHQ targeted the encryption installed to protect information hosted by Hotmail, Google, Yahoo and Facebook in 2012.It expects to crack the encryption of 15 certification authorities and 300 VPN providers by 2015.

According to the security expert Bruce Schneier, confidence in the Internet is based on cryptography. Uncertainty about the confidentiality of Internet communications can lead to self-censorship, and ultimately lead to an end to the use of the network for communications. By targeting the means of ensuring the confidentiality of online information exchanges, GCHQ has undermined the very basis of users' confidence in the Internet.

Confusing journalism and terrorism

Snowden's disclosures exposed the activities of the U.S. and the UK. The possession by The Guardian of files provided by Snowden, some of which proved that GCHQ carried out widespread surveillance of ordinary citizens, incurred the wrath of Prime Minister David Cameron's government. The paper's editor Alan Rusbridger spoke of the pressure from Whitehall to suppress the scandal of the GCHQ wiretaps. Rusbridger was contacted by Sir Jeremy Heywood, the cabinet secretary, who gave him an ultimatum: hand over the files or face legal action.

Faced with these threats, issued in June last year just after the first stories in the »NSA files« series appeared, Rusbridger agreed to destroy the data, having previously sent copies to two publications based in the United States under the protection of the First Amendment to the U.S. constitution. A surreal scene unworthy of British democracy then took place in the basement of The Guardian's offices, where GCHQ officials supervised the destruction of computer hard disks containing the files.

The British government did not stop there. On 18 August last year, David Miranda, the partner of former Guardian blogger Glenn Greenwald, was detained at Heathrow Airport on his way home to Rio de Janeiro from a business trip to Berlin. He was held for nine hours under the UK's Terrorism Act and all his equipment was seized.

The wrongful arrest of Miranda, although clearly linked to his and Greenwald's activities and unrelated to any alleged terrorist activities, was not ruled unlawful when he challenged it in the High Court. However, Frank La Rue, the UN special rapporteur on freedom of expression, expressed concern about the abuse of anti-terrorism powers in the UK: »The protection of national security secrets must never be used as an excuse to intimidate the press into silence and backing off from its crucial work in the clarification of human rights violations.«

Earlier this month, leaked documents published by Greenwald showed how GCHQ and the NSA persecuted WikiLeaks and the »human network« that supports it.

A presentation used by GCHQ to explain the capabilities of its unit the Joint Intelligence Threat Research Group shows screenshots of a program codenamed »Anticrisis Girl«, allowing the analysis of data gathered as part of Tempora.

WikiLeaks features prominently among the »targets« exposed by these screenshots. Those who use and visit WikiLeaks, whose only »wrongdoing« was gathering and publishing information in the public interest, have thus been victims of active surveillance. Similarly, users of the file-sharing website Pirate Bay have also been monitored.

The law be damned

The interception of telecommunications is enshrined in British law through the Regulation of Investigatory Powers Act 2000. This specifies that authorised surveillance must be proportionate to what is sought to be achieved by carrying it out, and that authorisation for legal telecommunications interceptions must be granted with the assurance that they are:

- in the interests of national security
- for the purpose of preventing or detecting serious crime
- in the interests of the economic well-being of the United Kingdom

The large-scale wiretapping carried out by GCHQ under the Tempora program clearly contravenes these principles since they are carried on a large scale and systematically, and are thus disproportionate. In order to comply with the law, GCHQ uses a loophole in the 2000 RIP Act which exempts the monitoring of foreign telecommunications.

Privacy International lodged a complaint against the British government in July last year, alleging data collection under the Tempora program was disproportionate. In January, a report by the European Parliament said GCHQ's surveillance activities appeared to be illegal. A member of the British Parliament, David Heath, has called for new legislation to ensure Britain's intelligence agencies can never intercept phone calls or email data without a specific warrant.

In a report on Internet surveillance published in June last year, the UN's Frank La Rue said the legal framework for surveillance must adhere to the principles of necessity and proportionality. Extreme surveillance measures should be used only as a last resort and when all other means have been exhausted.

UZBEKISTAN: EXPERT COMMISSION ON INFORMATION AND MASS COMMUNICATION

WELCOME TO DIGITAL TYRANNY

Since the bloody repression of protests in Andijan in 2005, the autocratic regime of Islam Karimov has done everything in its power to extend to the internet the absolute power that it wields over traditional media. The government has systematically established institutional structures, legislative tools and advanced technology to guard against any threat from online content. The Expert Commission currently heads this system of control and censorship.

Blocking experts

Created by the government in August 2011, the **Expert Commission on Information and Mass Communication** is the top agency in charge of web regulation. The commission is tightly controlled by the council of ministers, to which the commission must file quarterly reports. Internal workings of the commission are opaque. This non-transparency extends to procedures for recruiting members.

The commission's principal task is evaluation of online publications to determine their possible »destructive and negative informational-psychological influence on the public consciousness of citizens«; whether they are intended to »destabilize the public and political situation«; and whether they violate Uzbek law. The commission must also decide if content meets a requirement to »maintain and ensure continuity of national and cultural traditions and heritage«. In carrying out these tasks, commission experts can open their own investigations or assign other agencies that specialize in control of online content.

Among the agencies available for consultation is the State Committee for Communication, Informatization and Telecommunication Technologies, which succeeded the Uzbek Agency for Communications and Information. The new committee also is under the complete control of the executive branch and is required to report regularly to the Council of Ministers. The council chooses the members of the Collegium, an internal agency in charge of planning and carrying out the committee's activities, as well as the appointment of its officials.

However, the committee's director and deputy director are appointed by the chief of state himself. These two officials are in charge of the Collegium and are also members of the executive board of Uztelekom, the country's main internet service provider, 51 per cent owned by the government.

Within the Committee, the Centre for the Monitoring of the Mass Communications Sphere specializes in analysis of online content, while the Computerization and Information Technologies Development Centre is responsible for the .uz internet country code and associated domains. Regulations on registration, usage and assignment are extremely strict.

In this context, the role of internet service providers is extremely sensitive. As the last link in the chain, they are subject to tight control by the Committee, and required to block all prohibited content. The 1999 telecommunications law authorizes license suspension or prohibition to those unable to prevent the dissemination of illegal content. Pressure on these technological middlemen frequently pushes them to exercise preventive censorship.

Service providers as whole are required to prevent access to prohibited sites or content, but site-blocking is carried out mainly at the network level at Uztelekom, which has the monopoly on internet access nationwide. A 2011 amendment to the telecommunications law effectively requires private service providers to go through Uztelekom for internet access. This monopoly, which has been strengthened considerably in recent years, greatly facilitates internet control.

Social media made in Tashkent

A 2007 amendment to the 1997 media law places news sites in the same category as other kinds of media. Under the amendment, these sites answer to the same standards applied to all media. Despite the absence of a clear definition of news site, the amendment requires those seeking registration for such a site (indispensable for legal existence), to go through a registration procedure similar to that required of other media. The procedure is arbitrary, and involves a content examination as a condition of accreditation.

Blogs and news sites are also subject to more general standards such as those laid out in Articles 239, 140 and 158 of the criminal code. These authorize severe penal-

ties for defamation and insults, especially those directed at the president. This is the law which in the past led, for many bloggers, to prison sentences or fines of 100 to 500 times Uzbekistan's minimum wage. The laws also authorize sentences of two to three years at hard labor, as well as prison sentences of up to six years.

Decree 216, adopted in 2004, specifies that internet service providers and operators are prohibited from disseminating content that calls for violent overthrow of constitutional order, for war and violence, that includes pornography, or that damages human dignity. Interpretations under the law are highly subjective.

Presently, the majority of independent sites that provide news, reflect political opposition and defend human rights are censored. Other sites are hit by temporary blocking, especially at times of major social and political events.

The Facebook, Odnoklassniki, Twitter and LiveJournal social networks, as well as the YouTube video platform, are also targeted by cyber-attacks that affect an entire site or certain pages. To restrain social media's growing popularity, Uzbek authorities have tried to promote domestic alternatives, including Id.uz (social network), Fikr.uz (blog platform), Utube.Uz (a sort of Uzbek YouTube). Most of these are designed for use only by Uzbekistan residents.

Leading-edge censorship

Uzbek agencies have steadily expanded their store of up-to-date surveillance and censorship technology, thanks not only to aid from partner countries, but to western and Chinese businesses. Uztelekom uses equipment from ZTE, a Chinese firm. In 2003, ZTE opened an office in Uzbekistan, where it has become the country's main supplier of modems, routers and mobile telephones. Notably, Uzbekistan in 2006 also acquired the SORM Russian large-scale surveillance system. The government requires all internet service providers and all telephone companies to install the system and to use it, at their own expense.

Article 27 of the constitution protects the privacy of communications and conversations, but no law guarantees protection of personal data. Consequently, intercepts can be used against anyone, and be accepted as evidence in court.

Access to VPNs is hampered ever more frequently. During the second half of 2012, nearly all proxies were blocked, and Psiphon 3 was made unusable. The TOR network remains accessible, but the *torproject.com* site, where web users can download the software, is blocked.

Precision-aimed operations

Targets of government censorship include independent and opposition news sites, as well as foreign sites, such as Fergananews.com, Uznews.net, UzMetronom.com, Centrasia.ru, EurasiaNet.org, NewEurasia.net, Harakat.net, Mediauz.ucoz.ru, Registan.net, and Deutsche Welle. Uzbek-language services of Radio Free Europe/ Radio Liberty, and of Voice of America and the BBC are also censored. They do not even appear in the www.uz.domestic search engine

The Uzbek government has shown its readiness at any time to launch targeted or massive campaigns to lock out online content. On 9 August 2011, on the eve of the opening of the »Internet Festival« of the UZ domain, marking the 20th anniversary of national independence, more than 20 major sites, notably foreign news portals such as the *New York Times, Reuters, Bloomberg,* and *Lenta.ru* were blocked. Also included in the blackout were the Google search engine, the Reporters Without Borders site, and addresses such as sovsport.ru (dedicated to sports news).

When authorities are unable to invoke criminal laws against defaming or insulting the president, they do not hesitate to fabricate cases designed to trap independent news providers. Salijon Abdurakhmanov, an independent journalist in the Karakalpakstan, region was sentenced to 10 years in prison in 2008 on a charge of drug trafficking. The sentence in fact was aimed at retaliating for his online reporting of the grave consequences of the Aral Sea ecological disaster. Prison conditions have caused severe effects on the health of the 63-year-old journalist, who suffers from a stomach ulcer.

More recently, a contributor to *Radio Ozodlik*, the Uzbek-language service of *Radio Free Europe/Radio Liberty*, has spent more than six months in prison in ghastly conditions, though he is 75 years old and in declining health. Known for his reporting on corruption and on injustice in his regional government, he has been targeted by a criminal case clearly manufactured to silence him. Arrested on 22 May 2013 and sentenced in August to five years in prison on charges of fraud and extortion, he was finally freed at year's end.

AMERICAS

CUBA: MINISTRY OF INFORMATICS AND COMMUNICATIONS

NO REVOLUTION ONLINE

The arrival of fibre optics in the island via the ALBA-1 submarine cable from Venezuela and the unblocking of some websites have offered a glimmer of hope, but Cuba still denies most of its population free access to the Internet. The Castro government has developed its own control model based on a local Intranet, sky-high Internet access costs and an all-pervading government presence.

Anti-revolutionary content vetoed

The country's censorship agency is the Revolutionary Orientation Department (DOR), which filters all news and information published by the official media, based on criteria set by the party. In other words, all content deemed »anti-revolutionary« is automatically blocked. These censorship regulations are not confined to the Internet. They are based on provisions in the criminal code that criminalize insults, slander, libel, abusive language and affronts to the authorities, institutions of the republic and heroes and martyrs of the nation, among others.

The ministry of informatics and communications was formed in 2000 to ensure the revolutionary ideology preached by the DOR is implemented on the Internet. Little information is available on the censorship technology used by Cuban authorities. The University of Information Science and the country's telecoms operator ETECSA, which is also the sole Internet access provider, both have censorship and monitoring departments that support the actions of the ministry. The blocking of Internet content is carried out by ETECSA.

Drip-feed of change

In 2011, the government made some concessions, such as unblocking certain websites like the Desde Cuba and Voces Cubana portals which hosted blogs by government critics such as the *Generación Y* blog run by **Yoani Sanchez**. However, this small step was cancelled out by the arrest of a dozen bloggers and netizens in late 2012, including Calixto Ramon Martínez who was released after spending seven months in prison. Arrests were less frequent in 2013, but it must be noted that change in Cuba takes place inch by inch and the situation remains at a standstill.

In 2008, the Internet penetration rate was just 1.2 percent. Since then the number of access points appear to have been increasing. In June 2013, 118 new »navigation halls« have been opened, according to the authorities. However, connection costs remain prohibitive, equivalent to one-third of the average monthly salary of about $21 U.S for access to the government-controlled Intranet.

The authorities maintain that in 2013 four Cubans in 10 regularly logged on to the Intranet, allowing access to email and some official websites. However, the independent news agency *Hablemos Press* estimates this figure at only two in 10. The Internet proper is available in international hotels but remains available mainly to tourists who can afford to pay up to $10 U.S., two weeks' salary for the average Cuban.

Internet connections are almost always monitored. Cubans must provide proof of identity to access the national network and browse under the watchful eye of CCTV cameras and surveillance officers stationed in Internet cafes.

The computers are equipped with software such as Avila Link, developed in Cuba, which are designed to shut down at the slightest hint of dissident behaviour. Independent Cuban news sites hosted abroad, such as Payo Libre, Hablemos Press, Cubanet, Cuba Encuentro and Martí Noticias are on the blacklist and cannot be accessed, even from international hotels.

Cuban authorities have long blamed the problems with Internet access on the U.S. embargo, but the activation of the ALBA-1 fibre optic cable makes this argument obsolete and highlights the authorities' desire to control the network and their fear of making the Internet freely available. High-speed Internet access via ALBA-1 is used only for some government functions.

If official statements are to be believed, 2014 will be a good year for accessing the Internet in Cuba. ETECSA plans to start installing ADSL lines by the end of the year in locations that already meet the technical requirements. However, the necessary infrastructure and funding are sorely lacking.

The telephone network is under-developed and entirely controlled by the national telecoms provider ETECSA. In these circumstances, it is difficult to see that the arrival of ADSL will have much effect. A plan was announced in January this year for Internet access via the cell phone network, made easier by a new system for paying for online packages from abroad. Not just a new opportunity for Cubans, it is also an economic strategy to bring foreign exchange into the country.

Nonetheless, some analysts see a trend towards greater openness and the news site Cubanet, based in the United States, has forecast seven technological developments over the next year, including the ability to access the Web via cell phones and the development of wifi on the island, and the opportunity for activists to learn about online security thanks to travel reforms that took effect in January last year.

Bloggers attacked as »mercenaries«

In the 2012 edition of its »Internet Enemies« report, Reporters Without Borders highlighted Cuban propaganda which continually attacks bloggers that criticize the government, accusing them of being mercenaries working for the »U.S. empire«. They have been the targets of a campaign of smears and defamation in the state news media and on external propaganda websites and blogs, such as *Blogueros y Corresponsales de la Revolución* and *Las Razones de Cuba*.

A U.S. government cable published by WikiLeaks in 2009 suggested the government feared bloggers more than other activists, these days more than ever. During blogger Yoani Sánchez international tour, she announced that upon her return to Cuba she planned to create a platform for free news and information in Cuba. »The worst that could happen is that they close us down on the first day, or block our access to the Internet«, she said. »But perhaps we shall also sow the first seeds of a free press.«

In response to the problems of Internet access, information is passed from person to person using a USB memory stick, and some people have tried to set up illegal access points. But agents patrol the streets to track down and destroy satellite antennas, and the risks for individuals are serious. Antennas are placed every 5 square kilometres by the government, in order to jam eventual illegal signals. Netizens are sometimes able to send Tweets blindly, using SMS messaging, with no guarantee that they will appear on Twitter. The micro blogging site is regularly blocked by ETECSA, sometimes for months at a time.

Bloggers and contributors to opposition websites such as *Hablemos Press* and *Payo Libre* are forced to send content via various diplomatic missions to post on sites hosted abroad. Others, such as the Miami-based site *Martí Noticias*, have correspondents on the ground.

Those involved in news and information inside Cuba are regularly the targets of raids on their premises and arbitrary arrests. They include **Mario Echevarría Driggs, David Águila Montero, William Cacer Díaz, Denis Noa Martinez** and **Pablo Morales Marchán**, who were detained for several days in October 2013.

Angél Santiesteban-Pratz, a writer and author of the blog *Los hijos que nadie quiso*, was sentenced to five years' imprisonment in February last year. Last month, at the end of his first year in prison, his lawyer was suspended for six months. Santiesteban's blog still keeps Cubans informed about his fate, thanks to activists outside the country.

