EUROPEAN PARLIAMENT

Federica Mogherini
High Representative of the European Union for Foreign Affairs and Security Policy and Vice-President of the European Commission

Brussels, 25th March 2015

Madam High Representative,

According to a Human Rights Watch Report publish on March 9 2014[1], Independent researchers at the Toronto-based research center Citizen Lab on March 9, 2015, reported new attempts by Ethiopia to hack into computers and accounts of Ethiopian Satellite Television (ESAT) employees based in the United States. The attacks bear similarities to earlier attempts to target Ethiopian journalists outside Ethiopia dating back to December 2013. ESAT is an independent, diaspora-run television and radio station used by Ethiopians to obtain news and analysis that is independent of the ruling Ethiopian People's Revolutionary Democratic Front. However, intrusive surveillance of these news organizations undermines their ability to protect sources and further restricts the media environment ahead of the elections scheduled for May 2015.

Citizen Lab's analysis suggests the attacks were carried out with spyware called Remote Control System (RCS) sold by the Italian firm Hacking Team, which sells surveillance and hacking technology. This spyware was allegedly used in previous attempts to infect computers of ESAT employees in December 2013. If successfully installed on a target's computer, the spyware would allow a government controlling the software access to activity on a computer or phone, including email, files, passwords typed into the device, contact lists, and audio and video from the device's microphone and camera.

Hacking Team previously told Human Rights Watch that "to maintain their confidentiality" the firm does not "confirm or deny the existence of any individual customer or their country location."[2] The firm has not reported on what, if any, investigation was undertaken in response to the March 2014 Human Rights Watch report, affirming that the use of its technology is "governed by the laws of the countries of our clients," and sales of its technology are regulated by the Italian Economics Ministry under the Wassenaar Arrangement, a multilateral export controls regime for dual-use technologies. The company further stated that it relies "on the International community to enforce its standards for human rights protection."

We would ask you, therefore, whether:

1. Have you or the Italian Government questioned the Italian company Hacking Team on whether it sold surveillance and spyware technology to the Ethiopian government, and if so, whether any safeguards were taken to prevent its misuse to further restrict media freedom?

[1] "They Know Everything We Do", Telecom and Internet Surveillance in Ethiopia, http://www.hrw.org/news/2015/03/08/ethiopia-digital-attacks-intensify.

[2] http://www.hrw.org/news/2015/03/08/ethiopia-digital-attacks-intensify.

EUROPEAN PARLIAMENT

2. Have you or any EU representative raised concern publicly or privately with the Ethiopian government over these practices of censorship and illegal surveillance?

3. Has the EU, as major aid donor, undertaken human rights due diligence on telecommunication projects in Ethiopia, to prevent directly or indirectly supporting violations of the rights to privacy or freedom of expression, association, or movement?

4. Which means does the Commission intend to put in place to regulate the export and trade of "dual use" surveillance and censorship technologies, requiring EU exporting companies to report on any human rights policies and due diligence activity to prevent rights abuses and remedy them if they arise?

Sincerely,

Ana Gomes (S&D)

Josef Weidenholzer (S&D)

Judith Sargentini (Greens/EFA)

Marietje Schaake (ALDE)