UPR Pre-Session Azerbaijan 2023

Access Now Statement

[Slide 1] My name is Natalia Krapiva, I am a Tech Legal Counsel at Access Now and today I will address the situation with digital rights in Azerbaijan and Azerbaijan's use of spyware in violation of human rights in particular.

[Slide 2] First, about my organization - Access Now is a human rights organization that defends and extends the digital rights of people and communities at risk.

By combining direct technical support, strategic advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

[Slide 3] Today, in my presentation I will 1) briefly discuss the Recommendations from the Previous Review; 2) Discuss Azerbaijan's unlawful use of spyware in violation of human rights; 3) and provide Recommendations

[Slide 4] We are not aware if Azerbaijan organized national consultations in preparation for the National Report. During the third UPR cycle, Azerbaijan received 265 recommendations, and at least 19 of them are related to digital rights, including:

- Protection of journalists, HRDs, and other civil society actors from harassment and persecution, online and offline

- Guarantee of the right to freedom of expression and freedom of assembly and association, online and offline

- Implementation of the the United Nations Guiding Principles on Business and Human Rights

[Slide 5] In 2021, Amnesty International's Pegasus Project identified over 1,000 Azerbaijani phone numbers selected for state surveillance with Pegasus spyware. Pegasus is a sophisticated spyware that allows an attacker to silently infect your mobile phone, capturing the entire content of your phone in real time, including calls, messages, pictures, turning on microphone and camera, and even changing your phone settings. The spyware is made by Israeli company NSO group, a notorious spyware developer that sells hacking techniques to governments.

At least 245 of these phone numbers belonged to Azerbaijani individuals who were identified as media workers, activists, HRDs, lawyers, opposition figures, business people, and academics. Amnesty International confirmed the phones of 5 individuals were infected, including RFE/RL

Azerbaijan journalists. Despite complaints, Azerbaijani authorities have not conducted an effective investigation into the matter.

[Slide 6] In May 2023, Access Now & partners documented Pegasus hacking of iPhones of 12 Armenian civil society actors in the context of Nagorno Karabakh war, including:

- Two RFE/RL Armenia journalists (covering the political crisis in Armenia caused by the war in Karabakh)
- Armenian Human Rights Ombudswoman (reporting alleged atrocities by Azerbaijani service members in Karabakh)
- Former Armenia MFA spokesperson (involved in the Nagorno Karabakh peacekeeping process with AM, AZ, US, RU, EU officials)
- Anonymous United Nations worker
- Activists, media workers, and a university professor

Citizen Lab found two operators of Pegasus spyware in Azerbaijan, targeting victims in Azerbaijan and Armenia

Despite wide international coverage and our demands for an independent investigation, no investigation has been launched by Azerbaijan government

[Slide 7]
Use of spyware threatens the right to privacy, freedom of expression and access to information, peaceful assembly, association, family life, health, education, work, and more. Individuals who would otherwise use their mobile device to obtain or transmit information, plan a peaceful gathering, communicate with family and friends, or share sensitive health, financial, or other information are discouraged from doing so by the mere threat that their government could be listening.

Use of spyware against civilians and humanitarian actors in armed conflict may violate international humanitarian law.

UNGA condemned unlawful or arbitrary surveillance and interception of communications as “highly intrusive acts” that interfere with human rights.

Calls for spyware moratorium by: SRs on FoE, FoA, racism & discrimination, extrajudicial killings, HRDs; High Commissioner for Human Rights; Costa Rica; Catalonia, and hundreds of NGOs & experts, including Access Now.

[Slide 8] Therefore, our Recommendations to the government of Azerbaijan are the following:

End surveillance, through the use of Pegasus hacking and similar software, of journalists, activists, lawyers, opposition figures, and HRDs at home and abroad;

Ensure prompt, impartial, and independent investigation into hacking allegations and hold individuals accountable for illegal surveillance; and

Fully cooperate with ECrHR, the UN, and all regional and international investigative bodies with respect to investigation of Pegasus hacking and other illegal surveillance