USA: NATIONAL SECURITY AGENCY

DATA THEFT ON A GLOBAL SCALE

In June 2013, computer specialist Edward Snowden disclosed the extent of the surveillance practices of the U.S. and British intelligence services. Snowden, who worked for a government sub-contractor and had access to confidential documents, later exposed more targeted surveillance, focusing on the telecommunications of world leaders and diplomats of allied countries. Activists, governments and international bodies have taken issue with the Obama administration, as the newspapers The Guardian and The Washington Post have revealed the extent of the surveillance. The main player in this vast surveillance operation is the highly secretive National Security Agency (NSA) which, in the light of Snowden's revelations, has come to symbolize the abuses by the world's intelligence agencies. Against this background, those involved in reporting on security issues have found their sources under increasing pressure.

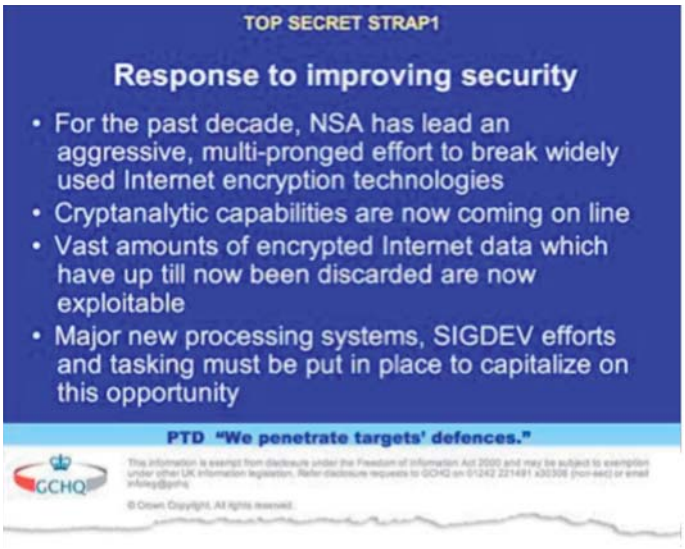
The U.S. edition of The Guardian is still able to publish information from Edward Snowden, while the British edition is not, but the country of the First Amendment has undermined confidence in the Internet and its own standards of security. U.S. surveillance practices and decryption activities are a direct threat to investigative journalists, especially those who work with sensitive sources for whom confidentiality is paramount and who are already under pressure.

The agency that doesn't exist

Based in Fort Meade, Virginia, the NSA has always operated behind a wall of secrecy. According to legend, its acronym was jokingly said to mean »No Such Agency« because its work took place far from the eyes of U.S. citizens. The glimpses we have had into its activities have come from whistleblowers such as Snowden, Thomas Drake and Bill Binney.

The U.S. agency has an official annual budget of $10.8 billion and is reported to employ some 100,000 people, mostly in signals intelligences (SIGINT). It has at its disposal vast resources for intercepting communications, 14 times the size those of the French DGSE external intelligence agency.

Snowden's disclosures showed that the NSA's eavesdropping on communications went far beyond observers' suspicions. However, U.S. intelligence services do not just carry out large-scale monitoring of private exchanges. They also conduct a decryption program codenamed Project Bullrun, another blow aimed at the heart of confidentiality, including that of journalists.



Classified exchanges between the NSA and Britain's GCHQ congratulating themselves on their success in cracking the security of the network and individual privacy. Image: The Guardian

As part of Project Bullrun, the NSA paid security software firms to install encryption systems that weakened the security of their products. The agency also used its influence with U.S. institutions to get them to lower security standards from agreed norms that were about to be adopted.

Other Snowden documents revealed that the U.S. firm RSA, a supplier of encryption software to governments and private firms, received $10 million from the NSA to reduce the security level of its BSAFE tool, which is used to enhance security in personal computers and other products, allowing the agency to monitor its customers. RSA denied there had been any such deal.

The legal framework

The legal basis for most of the surveillance practices disclosed by *The Guardian* and *The Washington Post* since June last year lies in the Foreign Intelligence Surveillance Act of 1978, amended by the 2001 USA Patriot Act, passed after the September 11 attacks, and by the FISA Amendments Act of 2008.

This legal framework defines the status of the federal Foreign Intelligence Surveillance Court, known as the FISA court, the arbiter for NSA surveillance requests in the secret judgments it renders. The criteria used by the court are broad, since monitoring a server through which communications pass is agreed if the court believes there is a reasonable assumption the communications include those from foreigners outside the United States.

Against this background, the surveillance of electronic exchanges among millions of users of Microsoft, Yahoo! Google, Facebook, PalTalk, AOL, Skype YouTube and Apple as part of the PRISM program was made possible.

The United States is part of the Five Eyes alliance, which also includes the British, Canadian, New Zealand and Australian secret services and whose purpose is to share expertise and resources in the interception of telecommunications. Documents disclosed by Snowden showed the NSA also worked with other, third party intelligence services. Among these informal partners are Germany's Bundesnachrichtendienst, believed to intercept up to 20 percent of the Internet traffic that passes through Germany, the Swedish agency FRA, regarded as a leading partner by the NSA because of its privileged access to submarine cables in the Baltic, and France's DGSE, which is believed to have established a protocol for exchanging data with the United States under the Lustre program.

The NSA's toolbox

The NSA works closely with Internet access and service providers that manage the »backbone« of the Internet, the network's hardware. Among these big names are AT&T, Level 3 and Verizon. These links allow the NSA to monitor the Internet at the infrastructure level. Most monitoring devices are based in the United States, the stronghold of the Web industry. Outside the border of the United States, the NSA has access to the submarine cables that carry 99 percent of the world's telecommunications, especially through its partnerships with GCHQ and the FRA.

Deep Packet Inspection technology, which allows packets of data to be intercepted as they pass through the network, is believed to have been installed in a number of data centers and concealed in the installations of ISPs. The U.S. telecoms giant AT&T has given the NSA access to its customers' metadata. The Electronic Frontier Foundation brought a class action case against AT&T on behalf of its customers, alleging violation of privacy laws.

A dedicated NSA unit, known as Tailored Access Operations (TAO), is aimed at intercepting the communications of specific targets. The agency has a catalogue of tools at its disposal that enable it to overcome the security measures traditionally used to make communications and data secure. The 50-page catalogue, disclosed by the German news magazine Der Spiegel, shows the scope of the NSA's expertise.

The most worrying of these tools is probably Quantum Insert, which enables the installation of spy software on specific machines. The idea is a simple one and involves redirecting the user to a fake Web page which installs spyware on the target computer. Britain's GCHQ has also used Quantum Insert, for example to spy on engineers of the Belgian telecoms company, Belgacom.

Pressure on journalists, sources and whistleblowers

The Obama administration has shown itself to be willing to interpret the protection of national security in a broad and abusive manner, at the expense of freedom of information. A witch-hunt was launched against journalists' sources who disclosed confidential information about the powers of the state.

James Risen, a Pulitzer Prize-winning American journalist, covered the trial of former CIA agent Jeffrey Alexander Sterling, a whistleblower who was prosecuted under the Espionage Act. In 2011, Risen was served with a subpoena from the Department of Justice ordering him to testify at the trial and ordering him to reveal his sources. The *New York Times* reporter fought the order, arguing that his right to protect his sources was guaranteed by law. In 2013, an appeals court in Richmond, Virginia, ruled that Risen could be made to testify at the trial. The journalist has made it clear he is determined to continue his fight to protect his sources.

On 12 September 2012, the journalist Barrett Brown was arrested by the FBI and held in a federal prison. The charges against him could have originally added up to 105 years in prison if he was convicted. The journalist was investigating the contents of over five million internal emails released through a hack on the private intelligence company, Stratfor. Brown was charged with 12 offences after he posted a link to the site that had published the emails.

The U.S. government already had the journalist in its sights for his part in exposing »Team Themis«, a shadowy project aimed at ruining the hackers' collective Anonymous financially and to silence journalists that were sympathetic to it. On 5 March this year, 11 of the 12 charges against him were dropped and the maximum prison term he faced was reduced to 70 years.

Whistleblowers are also in the firing line. Snowden has been prosecuted for »unauthorized communication of national defense information« and »wilful communication of classified communications intelligence information to an unauthorized person«. His case is the seventh brought under the 1917 Espionage Act by the Obama administration.

Before Obama's first term, the Espionage Act, intended to be used against those who aid an enemy, had been used only three times. The U.S. authorities have also revoked Snowden's passport with the aim of preventing him from travelling. Afraid to return to the United States, where officials have had harsh words for him and where a fair trial seems unlikely, Snowden is stuck in Russia, which gave him temporary asylum until summer this year. Several European countries have refused him asylum.

Chelsea Manning was sentenced to 35 years' imprisonment last year for leaking secret military and State Department documents to WikiLeaks. Among them was the »Collateral Murder« video, showing U.S. troops in Iraq firing on civilians, killing a Reuters photojournalist and seven other people. The case against Manning was also based on the 1917 Espionage Act, even though this archaic law is in no way applicable to modern whistleblowers.

Manning was also convicted under the Computer Fraud and Abuse Act for using an unauthorized program, Wget, to download files that he passed on to WikiLeaks.

Jacob Appelbaum, a developer of the Tor privacy tool, is a journalist with *Der Spiegel.* He is a committed privacy advocate and has worked with WikiLeaks several times. After being harassed by the U.S. authorities, Appelbaum, an American, decided not to return to the United States in the wake of Snowden's disclosures. He now lives in temporary exile in Berlin, where he says he has also been the target of surveillance by the intelligence services.

The NSA has been helped in its determined pursuit of WikiLeaks by GCHQ, since all visitors to the website have been monitored by the British agency's TEMPORA surveillance system. Their IP addresses and the terms entered in search engines to access the site are intercepted and recorded.

MIDDLE EAST AND NORTH AFRICA

BAHRAIN: MINISTRY OF INTERIOR, NATIONAL SECURITY APPARATUS

NO INTERNET SPRING

Three years after the start of a popular uprising, the Bahrain monarchy continues to use all the resources at its disposal to gag those calling for democratic reforms and respect for human rights. As the Internet is now the space preferred by Bahrainis for expressing their demands and sharing information, the authorities are constantly trying to improve their Internet surveillance and censorship methods in order to contain the dissent and protect Bahrain's international image. The two government bodies at the heart of the online crackdown are the Ministry of Interior and National Security Apparatus (NSA).

The interior ministry's armed wings

The Ministry of Interior (MoI) is the central Internet control body in Bahrain. It is assisted by two units that are under its authority – the Central Informatics and Communication Organization (CICO) and the General Directorate for Combatting Corruption and for Electronic and Economic Security.

Originally created to build a database of citizens' personal details, the CICO has evolved over the years, receiving powers by royal decree that are much more extensive and include blocking websites on a list compiled by the ministry. Its premises house the Internet surveillance and censorship equipment, including the BlueCoat servers that enable ISPs to implement the ministry's blocking decisions.

According to the NGO Bahrain Watch, the CICO also uses technology provided by Gamma International, including its FinFisher software suite. FinFisher can install spyware on the computers and smartphones of targeted dissidents, controlling their webcams, logging keystrokes and recording phone and Skype calls. The servers that recover and store this information are also located inside the CICO's premises.

The Directorate for Combatting Corruption and for Electronic and Economic Security was created in 2012 with the task of combatting the »crime of defamation«, especially on online social networks. It calls on the public to report »online smear campaigns tarnishing the reputation of naional symbols and leading public figures«.

Bahraini-style NSA

While the Ministry of Interior operates openly, the same cannot be said of the National Security Apparatus (NSA). The general public knows little about this entity although, ever since its creation by royal decree in 2002, it has played a growing role in monitoring and cracking down on government opponents and human rights activists. It answers directly to the prime minister and its director is named by royal decree.

The NSA's official mission is identifying and monitoring any activity that could endanger the kingdom and its institutions, and any threat to the country's security. The NSA's distinguishing characteristic is its autonomy. It does not depend on any ministry, not even the interior ministry, but uses the latter's resources to accomplish its mission and to track down dissidents. It has authority over the CICO and the information ministry.

In addition to its surveillance capacities, the NSA has the power to arrest and imprison Bahraini citizens. To do this, it can use the Special Security Forces, a paramilitary force of 20,000 men, of whom 90 per cent are mercenaries.

Draconian decree-laws

The legislation governing the media consists of the Press and Publications Law (decree-law No. 47) and the Telecommunications Law (decree-law No. 48), both dating from 2002. These two laws permit Internet control and censorship. Posting content that criticizes Islam or the king or that incites violence or the overthrow of the government is punishable by up to five years in prison.

Information providers hounded

Since the start of the pro-democracy demonstrations in February 2011, many websites have been blocked for posting articles critical of the regime. They include the sites of the *Al-Quds Al-Arabi* daily and the *Bahrainmirror*. YouTube and Facebook pages containing videos of demonstrations or of the Bahraini police using violence against demonstrators have also been blocked, as have censorship circumvention software such as »Hotspot Shield« and even »Google Translate«.

The netizen **Zakariya Rashid Hassan** died in detention on 9 April 2011, a week after being arrested by the NSA on charges of inciting hatred, disseminating false news, promoting sectarianism and calling for the overthrow of the government on online forums. He ran an online forum that provided information about the village where he was born, Al-Dair. The site has been closed since his arrest.

Freelance photographer **Hussain Hubail** was arrested on 31 July 2013 and was charged three weeks later with »managing (electronic) accounts calling for the government's overthrow«, »promoting and inciting hatred against the government«, »inciting others to disobey the law«, and calling for illegal demonstrations. He is still being held and has reportedly been mistreated and tortured in detention. On 16 February 2014, a judge postponed hearing his case for a month.

Jassim Al-Nuaimi, a blogger who was very active during the uprising, was arrested at his home by masked plainclothesmen on 31 July 2013 on charges of using social media to incite anti-government hatred and call for illegal demonstrations. After being held for several days at the General Directorate of the Criminal Investigation Department (CID), he was transferred to Dry Dock prison on 3 August, only to be transferred back to the CID and then taken before a prosecutor and allegedly forced to sign a confession. He was also reportedly mistreated and tortured. As with Hubail, a judge postponed hearing his case for a month on 16 February 2014.

The blogger **Mohamed Hassan** was released a few weeks after being arrested on 31 July 2013 but is still facing charges of »managing (electronic) accounts calling for the d overthrow«, promoting and inciting hatred against the government, inciting others to disobey the law, and calling for illegal demonstrations.

Abduljalil Al-Singace, a blogger who ran the Al-Haq Movement's human rights bureau, has been held since March 2011 and is serving a life sentence that was upheld on appeal on 4 September 2012. He is one of 13 opposition leaders and activists convicted of »creating and running a terrorist group aimed at changing the constitution and system of monarchy (…) by force«, »being in contact with a foreign terrorist group that acts in the interests of a foreign country and carries out hostile actions against Bahrain«, and »raising funds for this group«.

IRAN: SUPREME COUNCIL FOR CYBERSPACE, WORKING GROUP FOR IDENTIFYING CRIMINAL CONTENT, REVOLUTIONARY GUARDS

Content filtering, control over Internet service providers, the interception of communications, cyber attacks and the imprisonment of bloggers and netizens are common practice in Iran. Three bodies are responsible for carrying out this policy of repression inside the country: the Supreme Council for Cyberspace, the Organized Crime Surveillance Centre and the Revolutionary Guards.

Supreme Council for Cyberspace

The Supreme Council for Cyberspace was formed in March 2012 by **Ayatollah Ali Khamenei**. Its mission is to protect Iranians from Internet dangers. It is composed of senior military and political figures including the speaker of parliament, the head of the judiciary the ministers of culture and intelligence, the commander of the Republican Guards and the attorney general.

Iran's legal system is expected to carry out the orders of the Supreme Council for Cyberspace but judges and prosecutors can also decide on their own initiative to block access to a site. Censorship procedures are far from clear in Iran.

Working Group for Identifying Criminal Content

The policies and decisions of the Supreme Council for Cyberspace are applied and carried out by the Working Group for Identifying Criminal Content. The group was created in 2008 under article 22 of the law on Internet crimes and has 13 members[1]. It comes under the responsibility of the attorney general. Since it was created, it has ordered the temporary or permanent closure of hundreds of news sites. On its website (add link here), the group encourages citizens to report criminal content and prides itself on having received 500,000 voluntary reports.

1 The ministers of education, information and communication technology, intelligence, justice, science, research and technology, culture and Islamic guidance, as well as the head of the police force, two members of parliament including an IT expert and a jurist, the head of the Islamic Propaganda Organization, the head of the national broadcasting organization and a representative of the Supreme Council of the Cultural Revolution.

Revolutionary Guards

This military organization was formed on 5 May 1979 to combat counter-revolutionary forces. It was placed under the direct authority of Ayatollah Ruhollah Khomeini, the leader of Iran's Islamic revolution. Khomeini. Since then, the Revolutionary Guards have become a sprawling network that exercises its influence in various sectors of Iranian society. Its privileged position allows it to act as the main agent in content filtering and online censorship, and cracking down on netizens.

