United Nations A/HRC/23/NGO/7

General Assembly

Distr.: General
14 May 2013

English only

Human Rights Council
Twenty-third session
Agenda item 5
Human rights bodies and mechanisms

Written statement* submitted by Reporters Without Borders International, a non-governmental organization in special consultative status

The Secretary-General has received the following written statement which is circulated in accordance with Economic and Social Council resolution 1996/31.

[3 May 2013]

* This written statement is issued, unedited, in the language(s) received from the submitting non-governmental organization(s).

The UN guiding principles on business and human rights must be applied to digital mercenaries

Reporters Without Borders (RWB) is an international organization which for 28 years has been defending press freedom and media workers. Based in Paris, it relies on a network of more than 150 correspondents in 130 countries, on 10 country chapters and on local and regional partner organizations. For nearly 10 years, RWB has been involved in policy debates concerning the role of information-technology and digital media companies.

Since 2003, the organization has been sending questionnaires to Internet company executives concerning their censorship and surveillance practices in countries that restrict freedom of information. In 2006, the organization revealed the involvement of Yahoo! Hong Kong in the court conviction of Chinese journalist Shi Tao, sentenced to 10 years in prison for having sent information by e-mail concerning censorship of information about the Tienanmen Square massacre. The disclosure prompted widespread media coverage as well as U.S. congressional hearings. These eventually led Yahoo! to acknowledge its responsibility and to apologize to Shi Tao's mother. The U.S. Congress, as well as the European Parliament, then summoned major Web companies to testify concerning their practices in repressive countries.

Subsequently, several of these firms agreed to a code of conduct developed by the Global Network Initiative (GNI). Reporters Without Borders participated in negotiations leading to formulation of the code, along with companies, NGOs, investment funds and academic experts. RWB did not sign the code, but greeted the initiative as a step in the right direction, given that the firms in question acknowledged for the first time their responsibility to protect freedom of expression in the countries where they operate.

In 2011, Reporters Without Borders requested sanctions against companies that sell surveillance and communication interception technology to repressive governments. The export of dual-use technology underlines the importance of corporate social responsibility to Internet freedom. In keeping with this understanding, RWB has demanded export controls on surveillance technology to countries that flout human rights.

More recently, RWB has joined Privacy International, the European Center for Constitutional and Human Rights, the Bahrain Center for Human Rights and Bahrain Watch in filing a formal complaint with the Organization for Economic Co-operation and Development against a company that produces digital surveillance software.

Internet surveillance technology must be included in the agenda

Of the working group on business and human rights

Censorship and surveillance on the Internet affect the exercise of basic rights. Freedom of expression on the Internet facilitates free debate on subjects of general interest. In the words of Franck La Rue, special rapporteur to the UN Human Rights Council on the promotion and protection of the right to freedom of opinion and expression: "by acting as a catalyst for individuals to exercise their right to freedom of opinion and expression, the Internet also facilitates the realization of a range of other human rights."[1]

[1] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression A/HRC/17/27 - 16 May 2011 - § 22

Internet surveillance enables identification of Web users, of their contacts and locations, as well as the reading of their communications. In repressive countries, this results in the arrest and mistreatment of journalists, netizens and other human rights defenders.

In a special edition on surveillance, the annual Enemies of the Internet report by RWB names five "digital era mercenaries." These companies' products have been or are being used by repressive governments to violate human rights and freedom of information. For example, surveillance and interception products by the Trovicor firm allowed the royal family of Bahrain to spy on and arrest media workers. In Syria, DPI (Deep Packet Inspection) products developed by Blue Coat enabled the government to spy on dissidents and netizens throughout the country, leading to arrests and torture. Eagle products sold by the Amesys firm were found in secret police installations of the Muammar Gaddafi Government.

In his 2011 report concerning freedom of expression online, Mr. La Rue's recommendations are addressed not only to governments but also to companies when they emphasize responsibility[2]. Given the importance of the private sector in providing Internet services, he insists on the need to avoid involvement the human rights violations of governments[3].

