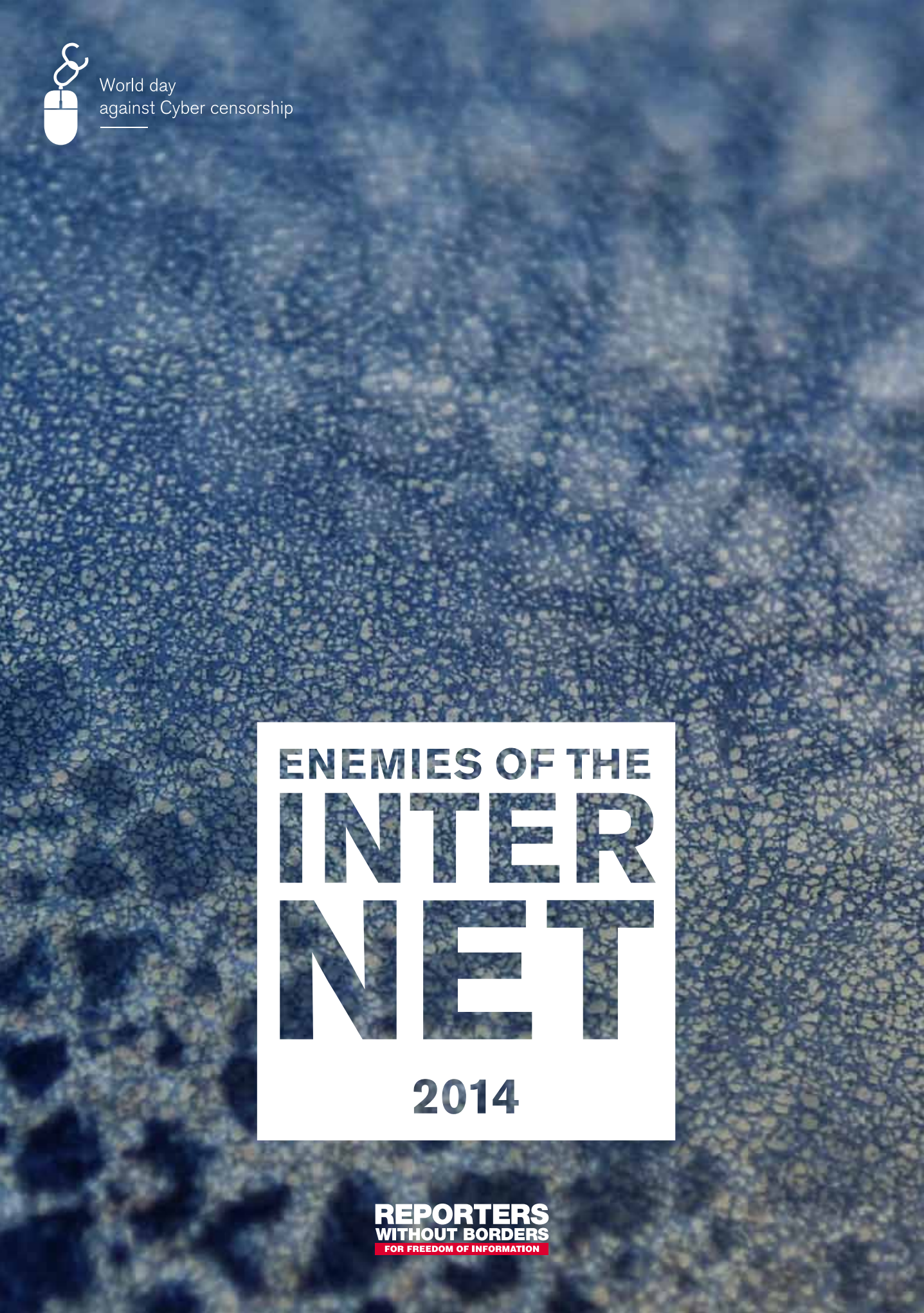
World day
against Cyber censorship
ENEMIES OF THE
INTER
NET
2014
REPORTERS
WITHOUT BORDERS
FOR FREEDOM OF INFORMATION

INSTITUTIONS THAT ARE ENEMIES OF THE INTERNET

12 March 2014

Get the full report at
12march.rsf.org

REPORTERS WITHOUT BORDERS
FOR FREEDOM OF INFORMATION

ENEMIES OF THE INTERNET 2014

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 they 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 be found in other agencies 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 Colombian (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 one 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.

RECOMMENDATIONS

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 360 NGOs in 70 countries and can be signed and supported on the thedaywefightback website.

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 of 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.

Head of Research Department
Lucie Morillon
lucie.morillon@rsf.org

Head of Africa Desk
Cléa Kahn-Sriber
afrique@rsf.org

Head of Asia Desk
Benjamin Ismaïl
asie@rsf.org

Head of Eastern Europe & Central Asia Desk
Johann Bihr
europe@rsf.org

Head of Middle-East & North Africa Desk
Soazig Dollet
moyen-orient@rsf.org

Head of Americas Desk
Camille Soulier
ameriques@rsf.org

Head of Afghanistan - Iran Desk
Reza Moini
persan@rsf.org

Head of European Union and Balkans Desk
Antoine Héry
ue@rsf.org

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

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

REPORTERS
WITHOUT BORDERS
FOR FREEDOM OF INFORMATION