In 2009, the Revolutionary Guards formed the *Organized Crime Surveillance Centre*, which is the public and media face of the online crackdown. When it was formed, the Centre officially announced the dismantling of a »malevolent« online network and the arrests of those behind the incriminated websites. A few days later, »confessions« of those arrested, together with their photos, were posted on the *Organized Crime Surveillance Centre* website http://www.gerdab.ir. Those arrested were forced to admit to their intention of »corrupting« Iranian youth by publicising pornographic sites and to participating in a plot supported by the Americans and the Israelis.

When the telecommunications sector was privatized in 2009, the Revolutionary Guards took over the Telecommunication Company of Iran (TCI), which owns the main Internet service provider in Iran. Every Iranian ISP has to lease its bandwidth from the TCI.

The TCI is also responsible for ordering the blocking of websites and boasts it has blocked access to millions of sites. In practical terms, thousands of sites and millions of pages cannot be accessed. Censorship, designed officially to protect the public from immoral content, has been extended to cover political news and information. **Today it is easier to access pornography online than websites that are critical of the government.**

The Revolutionary Guards run several parallel branches and sections that specialise in repression. The intelligence department, analogous to the intelligence ministry, has a detention centre in Evin prison, known as section 2A, where no laws apply. Several former detainees report that solitary confinement and torture are routinely used to obtain confessions. The netizen **Vahid Asghari**, whose only crime is hosting the websites of government opponents, has been held since 2008 and subjected to such atrocities.

Halal Internet

No matter how diligently the Supreme Council for Cyberspace and the Working Group for Identifying Criminal Content work to make the Internet a »safe« place for Iran's citizens, it is not enough for the Iranian authorities. For more than 10 years they have been working to establish a national network that is not connected to the World Wide Web, known as »our own Internet« or the »Halal Internet«. The government of former president Mahmoud Ahmadinejad, supported by the Supreme Leader of the Islamic Revolution, Ayatollah Ali Khamenei, moved quickly to set it up after a series of cyber attacks on Iran's nuclear installations. Ahmadinejad's successor Hassan Rohani followed suit. On 23 January this year, the official news agency ISNA quoted the president as saying a national news and information broadband network was on the agenda for next year.

The authorities' Halal Internet idea has been around for 10 years or so. To help implement the closed network, Iran has sought expertise from another country well versed in the control of information: China. Their co-operation was unveiled by the deputy information minister, Nasrollah Jahangiri, during a visit to Iran by a delegation from the Chinese State Council Information Office. In an official statement on the information ministry website, he said: »We welcome co-operation between our two countries in the management of the Internet market … We hope to take advantage of the expertise of Chinese companies to install a national news and information network in Iran…«

News websites attacked, netizens persecuted

According to information received by Reporters Without Borders, the email accounts of Iranian Internet users, mostly journalists and political activists, were targeted by a wave of online attacks in late 2013. This is a method often used by the Islamic Republic to identify sources and contacts and to gather evidence against journalists and political activists

On 12 July, the website Narenji (»orange« in Farsi), which specialises in new technology, reported that seven members of its editorial staff had been arrested and the site could no longer be updated. The statement was removed from the site a few hours later.

Local journalists reported that eight young new media specialists had been detained. Ali Asghar Hormand, Abass Vahedi, Alireza Vaziri, Nassim Nikmehr, Malieh Nakehi, Mohammad Hossien Mossazadeh and Sara Sajad were arrested and taken to an unknown location after their homes were searched and personal effects removed.

On 13 July, a Tehran Revolutionary Court sentenced seven contributors to the Sufi website Majzooban Noor to long prison terms. They were found guilty of propaganda against the state, insulting the Supreme Leader and endangering national security. Hamidreza Moradi was jailed for 10 years, Reza Entesari for eight-and-a-half years, and Mostafa Daneshjo, Farshid Yadollahi, Amir Islami, Omid Behrouzi and Afshin Karampour for seven-and-a-half years each. All were also banned from political and journalistic activity for five years. The netizens, who had been held in Evin prison since September 2011, and their lawyers boycotted the hearings in the unfair trial.

On 4 December 2013, a website allied with the Revolutionary Guards reported that the Guards' intelligence section had arrested 16 cyber-activists in the city of Kerman. They were accused of »being in contact with enemy media outlets based abroad with the aim of producing content for educational websites targeted at citizen-journalists«.

In early December, cyber attacks were launched against several opposition and news websites, including Nedai Sabaz Azadi, Sabznameh, Sabez Procxi, Norooz, Ostan-ban, and 30mail. Responsibility for the attacks was claimed by the cyber army of the Revolutionary Guards in Kerman province.

The website Entekhab (The Choice) has been unavailable since 1 February as a result of a complaint made by the Tehran public prosecutor and a closure order issued by the Tehran media court.

Entekhab editor Mstafa Faghihi told the government news agency Irna that the site was blocked for publishing a letter in which a university academic criticized Iran's nuclear policy as well as other sensitive issues such as public health and education.

On 16 February, a Tehran revolutionary court sentenced Arash Moghadam to eight years in prison on charges of anti-government propaganda and »insulting Islam's sacred values« in connection with content he posted on Facebook.

Arrested at his Tehran home by men in plainclothes last August, he had been detained ever since in Section 350 of Tehran's Evin prison.

SAUDI ARABIA: COMMUNICATIONS AND INFORMATION TECHNOLOGY COMMISSION, INTERNET SERVICES UNIT

Surveillance and censorship of the Internet, relentless in the kingdom for many years, intensified after the popular uprisings in the Arab world in 2011, cutting still further the only free space where non-official views, news and information could be published. The latest target in the Saudi authorities' sights is the video platform YouTube, which has been blocked since last December. Six months earlier, the Viber messaging service was cut off.

The main Internet Enemies are the Communication and Information Technology Commission and the Internet Services Unit. Far from concealing their actions, the authorities openly attest to their censorship practices and claim to have blocked some 400,000 sites.

The main regulatory agencies

The Communications and Information Technology Commission (CITC) has been responsible for regulating the Internet in the country since 2006, censoring thousands of websites.

The Saudi Arabian National Center for Science & Technology (SANCST) was established as an independent scientific organization in 1977 to promote the development of science and technology in Saudi Arabia. There was a change of direction in 1985, when the centre became the King Abdulaziz City for Science and Technology (KACST). This is the backbone of the Internet in Saudi Arabia and the place where all Saudi domain names are registered. Since October 2006, the CITC has taken over its content-filtering role.

Citizens are encouraged to report sites with a view to having them blocked. These requests, previously centralized and managed by the Internet Services Unit (ISU), linked to the KACST, are now handled by the CITC, as stated on the ISU site. It takes just a few mouse-clicks for a user to report a site or a page to be blocked or unblocked.

Late last year, after an article was published in the newspaper *Al-Hayat*, there was a rumour that the Saudi broadcasting authorities wanted to create a new body to censor and monitor video content on YouTube and other sites.

Another idea under consideration was to require Saudis who wanted to share videos online to obtain a permit from this new agency and comply with its terms and conditions for the production of content. Only YouTube use compatible with Saudi »culture, values and traditions« would be permitted. It was not clear whether such censorship would apply to videos posted in Saudi Arabia itself or to all YouTube content. The head of the commission was critical of the article, but he stopped short of denying it.

The whole thing was tied together by the state-owned company Saudi Telecom Company (STC), which for long was the country's sole telecoms operator for mobile and Internet technology before the market was opened up. However, all licences of private companies are granted by the STC.

Internet cafés are also monitored. They must have concealed video cameras and keep an accurate record of their customers and note their identities.

The licence – stamp of approval

Culture and information minister Abdul Aziz Khoja, published new regulations for news and information websites in January 2011 aimed at reinforcing Internet censorship and dissuading Web users from creating their own sites and blogs.

According article 7 of the regulations, online media, the websites of so-called traditional media and platforms offering audio and video content or advertising now have to register with, and receive accreditation from, the culture and information ministry for a licence that must renewed every three years. A licence is valid for only three years. An applicant must be a Saudi national, aged at least 20, have a high school qualification and be able to produce »documents testifying to good conduct«.

All these online media will also have to identify the company that hosts them. According to the original regulations, the ministry would also have had to approve the editor of each online newspaper, who would be the guarantor of the site's entire content. However, the minister scrapped this provision after an outcry. The ministry will now just have to be notified of the editor's name. Its approval will not be required.

Online forums, blogs, personal websites, distribution lists, electronic archives and chat sites thereafter had to be registered. Bloggers were able to identify themselves »if they want«, but anonymity was clearly regarded as undesirable. Last month the authorities ruled that bloggers must use their real names.

Under article 17, any breach of these regulations will incur a fine and a partial or total block on the website concerned. Fines can be as high as 100,000 Saudi rials (20,000 euros). The ministry retains the right to broaden the scope of these measures.

Strict content filtering policy

A strict filtering policy is applied to any content deemed by the authorities to be pornographic, or »morally reprehensible«. Websites that discuss religious or human rights issues or the opposition viewpoints are also blocked.

Prohibited websites now include the Arab Network for Human Rights Information (ANHRI), and the sites gulfissues.net, saudiinstitute.org and saudiaffairs.net. Other sites have been blocked in response the Arab uprisings. In addition, there is increased surveillance of online forums and social networking sites, especially those that are participative.

The CITC announced in June last year that it had cut off access to the Viber messaging service, a free voice-over-Internet application, because it had failed to meet »the regulatory requirements and laws in Saudi Arabia«.

The authorities decided to target YouTube last December after the success of the campaign to allow women to drive in Saudi Arabia and of the video »No Woman, No Drive« a parody of the Bob Marley song »No Woman, No Cry« by the Saudi comedian Hisham Fageeh.

Last month, the NGO Arab Network for Human Rights Information, reported the closure of dozens of sites that were »opposed to the values of the Saudi government« and that 41 others had been shut down on the grounds that they had not complied with legislation requiring them to be registered.

Cyber dissidents jailed

Bloggers who dare to tackle sensitive subjects are liable to retaliation by the censors. Last July a Jeddah criminal court sentenced the cyber-activist **Raef Badawi** to seven years in prison and 600 lashes. The founder of Saudi Liberals, a website for political and social debate that has been censored since its creation in 2008, Badawi has been held in Jeddah's Briman prison since his arrest on 17 June 2012.

He was accused of creating and moderating a website that insulted religion and religious officials, including the Committee for the Promotion of Virtue and Prevention of Vice, and violated the Sharia's basic rules. Judge Faris Al-Harbi added three months to his sentence for »parental disobedience«.

Tariq al-Mubarak, a blogger and columnist who writes for the London-based Saudi newspaper *Asharq al-Awsat,* was arrested on 27 October last year after he wrote opinion pieces for the newspaper on subjects regarded as controversial in Saudi Arabia. In one of his stories published in its print edition on 6 October and headlined »It's Time to Change Women's Place in the Arab World«, he criticized the ban on women drivers. In another column published on 26 October and entitled »When the mafia threatens…«, he deplored the reign of terror in Arab societies that prevented people from fully enjoying fundamental freedoms. He was released after spending eight days in detention.

In late October, human rights lawyer Waleed Abu Al-Khair – Raef Badawi's counsel – was sentenced to three months' imprisonment for signing a petition in 2011 that criticized the heavy sentences imposed on 16 Saudi reformists.

SYRIA: SYRIAN TELECOMMUNICATIONS ESTABLISHMENT, SYRIAN COMPUTER SOCIETY

ONLINE TRACKING IS A FAMILY AFFAIR

In March 2011, the government of President Bashar al-Assad violently cracked down on peaceful demonstrations calling for democratic reforms. The authorities strengthened their control over all means of communication, including the Internet. This was relatively straightforward because of the stranglehold the authorities and the Assad family have over the telecoms infrastructure through three companies – the Syrian Telecommunications Establishment (STE), the Syrian Computer Society (SCS) and Syriatel. These companies ensured a reduction in Internet capacity in order to slow down the circulation of news and images of the demonstrations and the subsequent crackdown. With the help of units within the security services, they can deploy a whole armoury of weapons to monitor the Web and trace activists and dissidents.

Control over the infrastructure

In 2011 figures, nearly 4.5 million Syrians, 20 percent of the population, were connected to the Internet network, which is controlled by two bodies: the Syrian Telecommunications Establishment (STE) and the Syrian Computer Society (SCS).

The STE, more commonly known as Syrian Telecom, is headed by President Assad and comes under the ministry of communications and technology.

There are a number of Internet service providers in Syria but the STE, the government-run ISP, is key since all the others depend on it and it controls most fixed connections. It has granted other ADSL operators the use of its cables. Alternatively, users connect via landlines and 56K modems. It administers all connection points between Syria and the global Internet network.

When the government orders the blocking of a word, of a URL or of a site, the STE transmits the order to service providers.

The SCS was set up in 1989 by Bassel Al-Assad, the eldest son of Hafez al-Assad, with the declared aim »to diffuse informatics culture by means of organizing conferences, symposia, seminars, lectures, and exhibitions, in addition to producing TV programs and issuing pamphlets concerning IT«.

The STE controls the cable network and the SCS all wireless networking, since it owns the 3G network infrastructure throughout Syria. After the death of Bassel, Bashar al-Assad took over as head of this body, which is now controlled by his wife, Asma.

Syriatel is a mobile network operator owned by Rami Makhlouf, a cousin of Bashar al-Assad's and it has no qualms about placing its technology at the disposal of the government in order to monitor the Internet.

The watchful eye of the security services

In addition to these bodies, each branch of the security services has a section devoted to Internet-related issues. The political security department and the state security department monitor the activities of Internet cafés. They make no bones about privatising surveillance by paying individuals to browse the Web, infiltrate Facebook groups and compile reports for the security services.

Syria's electronic army

The Syrian Electronic Army (SEA) first appeared on Facebook in April 2011. In mid-May 2011 a site was launched by »Syrian enthusiasts« to fight those who use the Internet, and especially Facebook, to spread hatred and destabilize security in Syria. The Syrian Electronic Army is not officially linked to the government but reports indicate that the domain name of the SEA was registered on 5 May 2011 by the Syrian Telecommunications Establishment and the site is hosted by SCS-NET, the SCS Internet service provider.

The cyber army floods the pages and websites that support the protests with pro-Assad messages and tries to discredit the opposition. Twitter accounts have been created to compromise information published under the hashtag #Syria. The SEA also hacked the Twitter accounts of several news organizations in 2013, including Reuters, the Associated Press, the Guardian, the Washington Post, the Atlantic Wire, CNN, Time and Al-Jazeera.

Jihadists play the same game

Unfortunately, the Syrian government is not the only agent of repression and control of information on the Internet. Jihadi groups such as Jabhat al-Nusra and the Islamic State of Iraq and the Levant (ISIS) also monitor news and information online. These organizations do not have the resources of the Syrian government but are still able to monitor social networking sites and infiltrate Facebook groups.

Muhammad al-Salloum, the editor of the magazine Gherbal, was forced to flee the country after he was kidnapped by ISIS in the southern outskirts of the city of Idlib in the Kafr Nabl region. The judge appointed by the group accused him of apostasy in his work as a journalist and the reports on the armed group that he posted online. The judge was particularly interested in the online activities of his fellow journalists, such as Mohammad Mallak, editor of the magazine Dawda.

Beware the malware trap

Internet content filtering, as carried out by the STE, is aimed at censoring all criticism of the government as well as the websites of opposition parties, Kurdish and Islamic sites, some news organizations and blogs, and foreign and domestic human rights organizations. The use of tools to bypass censorship and log on to censored sites is banned.

For years records have been kept of Internet users in Syria. Internet café owners must log users' identities and usage times, as well as which computer was used. This information is then sent on to the security services. The IP addresses of machines in Internet café are registered and cannot be changed without prior agreement.

Anyone wishing to take out an Internet subscription must provide the ISP with a copy of their identity card and the telephone number of the line that they plan to use for Internet access.

The authorities use a huge array of techniques to gain access to the Facebook accounts and email inboxes of government opponents. Phishing, »man in the middle« attacks and planting malware are frequently used in Internet attacks in Syria. Syrian authorities have taken advantage of Iran's expertise in online surveillance and has used filtering equipment supplied by the U.S. firm Blue Coat, named an »Internet enemy« by Reporters Without Borders in 2013. The case shows just how important it is to keep track of Internet surveillance and censorship equipment that is exported.

Dissidents voices silenced

Such Internet surveillance has allowed the government to arrest many Syrian activists, media workers and dissidents since March 2011. Syrian security services have launched an all-out manhunt for news providers who assist or have contact with foreign news organizations or reporters. Dozens of Syrians involved in the news industry have been arrested and tortured after giving interviews to foreign news organizations about the repression in their country.