The Forum on Business and Human Rights should provide an opportunity for the information technology sector to commit to the implementation of the UN Guiding Principles framework to 'Protect, Respect and Remedy' as endorsed by the Human Rights Council. on 16 June 2011.

Recommendations

Reporters Without Borders hopes that discussions in the Forum and the working group will lead to a thorough examination of the roles and obligations of all sectors involved.

1. To the states:

Regulations to protect human rights are urgently needed

Many countries, aware of the growing importance of cyber-security, have developed and exported surveillance technology with potential for other uses. While legitimate to combat cybercrime, it can become a formidable censorship weapon in the hands of authoritarian regimes. Failure to control commerce of these "digital weapons" allows authoritarian governments to identify media workers and netizens, and, as in Bahrain and Syria, to arrest and torture them.

- In keeping with Guiding Principle 3, states must create legislative and regulatory frameworks to control these companies' activities.

[2] "While States are the duty-bearers for human rights, private actors and business enterprises also have a responsibility to respect human rights." Ibid, § 45

[3] "Given that Internet services are run and maintained by private companies, the private sector has gained unprecedented influence over individuals' right to freedom of expression and access to information. Generally, companies have played an extremely positive role in facilitating the exercise of the right to freedom of opinion and expression. At the same time, given the pressure exerted upon them by States, coupled with the fact that their primary motive is to generate profit rather than to respect human rights, preventing the private sector from assisting or being complicit in human rights violations of States is essential to guarantee the right to freedom of expression.". ibid, f § 44

- States must regulate and monitor trade in surveillance products, including foreign activities as recommended in Guiding Principle 2: "States should set out clearly the expectation that all business enterprises domiciled in their territory and/or jurisdiction respect human rights throughout their operations."
- The European Union and the United States have prohibited the export of surveillance technology to Iran and Syria. While this action is commendable, it is insufficient. European governments must adopt a harmonized approach to control these exports. Likewise, the USA should adopt a policy along the lines of the Global Online Freedom Act. On 11 December 2012, the European Parliament endorsed the "Digital Freedom Strategy" proposed by Marietje Schaake, and it must become operational.
- States must ensure that repressive technologies be included in the Waassenaar Arrangement of July 1996. The accord is designed to promote "transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies. The Arrangement now has 41 participating states, including France, Germany, the United Kingdom and the United States.
- In all international bodies and forums whose mandate includes telecommunications and the Internet, states must reaffirm their commitment to uphold human rights and freedom of expression.
- Legal and non-judicial mechanisms must be put in place (see Principles 25 and 26) in order to enable action against companies involved in these activities.

2. To information technology companies:

Adopt and apply the guiding principles to research and commercial activities

- Principle 13 effectively requires that the companies make a fundamental shift in the way they operate. Ethical codes and export tracing mechanisms must be put in place.
- Companies should commit to the obligations derived from Principle 16 (adopt a human rights Policy); 17 (carry out human rights due diligence); 21 (provide transparency and accountability); 22 (provide remediation for adverse impacts); 29 (establish grievance mechanisms).
- When putting the Principles into effect, companies must consider the issue of the impact of their technology on human rights at every stage of work, starting with research and development.

3. To the forum and the working group:

Take a sector-specific approach and initiate inquiries

- In the framework of the second Forum, the issue of companies' responsibility for protecting Internet freedom must be addressed to pave the way for the implementation of the Guiding Principles by the information technology sector.
- The Working Group must take up this issue in its missions to various countries. For example, In the USA it is important to hear directly from the executives of American companies named by NGOs as having transferred surveillance technology.
- Victims of online surveillance should have access to the Working Group during its missions.

- Collaboration with Special Rapporteur Franck La Rue should be considered, to enable joint work on the issue of information technology companies' responsibilities.
- Finally, a declaration in favour of adoption of the Global Online Freedom Act is also recommended.