The experiences of those who have been released are enlightening: the intelligence agents who questioned them knew all about their activities and their contacts. Countless people have been arrested for »liking« a page supporting the uprising or for posting videos of demonstrations. Some of these cases are listed below:

Taymour Karim, a 31-year-old doctor, took part in anti-government protests. After his arrests in December 2012, he refused to divulge the names of his friends. However, his computer had already yielded its secrets to his interrogators. »They knew everything about me«, he said. »The people I talked to, the plans, the dates, the stories of other people, every movement, every word I said through Skype. They even knew the password of my Skype account.«

Shaza al-Maddad, a contributor to several commercial news organizations such as the opposition news site all4syria.info, was arrested by Syrian intelligence in November 2012. She was held for 60 days by the security services then imprisoned for more than 9 months. The government seized all her belongings and froze her assets. She managed to flee to Lebanon in September last year and now lives in Europe.

Ali Eid was the Syria correspondent of the Saudi newspaper *Akkad* and also worked for the Syrian news agency *Sana* until he resigned in June 2012. He was arrested several times for reporting on mass demonstrations and on abuses carried out by army troops. In March 2012, government militiamen insulted and beat him up because of his news reports from the Deraa region.

Eid was summoned several times by the air force intelligence service. He was subjected to ill-treatment and abuse during questioning after his final summons in September 2012, when it was discovered he had contributed to foreign news organizations including *Al-Jazeera*.

Eid decided to leave for Egypt and then moved to another nearby country in January 2013.

UNITED ARAB EMIRATES: TELECOMMUNICATIONS REGULATORY AUTHORITY AND CYBER-CRIME UNITS

TRACKING »CYBER-CRIMINALS«

Feeling threatened, the Emirati authorities took advantage of regional political tension in 2011 to step up control of information and communications with the aim shoring up the regime. They tried to impose a new blackout in 2013 on the trial of 94 Emiratis accused of links with Al-Islah (a party affiliated to the Muslim Brotherhood) and conspiring against the government. Only carefully chosen national media were allowed to attend the hearing and two netizens were convicted for tweeting about the trial.

The Telecommunications Regulatory Authority (TRA) and the cyber-crime units attached to the security apparatus coordinate Internet surveillance and censorship. The adoption of a cyber-crime law (Federal Legal Decree No. 5/2012) in late 2012 reinforced the legislative arsenal for gagging criticism in a country where the judiciary is under the executive's control.

TRA and filtering

Created in 2003, the Telecommunications Regulatory Authority (TRA) is responsible for overseeing the telecommunications sector and information technology in the UAE. It reports to the cabinet, which is the UAE's chief executive body. It is also responsible for Internet regulation and compiling the list of sites to be censored.

The TRA counts on compliance by the UAE's two Internet Service Providers: **Emirates Telecommunications Corporation** (better known as **Etisalat** or »communications« in Arabic), which was for a long time the only ISP and mobile phone operator and still is the main one, and **Emirates Integrated Telecommunications Company (EITC)**, better known as **»Du«**, which was launched in February 2006.

The TRA website lists seven categories of websites that are blocked in the UAE:

1. Content conflicting with UAE ethics and morals, including nudity and dating
2. Content containing material that expresses hate of religions
3. Content conflicting with UAE Laws
4. Content that allows or helps users to access blocked content
5. Content that directly or indirectly poses a risk to UAE Internet users, such as phishing websites, hacking tools and spyware
6. Content related to gambling
7. Content providing information about purchasing, manufacturing, promoting and using illegal drugs.

Some sites post the list of blocked sites. In reality, they include all websites or web pages covering subjects related to the human rights situations (including the site of the Emirates Centre for Human Rights) or to political and even religious matters. The online versions of some newspapers, and proxy sites are also inaccessible. Skype was inaccessible until 2013. The filtering has been stepped up since the Arab uprisings.

The **cyber-crimes law** that was adopted at the end of 2012 (Federal Legal Decree No. 5/2012) reinforced repressive legislation dating back to 2006. The long list of online activities that are criminalized by this law constitutes a grave threat to freedom of expression and information in the UAE. Defaming the state and its institutions online is among the activities punishable by imprisonment. Many human rights organizations, including Reporters Without Borders, have expressed their concern about the use of this law to restrict freedom of expression and information and to crack down on dissent.

Cyber-police and Internet surveillance

The authorities use a cyber-police force to monitor the Internet, including its use by human rights activists. Abu Dhabi's State Security Apparatus (usually referred to as the SSA) has created a unit specialized in cyber-crime to spy on the Internet and its users. Abu Dhabi's SSA is widely reported to get its orders from the emirate's crown prince.

A special unit called the Department of Anti-Electronic Crimes has also been created within the Criminal Investigation Department of the Dubai police. As the authorities have a very broad view of what constitutes cyber-crime, many journalists, bloggers and human rights defenders have run afoul of this unit.

Referring to its round-the-clock cyber patrolling, the unit's deputy director, Maj. Salem Obaid Salmeen, said in an interview in April 2012: »These electronic patrols are detecting and tracking all topics and materials written and presented on these websites.« He also said: »Dubai's police is equipped with the latest technologies in the field and has a qualified team specializing in anti-electronic crimes«, adding that they could identify someone from data kept for up to 18 months on servers. Any person »subjected to abuse, insult or defamation on social networking sites« could file a complaint with the unit, which would initiate proceedings against the site after verifying the complaint.

A UAE presidential decree created a »National Department of Electronic Security« in 2012. Little has emerged about this new entity, how it operates or what its function are. The lack of transparency has encouraged rumours. According to some, it is an extension of Abu Dhabi's SSA.

Arrests of netizens

Two Emirati netizens were convicted under the cyber-crime law in 2013 for posting information about a trial during the first half of the year in which 94 Emiratis (known as the "UAE 94") were accused of plotting against the government and being members of Al-Islah, a local group with links to Egypt's Muslim Brotherhood.

One of these two netizens, **Abdullah Al-Hadidi**, who was arrested on 22 March 2013, received a 10-month jail sentence that was confirmed on appeal on 22 May. He was released on 1 November after being deemed to have completed his sentence.

The other, **Waleed Al-Shehhi**, arrested on 11 May 2013, was sentenced on 18 November 2013 to two years in prison and a fine of 500,000 dirhams (100,360 euros) for tweeting about the trial. He was convicted under articles 28 and 29 of the cyber-crime law, which forbid the use of information technology for activities »endangering state security« and »harming the reputation of the state«. Shehhi said he was mistreated and tortured following his arrest but these claims were never investigated, in violation of article 12 of the UN Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment.

Other information providers have been arrested under the cyber-crime law. **Mohamed Al-Zumer**, for example, was sentenced on 25 December 2013 to three years in prison and a fine of 500,000 dirhams on charges of »insulting the country's leaders« and »defaming the security apparatus« on Twitter and YouTube for accusing them of torturing prisoners of opinion. In a video, he also reportedly criticized a contract that Abu Dhabi's crown prince signed with the security company Blackwater for the creation of a private militia to suppress any civilian unrest. His YouTube account (islamway11000) has been closed ever since.

In the same trial, **Abdulrahman Omar Bajubair**, a netizen currently living in Qatar, was sentenced in absentia to five years in prison on a charge of defaming judges by creating and running the @intihakatand and @uaemot Twitter accounts, which document the mistreatment of prisoners of opinion. Another netizen, **Khalifa Al-Nuaimi**, was acquitted under the cyber-crime law but is still serving the sentence he received in the UAE 94 trial.

ASIA AND PACIFIC

CHINA: STATE INTERNET INFORMATION OFFICE

THE GREAT FIREWALL GETS HIGHER

China's leaders realized at a very early stage that the Internet was not just a free speech medium but also a major political challenge. To justify their oppressive censorship and systematic surveillance of the Internet and its users, they stress the need to ensure the country's stability and harmony. Although China's Internet is one of most regulated in the world, it continues to serve as an exceptional vehicle for circulating information.

Since 2011, it is the *Guojia Hulianwang Xinxi Bangongshi* or State Internet Information Office (SIIO) that drafts the government's directives on the dissemination and censorship of information online. It is attached to the *Guowuyuan Xinwen Bangongshi* or State Council Information Office (SCIO), also known as *Guoxinban* for short.

The head of the SCIO, Cai Mingzhao, is a former editor of *People's Daily (Renminribao)* and former deputy president of the official *New China* news agency *(Xinhuashe)*. He is also deputy head of the Department of Communication of the Central Committee of the Chinese Communist Party (CCP) and head of the Central Committee's Office of External Communication. His predecessor, Wang Chen, another former *People's Daily* editor, was elected general secretary of the Permanent Committee of the National People's Congress.

China's leading propaganda agency, the SIIO is also the world's most centralized censorship office. It is in charge of approving the content circulating on the Internet and on related services. It also supervises the online dissemination of information coming from the CCP and the government. The propaganda may be disseminated by means of official blogs or by the so-called »50 Cent Party« (Wumaodang), bloggers who are recruited and paid the derisory sum of 50 cents for every post carrying pro-government information or promoting the party line.

Far from being just a censorship and propaganda office, the SIIO also performs a regulatory function, which includes supervising the allocation of IP addresses to users and the registration of sites and domains, and Internet Service Providers. In western countries, all these different informational and regulatory functions are usually handled by many different administrative entities or by the private sector.

Directives and self-censorship

The government relies heavily on both self-censorship and censorship by Internet companies. The SIIO is empowered to supervise and punish sites that do not follow the »public commitment to Internet industry self-discipline in China«, a set of rules drawn up »in collaboration« with the Internet Society Of China (ISOC), an alliance of 140 leading Internet entities. Thousands of organizations have signed this »self-censorship undertaking«, including Yahoo, Microsoft and Google.

Bloggers and journalists have a general idea of what content is permitted and what is banned, but the »red lines« that must not be crossed can change at any time. Every day, the government sends »directives« to the media specifying the subjects to be avoided and the subjects to be played up. These directives from the SIIO, or directly from the SCIO, may concern any subject, regardless of how big or small a danger the authorities may think its coverage represents.

Under such conditions, journalists themselves suppress a great deal of content. A recent directive even called for the Reporters Without Borders press freedom index to be censored. While the authorities are aware that a censorship order is not enough to suppress all information on a sensitive subject, it creates obstacles and limits people to what they can find on independent sites or social networks.

The Great Firewall

The entirety of the technology used by China to control the flow of information is often referred to as the »Great Firewall« (Fanghuo Changchen), in allusion to the Great Wall of China. Launched under the name of Golden Shield and gradually installed from the late 1990s onwards, this system has benefitted from the technology, material assistance and skills of the US network equipment and security company Cisco Systems.

The censorship is based on very expensive surveillance technology that all website creators must install at their own cost. It enables surveillance of visitors to the site and rapid identification of the authors of all content, comments and messages. It also includes a system that automatically delays posts until they have been geolocated and human censors have vetted subjects and keywords. To understand how such a system works, Harvard University researchers create a pseudo-social network platform and carried out a detailed analysis of the functions and capabilities of the software used. After a supplier revealed to them that, to satisfy the Chinese government, a site must employ two or three censors for every 50,000 users, they calculated that Internet companies in China employ a total of 50,000 to 75,000 censors.

The technology has evolved quickly in recent years and the authorities now have many tools at their disposal for censoring and monitoring the most active online journalists, bloggers and cyber-dissidents.

VPNs and »obfuscated bridges«

Virtual Private Networks (VPNs) are one of the most effective ways to evade Internet censorship and surveillance (as long as you can trust the VPN's owner). This is also true in China, where the government blocks sophisticated circumvention tools such as TOR. Nowadays, thanks to a system of »obfuscated bridges«, it is still possible to connect to the TOR network and thereby evade censorship anonymously. But few Chinese Internet users seem to be aware of this new software. It is hard for the Chinese government to block VPNs not because of their technical superiority but because they are constantly used by the major western corporations operating in China. Blocking them would cause an outcry and would reduce China's attractiveness for entrepreneurs and investors. The censors nonetheless often render encrypted connections unusable.

Deep Packet Inspection

The government's censorship and surveillance policies includes intensive use of Deep Packet Inspection (DPI), a form of filtering that allows closer inspection of user-generated Internet traffic. DPI is not only used to inspect content but also to slow connections to »undesirable« content and platforms such as Facebook or RWB's website (rsf.org). According to several reports, searching for specific terms on Baidu or Google often causes a connection to slow right down and even become unusable. In 2012, Google's Hong Kong-based Chinese-language search engine warned users against entering sensitive search strings and advised using alternatives. This advice was removed at the Chinese government's request.

Depending on the news and the region

Since Xi Jinping became president in 2013, there have been official campaigns against corruption and online rumours. But the conduct of these campaigns is reserved for the authorities. Any lowly journalist or blogger accusing a party member of corruption is severely punished. In July 2013, the journalist **Liu Hu** accused a party official of involvement in corruption. He was arrested on 23 August on charges of spreading false rumours and defamation and is still facing prosecution.

Many bloggers have been targeted by the campaign against online rumours that was launched in September 2013. According to a specially-issued legal »interpretation«, any »defamatory« online content that is viewed more than 5,000 times or re-posted more than 500 times could result in a sentence of up to three years in prison under article 246 of the penal code for the person who originally posted it. The same month, a 16-year-old school student who questioned the actions of the police on his Weibo account was detained for six days.

Internet control is reinforced whenever the authorities are particularly concerned about the possibility of unrest or protests, especially during major political events. There were crackdowns on bloggers during the Communist Party's 18th Congress in November 2012 and Xi Jinping's installation as president in March 2013.

In November 2012, even Google and Gmail were rendered inaccessible inside China. At the same time, the cyber-dissident **Hu Jia's** Sina Weibo account was shut down for the third time in the space of two months, while certain keywords such as »18th Congress« (十八大) or homophones were censored in Sina Weibo's search engines.

China's provinces are not all treated alike. The »autonomous regions« of Tibet, Inner Mongolia and Xinjiang are subject to much more intensive and sustained Internet censorship than other provinces. Social networks such as Twitter are Facebook are censored and using proxy servers to evade censorship is much riskier. With Internet speeds that are more than twice as slow as in big cities such as Beijing or Shanghai (less than 1.5 Mbps as against 4 Mbps), content control is much harsher, like the treatment of bloggers.

The persecution of **Ilham Tohti**, a prominent Uyghur academic and editor of the Uygurbiz.com website, is emblematic. The target of constant police surveillance, he was held for more than a month in 2009, at a time of rioting in Xinjiang. Arrested again in January 2014, he has been held incommunicado ever since on a charge of separatism, which carries a possible life sentence.

Uyghur-language sites are often blocked and, at times of unrest or rioting in Xinjiang, almost all of the most popular sites, such as Diyarim (www.diyarim.com), Xabnam (www.xabnam.com) and Ulinix (www.ulinix.com), are inaccessible. In a survey of websites dedicated to the Uyghur community in 2009, Reporters Without Borders found that the authorities blocked 85 per cent of the tested sites. Most displayed »connection expired« or temporary error messages, masking the fact that they had been permanently blocked.

In Tibet, filtering and surveillance software has been installed in all public places and companies with Internet connections. The Communist Party boss in Tibet, Chen Quanguo, often steps up content surveillance and censorship. In March 2012, the monitoring of phone and Internet networks was intensified and access to many Tibetan exile blogs and media websites such as Sangdhor.com and Rangdrol.net was blocked. Chen announced in November 2013 that the government would do its utmost to ensure that »only its voice is heard« and that no one received the Dalai Lama's propaganda on the Internet, TV or any other medium.

The world's biggest prison for netizens

China, which has the most sophisticated Internet censorship system, continues to be the world's biggest prison for netizens. At least 70 online information providers are currently in prison because of their Internet activities. They include Nobel peace laureate **Liu Xiaobo**. And at least three of the 30 currently imprisoned journalists were convicted for what they posted online.

The arrest of **Liu Hu**, a journalist with the daily *Xin Kuai Bao* (Modern Express), on 23 August 2013 is indicative of how media personnel are hounded in China. He was charged with disseminating false rumours because he used his Weibo account to urge the authorities to investigate an official for suspected corruption.

Even after release from prison, cyber-dissidents such as **Ai Weiwei** and **Hu Jia** are subject to constant harassment and surveillance, and sometimes house arrest. Hu Jia was arrested on 25 June 2013 while celebrating his birthday with friends, some of them influential bloggers. **Chen Guangcheng's** family has been hounded ever since he fled to the United States. Chen announced in Washington on 5 March 2013 that his jailed nephew, Chen Kegui, had been tortured in detention. Two days later, the police tried to kidnap Chen Kegui's son from a kindergarten but were prevented by Chen Guangcheng's elder brother. **Liu Xia** has been under house arrest ever since her husband, Liu Xiaobo, was awarded his Nobel in December 2010. Her brother, Liu Hui, was sentenced to 11 years in prison in June 2013 on a trumped-up real estate fraud charge.

The Chinese authorities try to get Internet firms to help then censor and track down dissidents. Shi Tao, a journalist and poet, paid the price in 2005. He was sentenced to ten years in prison on a charge of divulging state secrets after Yahoo's Hong Kong office provided the information that allowed the authorities to identify him as the person who had circulated an email about Tiananmen Square censorship. Since then, Yahoo's collaboration with the regime has been linked to three other cyber-dissident arrests. Yahoo said it had no choice but to comply with China's law. Unfortunately, it is not alone.

Cracks in the Great Wall?

China is constantly trying to introduce ever stricter controls on Internet use and access to international content but the exponential growth in the number of Chinese Internet users and the steadily expanding volume of content available online is stretching this censorship model to the limit. In particular, social networks such as Sina Weibo, which function as very efficient real-time information tools, are hard to censor effectively with today's resources.

President Xi Jinping was »appointed« head of a cyber-security committee on 26 February 2014. He said he wanted to turn China into a »cyber-power« but stressed that there would be no national security without cyber-security. As long as social networks keep on mocking and embarrassing officials, even questioning their position in the party, the regime will continue to adapt its technological arsenal and human resources to its censorship needs.

INDIA: CENTRE FOR DEVELOPMENT OF TELEMATICS

BIG BROTHER UP AND RUNNING

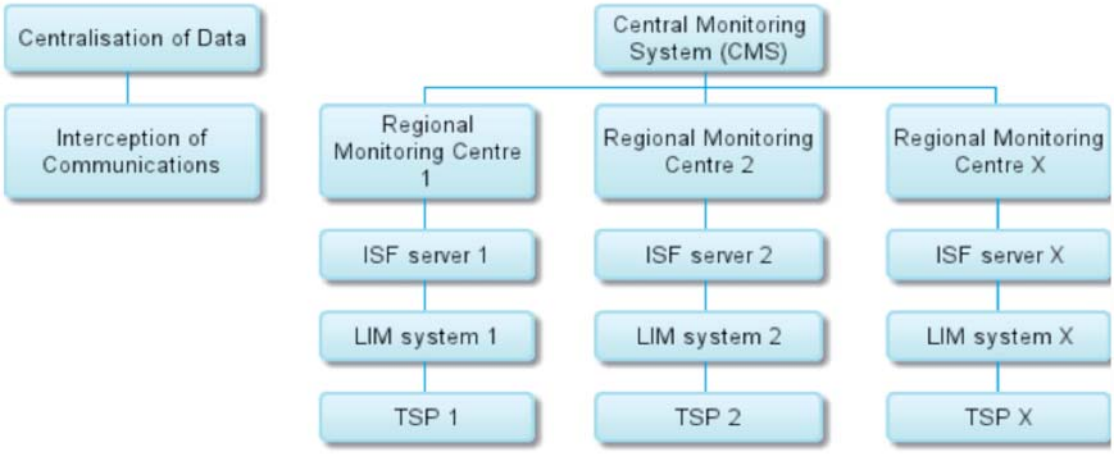
The Indian government carefully refrained from joining the wave of condemnation that followed Edward Snowden's revelations of the scandalous scale of NSA surveillance. India had reason for silence. The extensive Indian surveillance system has been expanded since the Mumbai attacks in 2008. The Central Monitoring System, developed by the Centre for Development of Telematics, allows the government direct, unlimited and real-time access to a wide variety of electronic communications without relying on internet service providers.

The fact that a surveillance system of that magnitude can be established is due to the absence of a legal protection of privacy and personal data. The mission of the Centre for Development of Telematics, created in 1984 by the Ministry of Telecommunications and Information Technology, initially consisted of developing digital communication technology.

Gradually, and in the absence of a law authorizing surveillance, this research centre has become the main contributor to a government-directed monitoring system designed on the massive scale that its objective required. Of India's 1.2 billion citizens, 213 million are web users and 13 per cent of the population use smartphones (Wearesocial.net, January 2014).

The ITA, a law crafted for surveillance

Initially, licence agreements signed by the government in 2002 compel internet service providers to transmit to the government private data concerning their customers. The companies, which bear the cost of software modified to perform this task thus pass on to customers the cost of monitoring them. In addition, some laws, above all the Information Technology Act, known as ITA-2000, authorize the collection of personal data on behalf of the government.



Architecture of Central Monitoring System (source: Centre for Internet and Society)

Amended in 2008 with no parliamentary debate, this law has prompted intense debate in civil society. Many organizations demand that the law be repealed or modified. This is not surprising, as some provisions of the law give the authorities a free hand to mount major surveillance operations against users of the web and other telecommunication technology.

Section 44 authorizes heavy financial penalties against any individual who refuses to provide »any document, return or report« to the government.

Section 66A provides for up to three years in prison for posting »grossly offensive« or »menacing« messages online. The use of vague definitions allows great latitude for officials who are targeting web users, effectively authorizing arbitrary practices. This provision has been singled out for heavy criticism. Some argue that it violates the principle of free expression, in violation of guarantees of fundamental rights in Part III of the Indian constitution. In late 2012, a legal claim a seeking judicial declaration that the provision was invalid was filed in the Allahabad High Court.

Section 69 authorizes the interception of any information transmitted by computer. Likewise, any person who refuses to decrypt his private information upon official request faces up to seven years in prison.

Section 80 authorizes the arrest of suspects even without an arrest warrant.

Since 2011, a series of amendments to the ITA, entitled the Guidelines for Cyber Cafe (PDF) requires internet cafe owners, already required to apply for business licenses, to register the identifies of their customers and save all users' search data, including their log-in information, for one year. A cafe owner must provide these data on demand from any police officer.

The heart of the organism: the Central Monitoring System

This surveillance system, established in 2008 and publicly disclosed in 2009, was designed by the Centre for Development of Telematics. The system is run by no fewer than 34 telecommunications surveillance units, known as Telecom Enforcement Resource and Monitoring cells. At an officially disclosed cost of $72 million, the system intercepts all telecommunications in the country, centralizing the data collected by regional control centres in all states.

The »Lawful Intercept and Monitoring Program« is an element of this giant surveillance system. Established amid great secrecy, then made public in September 2013, it covers all kinds of telecommunications in addition to the internet. The system allows authorities to mount web searches using keywords deemed »sensitive«, without specific authorization, and without notice to internet service providers. This program clearly violates a 2006 government commitment to a policy entitled »Instructions for ensuring privacy of communications«. The policy followed a wiretapping scandal. The LIM, established by the Centre for Development of Telematics, allows analysis of all internet activities, including standard navigation, emails and even Voice over Internet Protocol programmes such as Skype.

With all service providers using a LIM system, itself built on of an »interception, store and forward« server, the collected data is transmitted directly to a »Regional Monitoring Centre«. These regional offices feed their traffic to the Central Monitoring System. The CMS is thus a national database created by the linking of regional databases, who mine user data via surveillance tools deployed by service providers.

Traditional interception systems transmit data only upon official request. But the CMS automates the interception process. The monitoring cells, as well as government agencies, enjoy direct access to web users' data, which is collected without service providers' approval from the internet or mobile phone networks. Agencies with access to this national database include the Intelligence Bureau, the Central Bureau of Investigation, the Directorate of Revenue Intelligence, the Research and Analysis Wing and the National Investigation Agency.

Silence in Kashmir

The Indian government keeps tight control over the internet in Kashmir. Frequently, the government orders internet service providers to suddenly and totally cut off internet access at certain times. The aim is to head off disturbances and, for example, to prevent demonstrations from being organized via social media. This was the case in 2010 and 2012, as well as in July 2013, following the killing of six civilians by Border Security Force officers.

The victims had joined a demonstration protesting a government raid on a mosque. The military responded by shutting down all internet and 3G mobile service in the region. The government subsequently denied having ordered the blackout, but telephone companies said they had been ordered to cut off service as a precautionary measure. An employee of the BSNL phone network told a journalist under cover of anonymity that the firm had received a verbal order to cut off mobile internet and voice service. Downloading speed was also reduced.

NETRA, state-of-the-art spyware

Not slowing down their remarkable progress, Indian authorities have established a spying system capable of real-time detecting of oral as well as written messages deemed to pose a threat. NETRA (NEtwork TRaffic Analysis) was developed by the Centre for Artificial Intelligence and Robotics, a laboratory operated by the Defence Research and Development Organization, a government agency. After small-scale testing, Netra was to be deployed nationally for all intelligence agencies over the course of this year, according to official information reported in the Indian press. The system will cover software such as Skype, status updates and messages posted on Twitter, blogs and forums.

Indian authorities, instead of enacting laws designed to protect citizens' private data, are vastly expanding the reach of surveillance. This policy raises the question of what will come of this endless technology race. Inevitably, repression will be one result.

First victims

With the CMS fairly recently established, only a handful of cases have come to light in which web users have been prosecuted based on the fruits of surveillance. However, a phone wiretapping scandal that broke in 2013 highlights the tendency toward mass surveillance. The so-called »Snoopgate« case grew out of evidence that Gujarat Chief Minister Narendra Modi and his interior minister were involved in wiretapping a young woman. The wiretaps allegedly conducted on behalf of the two men date back to 2009 and allegedly were installed by the state police upon Modi's order.

Another example of the trend toward surveillance in India occurred in November 2012, when two 21-year-old woman were arrested by the police, and placed in detention under Section 66A of the ITA-2008. One of the two, Shaheen Dhada, had commented on Facebook about a national halt of mass transit during the funeral of Indian politician Bal Thackeray. The other young woman, Rinu Shrinivasan, had »liked« the comment. They were freed on bond before the end of the 14-day detention period.

NORTH KOREA: CENTRAL SCIENTIFIC AND TECHNOLOGICAL INFORMATION AGENCY, GROUP 109, BUREAU 27

THE WEB AS A PAWN IN THE POWER GAME

North Korea is one of the few countries where censorship can be judged by what is seen online, rather than what is missing. The country is not linked to the Internet proper and the authorities keep most of the population isolated from the rest of the world and even from the national intranet. The intranet was developed by the Central Scientific and Technological Information Agency (CSTIA) and is highly restricted and closely controlled by the domestic intelligence agencies. Its goal is not to keep the population informed but merely to broadcast the official ideology and strengthen the technical skills of those who work for the fatherland. To enforce this wall of silence, special units such as Group 109 and Department 27 are dedicated to tracking down digital devices brought in from outside the country.

Watertight network

The CSTIA manages access to the World Wide Web. Until 2012, the wired telecommunications system was routed via the Chinese telecoms provider China Netcom and provided North Korea's only link to the global network. In April, a partnership between North Korea and the Thai Internet service provider Loxley Pacific, known as Star Joint Venture, linked the network to the satellite communications provider Intelsat, offering an alternative in the event of problems with China Netcom. Despite the higher speeds offered by the new connection, the authorities' policy of control severely restricts opportunities for browsing the Web for the few Internet users in North Korea. The Pyongyang University of Science and Technology (PUST) provides an example. In 2012, there was just one IP address available for the whole university. Additionally, a record of all previous connections to the outside world is kept on an HTTP server.

The Internet – necessity and threat

For North Korea, the Internet is almost exclusively a means of obtaining the technical information necessary for the country's scientific development. The few researchers and engineers who have access to the network or are able to receive news and information from Koreans abroad are strictly supervised by the government, which ensures that no content that is contrary to the »Juche« ideology formulated by the country's founder and »eternal president« Kim Il-sung falls into their hands.

The connection to the World Wide Web, which is enjoyed by some scientists and researchers, is routed via the ministry of posts and telecommunications, which thus has control over every user who is connected and makes sure only pages for purely scientific purposes are consulted. No cases of illicit browsing have been logged up to now, probably since the harshness of the North Korean regime is enough to deter scientists from visiting »counter-revolutionary« sites.

Computer room at Kim Il Sung University in Pyongyang (AP photo)

All technical and scientific know-how, previously centralized in Pyongyang's main library, the Grand People's Study House, can now circulate freely to the rest of the country thanks to the establishment of a national intranet network dubbed Kwangmyong (»Bright Star«).

The network, which is not connected to the rest of the world, was implemented in 1997 by the CSTIA and allows authorized users to access all information made available by the authorities via a browser, a search engine, email and a discussion forum.

A search page on the Kwangmyong national intranet. Photo: Eric Lafforgue (attendre la permission) https://secure.flickr.com/photos/mytripsmypics/8485292546/

Everyone using the national intranet is monitored by the authorities. Although all pages on the intranet are pre-filtered so that the content causes no political problems, messages exchanged by users are monitored individually. Here, too, scientists are aware of the in-depth monitoring to which they are subjected and know that they would incur severe punishment if they indulged in political discussions or criticism of the government.

Officially, 2 million North Koreans have access to a computer but few are connected to the national intranet. Everyone who owns a computer must register with the authorities. As a consequence, smuggled digital media such as CDs, DVDs and USB sticks have become an important source of news and information from outside the country within just a few years. People can read the content they contain using hi-fi or digital devices that they obtain by similar means, i.e. at vast expense on the black markets scattered throughout the country.

Although the government fears the contamination of its citizens by harmful foreign ideology, it has nonetheless speeded up the development of its telecommunications infrastructure. Last year, the mobile operator Koryolink, a joint venture launched in 2008 between the Egyptian firm Orascom Telecom and the Korea Post and Telecommunications Corporation (KPTC), began providing 3G mobile services for more than 2 million subscribers. This network also operates in isolation and international calls are not permitted. The service is available in all big towns and cities and along the main road and rail routes across the country.

In February last year, Jean Lee, Pyongyang bureau chief for the U.S. news agency Associated Press, was the first member of the foreign media in North Korea to post a wireless Tweet. This was made possible by the new 3G network developed by Koryolink and was symptomatic of greater openness on the part of the authorities, for reasons that are still unexplained.

This connection is available only to foreigners and at great expense: 150 euros to buy a SIM card, 10 euros for a monthly subscription and 150 euros for 2 gigabytes of data. It must also be registered with the government's Korea Communications Center.

Group 109 – censorship's elite force

Numerous departments, groups and units are dedicated to controlling information and cracking down on those who might try to seek information or to circulate censored content. Group 109 is an inter-agency surveillance unit created by Kim Jong-il in 2003. Believed to have been run by his successor Kim Jong-un before he came to power, it is one of the agencies responsible for tracking down content, equipment and digital media that have come from abroad.

According to testimony to a UN commission that was published last month, Group 109 regularly herds people into stadiums where they are made to observe those caught red-handed who are then sent to prison camps to deter others from obtaining illegal content. Agents of Department 27 also carry out unannounced inspections at private homes to try to identify anyone who has secretly acquired contraband electronic equipment, usually from China, in order to receive radio programmes broadcast by North Korean exiles or foreign stations transmitting on short wave, such as the Voice of *America or Radio Free Europe*.

Propaganda as a tool of censorship

The dissemination of North Korean propaganda via the Internet is an increasing part of censorship online, aimed at presenting a positive view of North Korea in contrast to the alarming reports by human rights organizations and the international community.

The means of spreading such disinformation became increasingly sophisticated between 2012 and 2013. Despite the fact that most North Koreans are kept well away from the World Wide Web, more and more sites are springing up, and to date there are at least 11 websites using the .kp domain.

These are aimed at boosting the government's propaganda internationally, being mainly directed at South Koreans and the North Korean community abroad. The information provided by these sites is mostly dedicated to the activities of leader Kim Jong-un, on whom it heaps praise, and the greatness of the country.

In January 2012, the party newspaper *Rodong Sinmun* launched a website in English, less than a year after it went online with a site in Korean. Most of its news is provided by the Korean Central News Agency (KCNA), but the website's launch marked an effort to generate publicity. In an attempt to broaden its relations with its audience, the international radio station *Voice of Korea*, which broadcasts in nine languages, published a letter in September last year announcing it had a new email address and calling on listeners to send information to the station, either printed or on CD, on a variety of topics such as »urbanism« and technology.

조선민주주의인민공화국 라지오 및 텔레비죤방송위원회
The Racio-Television Broadcasting Committee of the DPR of Korea
Le Comité de radiodiffusion et Télévision de la RPD de Corée

Dear listeners,
We would like to thank you for regular listening and helpful opnions and impressions.
How about weather in your town? Please take care of yourself in consideration of the change of weather.
We were glad to read your letters that you had a better understanding of our country through our internet and broadcast.
In the future we will do evertything in our power to produce programmes you like.
Now we inform you of the e-mail address of our Voice of Korea. The e-mail address is VOK@star-co.net.kp. The address will help further developing the friendly relations between our broadcast and listeners.
We hope you would have close contacts and actively cooperate with our broadcast through our e-mail address.
Friendly regards
Looking forward to your reply.

* English or French books or CD-medias about internet, afforestation, urbanism, laughing stories (humor novels), world-famous men and women stories, and technology will be strongly appreciated. Thanks a lot.

Voice of Korea

Letter sent by the Voice of Korea radio to listeners (source: northkoreatech.org)

A dozen YouTube channels relay programmes broadcast by the main TV station *KCTV* and the news agency *KCNA*. The agency's own site was brought updated in January last year, a few weeks before the *Pyongyang Broadcasting Station,* aimed at South Korea, China and Japan, launched its own website, called *Great National Unity.*

Among the new propaganda tools deployed in 2013 was a series of podcasts, uploaded to Apple's iTunes media platform by the North Korea's China-based website Uriminzokkiri.

Cyber war between the two Koreas

Since Internet access is strictly controlled and the national intranet purged of sensitive content, the real information war is ultimately being waged via the global network, i.e. outside the country. In March last year, the three main broadcasters in South Korea, *MBC, KBS* and *YTN*, were the targets of cyber attacks which shut down their servers.

This was believed to have been carried out in response to a previous attack on North Korea blamed on South Korea and the United States. Other attacks were recorded in the weeks that followed. By turns, Pyongyang and Seoul have been targeted by hackers working for their governments, and also by activist groups. The group Anonymous has carried out several attacks on North Korean websites, including that of the *KCNA* news agency.

PAKISTAN: PAKISTAN TELECOMMUNICATION AUTHORITY

In February, 2012, Pakistan's information technology minister invited bids for deployment of a national internet filtering system. China's »Great Firewall« was the inspiration. Pakistani authorities' intent to limit free information access online was confirmed in September, 2012, when Pakistani internet users were denied access to the entire YouTube platform, an official response to posting of the film, »The Innocence of Muslims«, which was deemed blasphemous. Currently, 20,000 to 40,000 sites are blocked in Pakistan. This massive censorship is the work of the Pakistan Telecommunication Authority, the main web regulation agency, itself closely controlled by the government and the military.

Online censorship upgraded

Created in 1997 by the Telecommunication Reorganization Act (1996), the PTA is the main Pakistani regulatory agency overseeing the internet and the telecommunications industry as a whole.[1] The agency is in charge of blocking and filtering, and of licensing internet service providers.

Many experts and human rights organizations challenge the agency's lack of transparency and independence. Aside from the fact that its members are directly appointed by the government and are accountable to the Ministry of Information Technology, the PTA has proved itself opaque in its operations.

For the past several years, members of government security agencies have been directly participating in internet blocking and filtering. The Inter-Ministerial Committee for the Evaluation of Websites, created within the information technology ministry in 2006, is assigned the mission of determining what online content should be blocked. In addition, the committee is assigned with making recommendations to guide the ministry's decisions concerning blocking and filtering. This obscure regulatory body is made up of government officials and security agency staff whose names have not been disclosed.

As a rule, the government issues blocking orders, which go through the inter-ministerial committee, which then transmits them to the information technology ministry and the PTA, which then notifies service providers. But, given the absence of a formal legal structure, the orders can also go directly to the PTA and service providers without participation by the inter-ministerial committee. A service provider that defies an order from the PTA risks a suspension of operating license.

Blacklist of prohibited sites and Netsweeper filtering

The PTA maintains a blacklist of URLs that are blocked through the Internet Exchange Point, the internet backbone over which most internet traffic reaches Pakistan. Blocking is also conducted by internet service providers.

With YouTube access still blocked, evidence points to official use of filtering technology. In June, 2013, Canada's Citizen Lab, a technology research and development organization, published a report in cooperation with the digital freedom defence NGO Bytes for All. The report demonstrated the use on Pakistan's PTCL telecommunication network of »Netsweeper« filtering technology, developed by a Canadian firm.

The PTCL network accounts for about 60 per cent of Pakistan's broadband capacity. The report reveals that the filtering technology was installed to carry out political and social objectives.

In 2006, the OpenNet Initiative, which investigates and reports on digital filtering and censorship, had already assembled evidence of filtering applied to blasphemous content and to sites advocating for the rights and autonomy of the Baloch, Sindhi and Pashtun peoples in Pakistan.

Justifications advanced for blocking and filtering include the fight against terrorism, condemnation of blasphemy and of pornography, as well as the protection of national interests. In recent years, blocking and arbitrary filtering of content have responded to the interests of the armed forces and the political class.[2]

1 Bytes for All report, pp. 3, 18

1 Bytes for All report, p. 3.

The allegedly blasphemous – especially, anti-Islamic – quality of some content is very often a pretext for the PTA to block online access. The authorities are aware of the ease with which they can justify blockage by citing citizens' religious devotion. The blocking of content defined as insulting to Islam is far from unpopular in Pakistan. In many cases, citizen petitions have led to court orders blocking sites. Since the early 2000s, Pakistan has been at the forefront of efforts to make »defamation of religion« a violation of international law.

The government bases its action on laws that do not focus specifically on the web, but which include anti-blasphemy laws and the Anti-Terrorism Act of 1996. The internet is barely mentioned in these statutes. According to Bytes for All, the anti-blasphemy laws now represent the greatest threat to online information freedom in the country. At the same time, content officially defined as anti-government propaganda, whether related to the Balochistan crisis or seen as disseminating a negative image of the political class or the armed forces is systematically made inaccessible to Pakistani web users (ONI report, 2012).

To date, the blacklist of sites is accessible only to the team assigned to establish the centralized database on which it is based. Given the non-transparency of the PTA concerning blocking, the precise number of blocked sites is also unknown. In a report published in November, 2013, Bytes for All estimates that the number may exceed 40,000.

Internet and Telecommunications Blackouts

Since 2012, Pakistani authorities have undertaken mass blocking of mobile phone service. This practice represents a major challenge to online information access because most citizens rely on their phones for internet access. According to Bytes for All, suspension of service during political or religious events has become the norm, especially in big urban centres such as Quetta and Karachi. Security reasons are often used to justify the shutdowns.

For example, on 14 August, 2012, Pakistan's independence day, the PTA ordered suspension of mobile phone service throughout Balochistan for reasons of national security.

Justifications for censorship

On 18 September 2012, the Pakistani government ordered access to the YouTube platform blocked, following posting of the »The Innocence of Muslims«, a film deemed blasphemous. Despite numerous legal motions filed in Pakistani courts challenging this abusive censorship, as well as official declarations making lifting of the blockage conditional on installation of an effective national filtering system, Pakistani web users remain unable to access YouTube.

During the May 2013 national election campaign a video critical of army generals by the band *Beygairat Brigade* was blocked on the Vimeo site.

On 25 September 2013, Pakistan's main gay site, Queerpk.com, was blocked without prior notice. The action took place despite the absence of sexually explicit or pornographic content. According to PTA spokesman Kamran Ali, »We blocked the website under the law because its content was against Islam and norms of Pakistani society«. The site's moderator then re-directed the site to another URL to allow access. The next day, PTA made that site inaccessible as well.

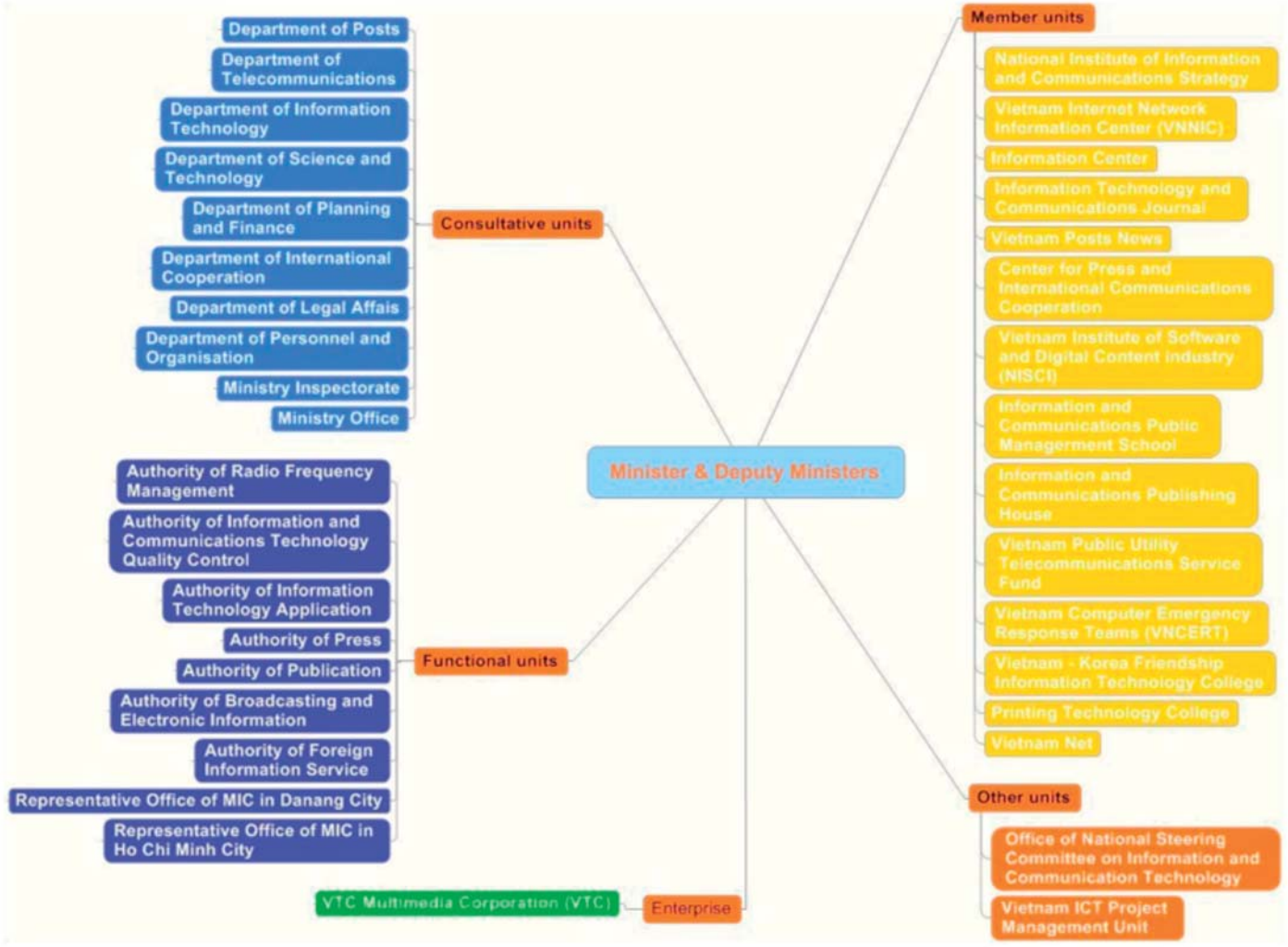
On 3 October, 2013, the provincial government of the Sindh region prohibited instant-message internet phone services including Skype, Whatsapp, Tango and Viber for a period of three months. Security officials claimed that these services were used by armed groups to plan attacks.

VIETNAM: MINISTRY OF INFORMATION AND COMMUNICATIONS

TARGETING BLOGGERS

The Vietnamese government tolerates no online political debate. Bloggers and cyber-dissidents who dare to question the government's legitimacy or domestic policies are ruthlessly suppressed. Authorities have deployed a judicial, administrative and technological strike force, based in the Ministry of Information and Communications, to control online information.

Internet regulation is the ministry's prerogative. The office in charge of the task is the Authority of Broadcasting and Electronic Information. The ministry prepares and proposes laws that allow authorities to justify to the international community prosecutions of bloggers and cyber-dissidents. In order to avoid submitting legislation to the National Assembly, where members could comment on or raise questions about proposed legislation – although there would be no risk of a bill being voted down – these laws take the form of decrees from the prime minister.



Organization chart of the Ministry of Information and Communications (source: http://english.mic.gov.vn/intro/PublishingImages/sodotochuc_en.jpeg)\\

Legislation by decree

These decrees are designed to muzzle information activists – and the platforms that carry their work – from the moment that the Communist Party of Vietnam classifies them as dangerous. For example, **Decree 97**, promulgated in 2009, focuses on political analyses produced by intellectuals and academics.

In November 2013, **Decree 174** was made public. In effect since 15 January 2014, the decree provides for new penalties for netizens who disseminate content that includes »anti-State propaganda«, or »reactionary ideologies« on social media such as Facebook. Although the criminal code already authorizes prison sentences for publication of content deemed »anti-State«, the new decree gives authorities even more latitude to charges netizens whose prosecution under **Articles 79** or **88** of the criminal code would prompted responses by Vietnamese civil society or the international community.

Decree 72: even tougher

Announced on 31 July 2013 and in effect since 1 September of that year, **Decree 72** constitutes an unprecedented assault on freedom of information in Vietnam. The government justifies this law, which restricts the use of blogs and social media to »dissemination« or »sharing« of »personal« information, citing requirements for intellectual property protection.

Decree 72, which expands authorities' legal arsenal, prohibits the use of social media to share information reported in the press. Authorizing the arrest of independent information activists who have not been accused of so-called anti-government propaganda or of »attempt to overthrow the government«, the decree constitutes a tool to maintain the Communist Party in power. At a time of major financial and political instability, the Party is attempting to prevent its legitimacy from being publicly challenged.

Thus, Prime Minister Nguyen Tan Dung has announced publicly that blogs could be used »only to provide and exchange personal information«. In August 2013, Hoang Vinh Bao, director of the Department of Radio, TV and Digital Information in the Ministry of Information and Communications, warned web users against quoting or sharing information issued by press agencies, as well as government websites.

This decree marks the harshest attack on freedom of information since the prime minister's signing of a 2011 decree providing for severe penalties against media personnel.

Online censorship

With private media prohibited, many people try to make themselves heard by putting up blogs and disseminating information. But these sites are relentlessly blocked by firewalls. Site owners often are arrested or subject to harassment if their content differs from the policies of the Communist Party of Vietnam.

The most recent official figures show that Vietnam has more than 3 million bloggers. According to the International Telecommunication Union, Vietnam ranks number three in Southeast Asia in number of web users, and number eight in all of Asia.

Internet businesses and service providers, such as Vietnam Posts and Telecommunications, which are state-owned and account for 74 per cent of the market, and Viettel, owned by the People's Army of Vietnam, are the major web surveillance agencies. On government orders, they block so-called »malicious« sites (including newspapers, blogs, and platforms for political oppositionist or human rights-advocacy content), using the Domain Name System. Passwords are frequently hacked, and connection speeds are often slowed on days when dissidents are arrested or put on trial.

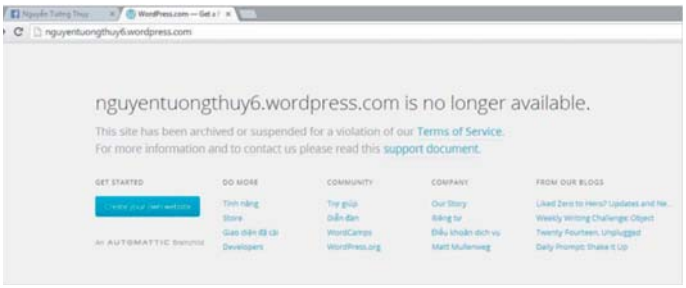
Rigorous surveillance is also the rule on the mobile phone network. Web navigation on the mobile internet is not secure, because the State controls the three major operators, which account for 90 per cent of the market.

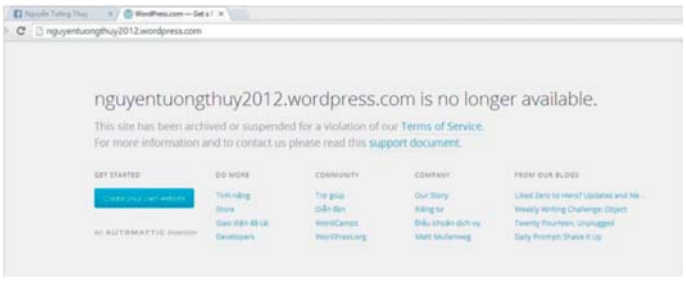
With more than 22 million members, Vietnam has seen the world's biggest growth rate in Facebook membership. Even so, Facebook has been blocked since 2009. The platform remains inaccessible through the major internet service provider, VNPT. Web users can still connect via other providers or by using tools such as VPNs, Tor, or proxy servers. The Wordpress platform is also targeted. In 2013, the connection to blogs that it hosts suffered a major slowdown, and many blogs could not be accessed without censorship-bypass tools.

Shadowing and tapping

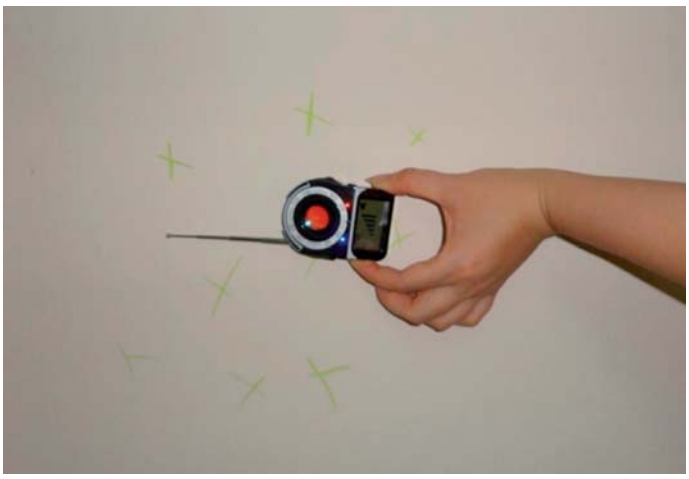
The Communist Party of Vietnam tolerates no online political debate. Anyone who defies this prohibition pays a price. Human-rights lawyer and blogger Le Quoc Quan was arrested in 2012 the day after he published an article criticizing Article 4 of the Vietnamese constitution, which upholds the leading role of the Communist Party in national affairs.

Two sites by blogger Nguyen Tuong Thuy, hosted on Wordpress, were shut down for »violation of terms of service«, with no explanation given to the blogger. In all likelihood, the shutdowns followed repeated demands by government agents.





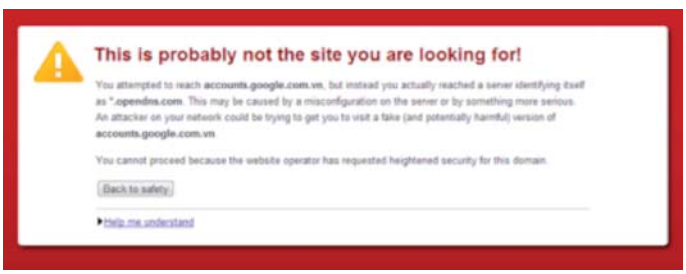
The so-called »nuisance« approach, which targets bloggers without the use of technological tools, reflects a larger official strategy. Use of surveillance and »physical« censorship expanded in 2013. The following of targets in the street, infiltration of pro-democracy movements and personal monitoring have become part of daily life for bloggers. In June, 2013, cyber-dissident Nguyen Van Dai publicly displayed the surveillance to which he was subjected in his own home. After acquiring an electronic bug detector, he found that authorities had been monitoring him from a room adjoining his apartment.



Detector showing the location of microphones hidden behind a wall in the apartment of blogger Nguyen Van Dai.

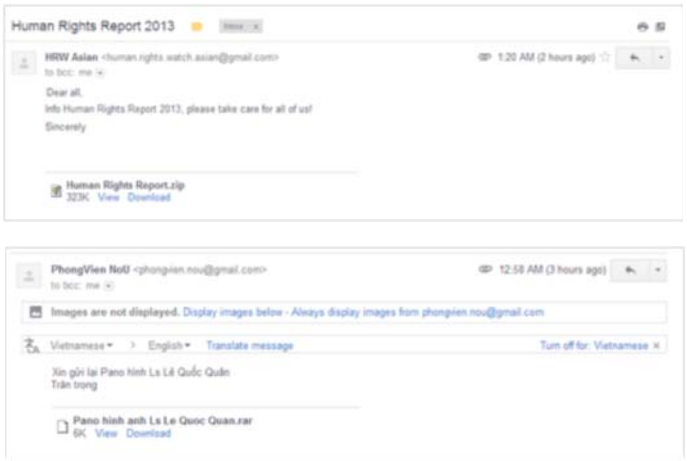
Since 2004, a special unit directed by the Ministry of Public Security has been in charge of operations against electronic crime of all kinds: credit card data theft, hacking, and illegal online gambling. The unit also enforces the prohibited information ban. Many bloggers have been arrested for posting illegal content about the Party. Some of them were taken in after having published criticism on their own blogs, or on their Facebook pages (among them, Huynh Ngọc Chenh, Ba Sam, J.B Nguyen Huu Vinh, Nguoi Buon Gio, Nguyen Quang Lap, Paulus Lê Van Son). Others, writing anonymously on collectively managed information platforms such Dan Lam Bao, Quan Lam Bao, Bauxite Viet Nam, Dong Chua Cuu The, Nu Vuong Cong Ly, as well as Paltalk forums, have been arrested following periods of official surveillance.

»Man in the Middle« attacks, which establish counterfeit sites designed to attract users looking for the genuine versions, are also designed to dissuade readers of content that censors deem sensitive from connecting to foreign-based sites, including their gmail accounts.



Screenshot taken by a Vietnamese cyber-dissident (source: anonymous).

To a growing extent, bloggers and citizen-journalists are receiving emails with attachments that contain viruses. These may install Trojan Horses or shut down users' computers. In using bloggers' contact networks or rendering their work devices inoperable, this malware disrupts targets' activities and discourages information activists from working in groups.



Emails sent to a blogger, with attachments containing malware.

According to the Electronic Frontier Foundation, an NGO, this kind of email has also been sent to an Associated Press journalist, as well as many Vietnamese activists. A Vietnamese blogger living in California was successfully targeted by an attack that led to his blog and his personal information being compromised.

According to the EFF, The group behind these attacks appears to have been operating since late 2009, and has been very active in the targeting of Vietnamese dissidents, people writing on Vietnam, and the Vietnamese diaspora. The [campaign] appears to be the work of a group commonly known as »Sinh Tù' Lệnh«.

Despite these attempts to hamper bloggers' information activity, new information platforms such as Vietnam Path Movement, Defend the Defenders, Vietnam Human Rights Committee, FVPoC (Former Vietnamese Prisoners of Conscience) and Vietmeme, were born in 2013 and 2014, especially in English. These sites reflect the growing determination of Vietnamese bloggers to make sure that their message is heard by the international community.

AFRICA

ETHIOPIA: INFORMATION NETWORK SECURITY AGENCY

Created in 2011 with »Secured Cyber for Peace Development and Democracy« (sic) as its official motto and revamped in 2013, the INSA is at the forefront of the Ethiopian government's Internet control and censorship strategy. Billed as the ultimate rampart against external attacks on Ethiopia's national security, in practice it uses aggressive spyware to monitor news sites and dissident sites, suppress independent reporting and impose the regime's monolithic views.

The INSA is an independent government agency that was created by the Ethiopian parliament in 2011 and revamped in 2013 by means of a legislative proclamation. Its mandate is to protect the country's vital transport, energy, aviation, communication and critical infrastructures from electronic attacks aimed at disabling and/or disrupting or destroying them. Its expanded duties since December 2013 include developing offensive capabilities, launching counter-attacks if and when needed in self-defence, and developing information communication technology tools for the government to systematize and standardize information documentation as well as cater to other ICT needs.

Although, the majority of INSA's ressources are dedicated to development tasks such as designing software for state entities or creating federal databases, the agency is de facto the organisation responsible for on-line surveillance and has a wide range of access to the country's computer and information's networks infrastructure. Thanks to the 2013 proclamation, it is empowered to investigate computers, networks, the Internet, radio and television, and social media (such as Facebook) for possible »damage to the country's social, economic, political and psychological well-being«. The justification given for these enhanced powers is that most infrastructures are now subject to computerized control and therefore social media, outlets, blogs and other Internet media are potentially able to instigate conflicts or war. In fact, the INSA also uses its mandate to monitor and control dissent online and on phone networks, in violation of users' privacy.

Its controlling capabilities are facilitated by the very low level of connectivity in Ethiopia. Despite colossal infrastructure efforts undertaken by the government, Ethiopia remains one of the least connected countries in Africa, with only 1% of Ethiopians having access to the Internet. This seems largely due to the monopoly position of the state-owned telephone and Internet service provider, Ethio Telecomm. Because of its monopoly, Internet access is costly, very slow and unreliable, and there is limited coverage outside of the capital, Addis Ababa.

Legal framework

As well as de facto absolute technical control, the INSA's work is facilitated by the overall political climate and an array of controlling legislation.

While the Ethiopian government admits only to »limited online surveillance«, it is clear, that it sees the Internet as a powerful tool that it rather keep under control. The most concerning element of INSA's power is the total lack of accountability it enjoys. The absence of check-and-balance mechanisms that would allow legislative oversight of the agency's activities allows it to engage in intrusive actions that violate privacy laws and liberty of speech, in total impunity.

On the legislative front, the INSA is buttressed by the July 2012 Proclamation on Telecom Fraud Offences (article 6), which extended the very controversial 2009 Anti-Terrorism Proclamation and the Criminal Code to include electronic communication. Officially aimed at protecting the state's monopoly of telecommunications and safeguarding national security, it violates international standards on the right to freedom of expression and information, especially as it does not define the »national security« it is supposed to protect. This proclamation is also worrying for its lack of clarity on the range of offences that are criminalized. Its criminalization of unofficial VoIP communications caused so much concern that the government was forced to issue a statement promising that Skype would not fall under its purview and that it would not be used to prosecute anyone using free Internet software to make and receive calls. Nevertheless the threat remains as the proclamation was signed into law without a written amendment.

Technology

The INSA is known to use spyware and other kinds of software to monitor and censor the online activities of Ethiopian citizens, whether social activists, opposition members or journalists. At one point, the Ethiopian government considered putting network security and content surveillance out to bid, but finally decided to let the INSA handle all of these duties using Chinese technology. To this end, the government signed an 800-million US dollar contract in August 2013 with ZTE, a Chinese telecom giant that is banned in the United States for alleged hacking of Internet systems and theft of intellectual property. It has also been banned from public bidding in Australia and its contracts have come under scrutiny in Britain.

There have been many credible reports, notably from academic research centres, that the INSA has for several years been using Deep Packet Inspection (DPI), an advanced network filtering method, to selectively target data traffic. In May 2012, it blocked access to the ToR network, which is used to access sites anonymously. The INSA has proved to have a significant technical arsenal for targeting and swiftly removing specific, politically-sensitive websites and web pages, censoring content deemed hostile to the regime and intercepting Internet-based voice communication.

According to Freedom House, Gamma International provided Ethio Telecom with its commercial spyware toolkit FinFisher from April to July 2012. FinFisher can be used to secretly monitor computers, turn on webcams, record everything a user types with a key logger and intercept Skype calls. According to Citizen Lab, FinFisher was used in March 2013 against suspected government opponents, ensnaring them by means of fake Facebook accounts or pictures of Ginbot 7, a persecuted political opposition group.

According to industry sources contacted by Freedom House, INSA technicians have used software that masks the user's identity to gather personal passwords and usernames.

Although there seem to be no hard and fast rules as to which websites should be blocked or allowed, the common denominator seems to be the expression of any kind of political dissent or criticism of the regime. The most obvious censorship method is »untransparent« blocking, in which a requested a web page appears as «Not Available» instead of saying it has been blocked.

Cases

Many journalists and dissidents claim to have had their phones intercepted and their emails read. They have no hard evidence but their claims are supported by the fact that evidence gathered from intercepted telephone conversations and illegally obtained emails was used in the 2012 trial of *Feteh* columnist Reeyot Alemu, who was sentenced to 14 years in prison.

Dureing these same legal proceedings, 5 other journalists were convicted. On line information has also been used to convict journalists, such as Mesfin Negash and Abiye Teklemariam who received eight years each based on accusations of making information about the radical opposition group, »Ginbot 7« available to Ethiopians through their news website, *Addis Neger Online*.

Three other journalists were condemned for their activities with *Ethiopian Satellite Television (ESAT)*, an independent satellite TV, radio and Internet news service run by Ethiopian diaspora members that often criticizes the government, and is considered by this latter »the voice of the terrorist organization Ginbot 7«. Journalists in exile Abebe Gellaw of *Addis Voice* and Abebe Belew of the Internet radio station Addis Dimts were sentenced in absentia to 15 years each, and Fasil Yenealem was sentenced to life.

More recently, ESAT, was hacked three times in the space of two hours on 20 December 2013. Already jammed from within Ethiopia several times in the past few years, it was attacked this time with sophisticated computer spyware that targeted two ESAT employees. Designed to steal files and passwords, and intercept Skype calls and instant messages, the spyware used an IP address belonging to Ariave Satcom, a satellite provider that services Africa, Europe and Asia. In each case, the spyware appeared to be Remote Control System (RCS), which is sold exclusively to governments by Milan-based Hacking Team. Reporters Without Borders named Milan Hacking Team as one of the corporate »Enemies of the Internet« in its 2013 report.

SUDAN: CYBER-JIHADIST UNIT, NATIONAL INTELLIGENCE AND SECURITY SERVICE, NATIONAL TELECOMMUNICATION CORPORATION

The Omar Al-Bashir regime has held Sudan in an iron grip for the past 25 years. As new technologies develop and internet penetration increases (17 per cent of the population was connected in 2012), methods of control and repression have also been evolving.

The Cyber-Jihadist Unit

In 2011, at the height of the Arab Spring, Sudan's ruling National Congress Party, fearing the spread of political challenges from abroad via social media, decided to upgrade its internet surveillance capability by forming a »Cyber Jihadist Unit« assigned to conduct »online defence operations« to »crush« internet dissidents.

Two hundred agents spread throughout the country, working in shifts to provide 24 hour-a-day capability, especially during peak internet usage hours – nights and weekends. The unit was strengthened in 2012, when the Sudanese blogosphere was experiencing an unprecedented boom, growing from 70 to 300 blogs over a period of 18 months.

The security services recruit agents from public higher education institutions including the National Ribat University. New recruits receive online piracy training in Malaysia and India. They are trained to monitor internet content, hack online accounts (email, Facebook, Twitter), block or take down sites and identify targets to put out of action.

However, the Cyber-Jihadist Unit on its own would be insignificant without the protection afforded by its parent organization, the NISS, the main agency for repression and censorship in Sudan.

The National Intelligence and Security Services

The Cyber-Jihadist Unit works with complete freedom of action thanks to the National Security Act of 2010, under which the NISS operates. This law reinforces the impunity with which NISS agents operate, allowing them to arrest any journalist and censor any publication on »national security« grounds. The NISS can keep an individual in detention for up to 45 days without charges, with the authorization renewable when the initial period expires.

Before the cyber unit was created, a series of laws had already authorized control and repression of online information. In 2007, adoption of the IT Crime Act further weakened freedom of expression on the web and imposed penalties of up to two years in prison and heavy fines. People who create web sites critical of the government risk these punishments. In 2008, a law requiring mobile phone owners to register their SIM cards allowed intelligence agencies to more easily trace journalists and activists through their phones.

National Telecommunication Corporation

The NISS and Cyber-Jihadist Unit are reinforced by the NTC. Founded in 1996, the NTC is a government agency in charge of regulating information and communication technology. The NTC formed an Internet Service Control Unit to decide what content should be accessible on the internet. If the government determines some information to be too sensitive, it blocks the host platform. This has occurred repeatedly since 2008 to the news site and forum, *Sudanese Online*, which posted information on the war in Darfur.

In response to the anti-government demonstrations that broke out nationwide in 2013, the NTC frequently blocked the sites for *Sudanese Online*, *Al-Rakaba*, and *Hurriyat* as well *YouTube* and other sites.

The agency went so far as to cut off the internet entirely for the entire country. In June-July 2013, the internet transmission system was slowed to the point that the network was **completely inaccessible for several hours**. On 25 September 2013, a total internet blackout lasted 24 hours. The objective was to hamper the organizing of demonstrations on social networks. As information flow came to a halt, the extent of official repression could not be known for several hours. The NTC denied official responsibility for the blackout, accusing demonstrators. But they had nothing to gain by cutting off their means of communication, and lacked the capacity to do so.

Faced with the expansion of online censorship, a growing number of opposition web sites install their servers abroad. *Sudanese Online*, for example, is hosted in the United States.

NTC and NISS agents' technological shortcomings and limited English-language skills stand as the last barrier against total government control of the internet. Content in English and its authors are subjected less frequently to officially sponsored attacks. The emphasis is on Arabic content, reflecting concerns over domestic developments.

Online news and netizens under attack

The pace of censorship accelerated in 2011-2012. In an effort to bypass controls, some media workers opted to post prohibited content on their Web pages or Facebook profiles. NISS agents then began targeting this form of online journalism. Private emails are increasingly intercepted, and mobile phones are used to geo-locate journalists and activists.

Popular uprisings in June-July, 2012 and June and September of 2013 prompted the arrests of numerous bloggers, journalists and activists. Agents often forced them to open and take down their Facebook and Twitter accounts. This forcible access to personal data also allows security forces to map dissidents' networks.

Video blogger **Najla Sid-Ahmed** was systematically harassed by security services in 2012 and forced to flee the country in July of that year. She became a target because of her videos documenting human rights abuses. NISS agents robbed her, confiscated her audio-visual material, and arrested her, holding her for several hours without food. She was then accused conspiracy and hate incitement, charges punishable by death in Sudan.

Journalist and activist **Somaia Ibrahim Ismail,** known as »Hundosa«, a government opponent, was arrested on 29 October 2010, then seized by security service agents who tortured her for three days, on the pretext of membership in an armed group. She fled the country in November, 2012.

On 22 June 2012, NISS agents arrested **Ussamah Mohamed**, whose tweets and blog postings made him very popular, especially in Burri, a neighbourhood on the outskirts of Khartoum. He was beaten for hours after refusing to unlock his iPhone. He was released in early August, 2012, after a detention marked by long interrogations focused on his Facebook and Twitter accounts, and online opposition forums.

Since 2008, due to its content about the war in Darfur and popular uprisings, the *Sudanese Online* site has been hit by repeated blocking, hacking and infiltration by the NISS cyber brigade. The unit penetrates online discussions to gather information on cyber-dissidents and spread false information. News sites characterized as oppositionist, such as *Al-Rakoba* and *Hurriyat* are frequently blocked. The longest-running of these actions hit Al-Rakoba, which was inaccessible for 10 months, from June, 2012 to April, 2013.

In September, 2012, following the posting of the online video, »The Innocence of Muslims«, which unleashed massive protests throughout the Arab world, NTC blocked YouTube access for one month.

Widespread internet blackouts aimed at shutting down media amount to another form of radical censorship that the regime uses to hamper freedom of information and repress all criticism.

INTERNATIONAL

SURVEILLANCE TRADE FAIRS: TECHNOLOGY AGAINST CRIME, MILIPOL, ISS WORLD

DEALERS AND SURVEILLANCE WEAPONS

In its 2012 report on surveillance, Reporters Without Borders drew attention to several western companies that were guilty of selling surveillance technology to authoritarian governments that violate human rights. The same technology was on display in 2013 at arms trade fairs that attract industrialists and government representatives from the four corners of the planet.

Technology Against Crime (TAC)

More than 600 people from 59 countries participated in the *Technology Against Crime (TAC)* forum held in the French city of Lyon on 8-9 July 2013. French interior minister Manuel Valls and a score of government ministers from all over the world attended the opening. The forum's sponsors and backers included Europol, the European Union and French arms and defence industry firms such as EADS and Thalès.

The technology on show at the TAC is supposed to be for use by police forces in combatting crime, including cybercrime. The firms with stands at the 2013 TAC included the Gamma Group and Hacking Team, which were among the companies that Reporters Without Borders identified as »Enemies of the Internet« in its special report on surveillance. The Gamma Group presented its range of »IT intrusion« products designed for spying on computers and smartphones. Hacking Team offered law enforcement agencies a software suit for hacking into computers and phones.

The presence of representatives from China, Iran and Azerbaijan among those attending the TAC raises questions about the use of these technologies by law enforcement agencies in these countries, which are in the habit of hounding dissidents.

Milipol

France hosted the 18th *Milipol* »internal state security« fair from 19 to 22 November 2013. Held annually in either France or Qatar and offering both conventional weapons and digital technology, this trade fair brings together arms companies and potential buyers. A total of 161 official delegations from 97 countries attended the 2013 fair. They included 18 government ministers, of whom *Milipol* named only three. Senior officials from Bahrain (ranked 163rd out of 180 countries in the 2014 Reporters Without Borders press freedom index) rubbed shoulders with representatives from the ubiquitous Gamma International. Gamma's FinFisher software suite, one of the most effective and intrusive software tools available, is already being used by the Bahraini government to spy on human rights activists.

ISS World

ISS World (Intelligence Support Systems for Lawful Interception, Criminal Investigations and Intelligence Gathering) is an annual conference held in Dubai, Prague, Johannesburg, Brasilia, Washington or Kuala Lumpur. The right credentials are needed to attend. The official documentation says only the representatives of governments, law enforcement agencies and telecommunications service providers, and the vendors of interception, surveillance or network services are allowed to register. Journalists are not welcome.

The WikiLeaks »Spyfiles« on the 2012 ISS World revealed that it brought together 2,740 representatives of 1,507 different entities from 110 countries including Afghanistan, Bangladesh, Belarus, Iraq and Sudan. Gamma International was also there. WikiLeaks reported that Gamma's representatives have visited Kazakhstan (161st in the 2014 press freedom index) and Ethiopia (143rd). Both countries are on the 2014 list of Enemies of the Internet. Jerry Lucas, the CEO of *TeleStrategies*, the firm that launched ISS World, said the final use of the technology on show at the conference was not his concern.

»The surveillance that we display in our conferences, and discuss how to use, is available to any country in the world«, Lucas said. »Do some countries use this technology to suppress political statements? Yes, I would say that's probably fair to say. But who are the vendors to say that the technology is not being used for good as well as for what you would consider not so good? I mean, you can sell cars to Libyan rebels, and those cars and trucks are used as weapons. So should General Motors and Nissan wonder, ›how is this truck going to be used‹? Why don't you go after the automakers? It's an open market. You cannot stop the flow of surveillance equipment.«

Wassenaar Arrangement

The kinds of surveillance technology sold at these arms fairs and forums belong to the category of »dual-use« products and services covered by the Wassenaar Arrangement. The purpose of this multilateral agreement is to regulate the export of both conventional weapons and a long list of goods and technologies that can be used for both peaceful and hostile purposes.

In late 2013, the Wassenaar Arrangement's participating states agreed to add two categories to the list of controlled dual-use goods and technologies: „intrusion software« and »IP network surveillance systems«.

Participating states are supposed to control their exports of the listed dual-use goods and technologies, to exchange information about their exports and to exchange information about the legislation governing these exports that is in effect in their countries. But the Wassenaar Arrangement is not legally binding. Reporters Without Borders therefore urges the European Union to establish a more effective mechanism for controlling the exports of surveillance technologies.

RECOMMEN-DATIONS

Internet censorship and surveillance have a direct impact on fundamental rights. Online free expression facilitates a free debate on subjects of general interest. It also facilitates development, good government and the implementation of democratic guarantees. In a resolution adopted on 5 July 2012, the UN Human Rights Council said that the rights recognized in the physical world should also be recognized online regardless of frontiers. It called on governments to »promote and facilitate access to the Internet and international cooperation aimed at the development of media and information and communications facilities in all countries«.

In practice, surveillance of communications networks continues to grow. It allows governments to identify Internet users and their contacts, to read their email and to know where they are. In authoritarian countries, this surveillance results in the arrest and mistreatment of human rights defenders, journalists, netizens and other civil society representatives. The fight for human rights has spread to the Internet, and more and more dissidents are ending up in prison after their online communications are intercepted.

At the national and regional level, at the UN level, in the European Union and in most national legislation, the legal and regulatory framework governing Internet surveillance, protection of data and the export of ICT surveillance products is incomplete and inadequate, and falls far short of international human rights standards and norms. The adoption of a legal framework that protects online freedoms is essential, both as regards the overall issue of Internet surveillance and the particular problem of firms that export surveillance products.

Internet surveillance

RWB draws attention to

- the fact that the right to privacy is enshrined internationally in the Universal Declaration of Human Rights (article 12), The International Covenant on Civil and Political Rights (article 17), the European Convention on Human Rights (article 8) and the American Convention on Human Rights (article 11);
- the report on surveillance by the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, highlighting the impact of surveillance on human rights in general and freedom of information in particular;
- the 13 International Principles on the Application of Human Rights to Communications Surveillance, which were developed by Access, EFF and Privacy International with the help of a group of international experts. They aim to provide civil society, private enterprise and states with a framework for determining whether surveillance laws and practices respect human rights. These principles have received the support of more than 400 NGOs in some 70 countries.

RWB urges

the United Nations

- to consider creating a **working group on digital freedoms**, attached to the UN Human Rights Council, with the job of gathering all relevant information on digital freedoms, Internet surveillance, protection of privacy online, digital censorship, other forms of infringement of digital freedom in member states and individual cases of digital freedom violations, and making recommendations to member states.

the European Union

- to include unrestricted Internet access and to guarantee digital freedoms in the EU's Charter of Fundamental Rights;
- to incorporate the promotion and protection of digital freedom in all of the EU's external actions, policies and funding instruments, including both development and assistance programmes and Free Trade Agreement negotiations. And to condition development aid on respect for digital freedoms;

- to insist on the importance of freedom of Internet access and digital freedoms in the EU accession criteria (Copenhagen Criteria), and to reinforce monitoring of respect for these criteria;
- in relations between EU member states and with other countries, and in international bodies such as the WTO, to treat Internet surveillance mechanisms as protectionist and as barriers to trade and exchanges, and to combat them as such.

Governments

- to treat unrestricted Internet access and other digital freedoms as fundamental rights;
- to adopt laws guaranteeing digital freedoms, including the protection of privacy and personal data against intrusions by law enforcement and intelligence agencies, and to establish appropriate mechanisms of legal recourse;
- to ensure that communications surveillance measures strictly respect the principles of legality, need and proportionality, in line with article 19 of the International Covenant on Civil and Political Rights;
- to promote greater transparency as regards the surveillance requests they address to businesses, including their number, legal basis and objectives.

Business and human rights

Reporters Without Borders has repeatedly criticized the criminal level of cooperation between certain new technology companies and authoritarian regimes. These companies provide dictatorships with communications surveillance software that allows their law enforcement and intelligence agencies to spy on government opponents and dissidents and to imprison them. Worldwide, at least 167 netizens were in prison at the end of February 2014 in connection with their provision of news and information. The companies that collaborate with these governments must be penalized. Governments must enact legislation capable of controlling the export of ICT surveillance products and of penalizing the companies involved.

RWB draws attention to

- the UN Guiding Principles on Business and Human Rights, which the UN Human Rights Council approved unanimously in 2011;
- RWB's constant advocacy with the UN and individual governments on the subject of surveillance and its many statements on the subject, including its written submission o the second UN forum on »Business and human rights« in Geneva on 2-4 December 2013;
- RWB's November 2012 position paper on the export of European surveillance technology;
- its many press releases and statements on this subject since the start of the 2000s, in particular, its September 2011 statement: »Companies that cooperate with dictatorships must be sanctioned«;
- the reports of various bodies such as the UN Working Group on the issue of Human Rights and Transnational Corporations, especially its report of 14 March 2013, and a 24 October 2013 report by France's National Consultative Commission on Human Rights entitled »Business and Human Rights: an opinion on the challenges for France's implementation of the UN Guiding Principles«;
- RWB's participation in **The Cause** (Coalition Against Unlawful Surveillance Exports), an international coalition that includes Amnesty International, Human Rights Watch, Privacy International and Digitale Gesellschaft.

RWB urges

the United Nations

- to **reinforce the mandate of the UN Working Group** on the issue of Human Rights and Transnational Corporations, in particular, by giving it the ability to receive individual complaints and to investigate individual cases of alleged human rights violations involving businesses;
- to consider drafting an **international convention on the human rights responsibilities of businesses** that uses the UN Guiding Principles as its starting point and develops them;
- to consider drafting an **international convention on the export of Internet surveillance technology** in order to control these exports and the sales of other technology that endangers netizens and threatens their freedom. This convention would establish an independent monitoring body, dissuasive penalties and rules that allow the export of products to be banned when there is a significant danger of their being used to commit or facilitate grave human rights violations.

the states participating in the Wassenaar Arrangement for regulating the export of conventional weapons and dual-use goods and technologies

While welcoming the Wassenaar Arrangement's decision to add »intrusion software« and »IP network surveillance systems« to the list of controlled dual-use goods and technologies, RWB urges participating states:

- to promote more transparency and to give civil society and national human rights institutions (NHRIs) better access to the Wassenaar Arrangement's plenary assembly;
- to consider establishing binding regulations on the export and transfer of dual-use technologies to certain countries, regulations that would be uniformly binding on all participating states;
- to reinforces states' obligations, especially as regards monitoring exporters' compliance with the requirement to report exports.

the European Union

- to establish a more effective European-level mechanism for regulating surveillance technology exports;
- to treat certain systems and services used specifically for jamming, surveillance, control or interception as single-use products whose export should be subject to prior authorization;
- to harmonize and standardize the procedures and penalties used in monitoring and regulating surveillance technology.

National Governments

To control the exports of Internet surveillance products more strictly, especially their export to war zones and to states that do not respect fundamental freedoms.

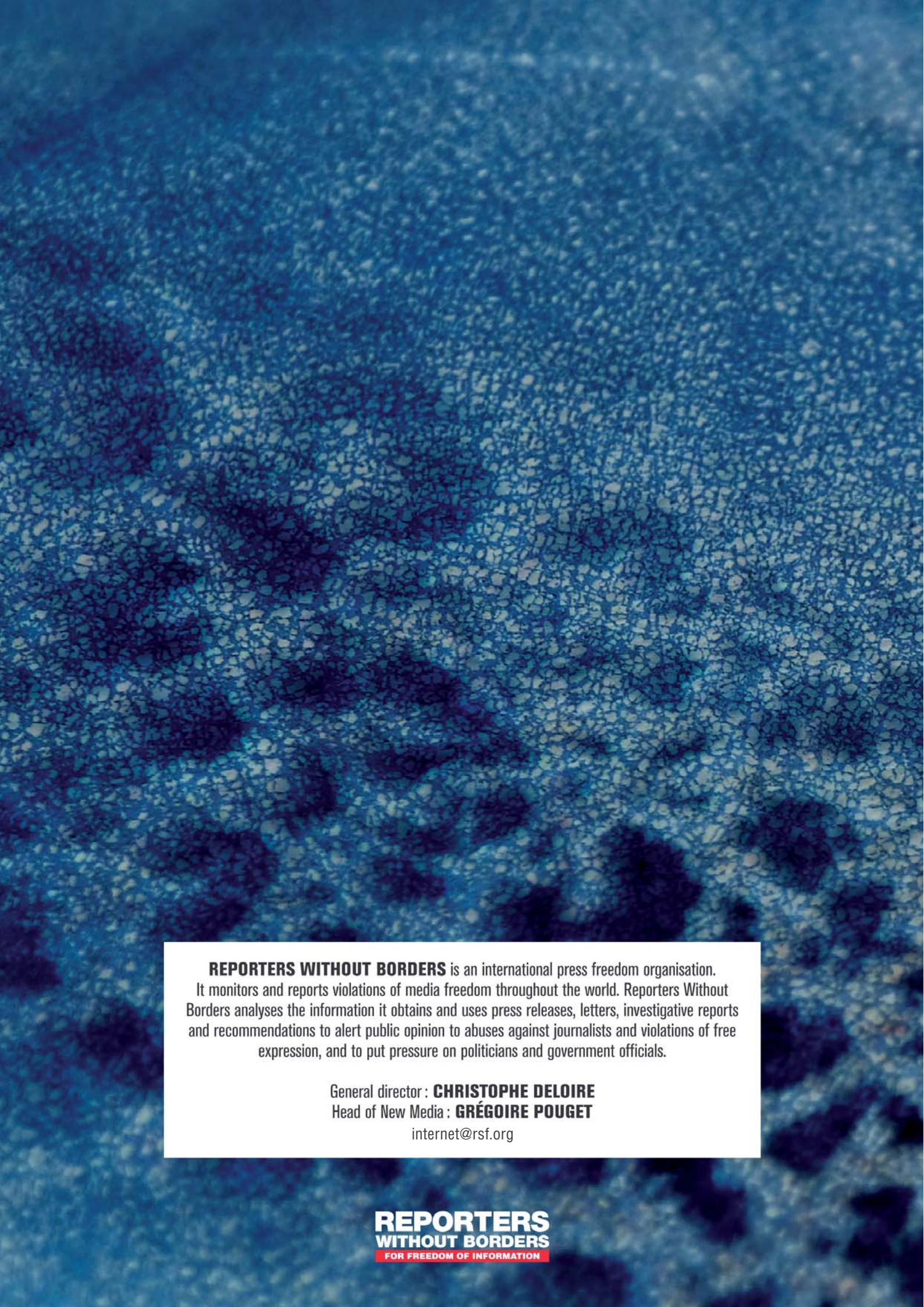
To amend current legislation and reinforce provisions for legal recourse in the following ways:

- by introducing legislative provisions on the criminal responsibility of businesses cooperating with regimes that violate human rights;
- by imposing a legal requirement on businesses to act with due diligence as regards respect for human rights;
- by ensuring that, as a result of this requirement, the state where a company has its headquarters is required to act as guarantor and to monitor the company's compliance with its international obligations;
- by introducing legislation that combats impunity and ensures the effectiveness of national judicial mechanisms by extending the exception to the principle of corporate autonomy to include human rights, so that companies can be held responsible for the actions of subsidiaries in other countries;
- by extending the international jurisdiction of national criminal courts so that they are competent to rule on crimes that a company has committed in another country.

Companies

To respect internationally recognized human rights.

- to adopt codes of ethical conduct and effective traceability mechanisms; and to establish mechanisms for informing personnel about human rights and increasing their awareness of human rights issues;
- to draft undertakings to respect the UN Guiding Principles and, in particular, to show due diligence as regards human rights and transparency;
- to envisage mechanisms for making reparations when their activities impact negatively on human rights.



REPORTERS WITHOUT BORDERS is an international press freedom organisation. It monitors and reports violations of media freedom throughout the world. Reporters Without Borders analyses the information it obtains and uses press releases, letters, investigative reports and recommendations to alert public opinion to abuses against journalists and violations of free expression, and to put pressure on politicians and government officials.

General director : **CHRISTOPHE DELOIRE**
Head of New Media : **GRÉGOIRE POUGET**
internet@rsf.org

REPORTERS
WITHOUT BORDERS
FOR FREEDOM OF INFORMATION