Access Now and EHRAC Joint Submission to the United Nations Human Rights Council on the Universal Periodic Review 44th Session Fourth Cycle for Azerbaijan

5 April 2023

About Access Now

Access Now is an international organisation that works to defend and extend the digital rights of individuals and communities at risk around the world. Through representation worldwide, Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the continued openness of the internet and the protection of fundamental rights. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions, and convenings such as RightsCon, we fight for human rights in the digital age. As an ECOSOC accredited organisation, Access Now routinely engages with the United Nations (UN) in support of our mission to extend and defend human rights in the digital age.[1]

About EHRAC

The European Human Rights Advocacy Centre (EHRAC) is an independent human rights centre that uses international legal mechanisms to challenge serious human rights abuses in Russia, Georgia, Azerbaijan, Armenia, and Ukraine, in partnership with committed local lawyers and NGOs. We aim to secure justice for victims of human rights violations and their families, and to bring about lasting systemic change in the region.[2]

Follow-up from Azerbaijan's third cycle

1. The Universal Periodic Review (UPR) is an important UN mechanism aimed at addressing human rights issues across the globe. Access Now and EHRAC welcome the opportunity to contribute to Azerbaijan's fourth review cycle. This submission examines Azerbaijan's use of Pegasus spyware technology in violation of the range of rights, including the rights to privacy, the right to freedom of expression, and the right to an effective remedy on and offline in Azerbaijan.

2. During the third UPR cycle, Azerbaijan received approximately 259 recommendations, supporting 152 and noting 101 recommendations.[3] Relevant recommendations regarding digital rights include, but are not limited to: 141.36, 141.37, 141.38, 141.40, 141.42, 141.43, 141.45,

[1] Access Now, available at https://www.accessnow.org/.
[2] EHRAC, available at https://ehrac.org.uk/en_gb/.
[3] UN Human Rights Council, Report of the Working Group on the Universal Periodic Review: Azerbaijan, UN Doc A/HRC/39/14, 11 July 2018.

141.46, 141.47, 141.49, 141.50, 141.53, 141.55, 141.57, 141.59, and 141.84.

Azerbaijan's international and domestic human rights obligations

3. Azerbaijan has signed the Universal Declaration of Human Rights (UDHR) and ratified the International Covenant on Civil and Political Rights (ICCPR), and the International Covenant on Economic, Social and Cultural Rights (ICESCR), among other international human rights instruments.

4. Azerbaijan's Constitution[4] contains several provisions which affirm the right to privacy, freedom of expression, freedom of peaceful assembly and association, and remedy on and offline throughout the country including, but not limited to:

    a. Article 24 states that "everyone has the right to freedom of thought and speech" and "no one shall be forced to proclaim or to repudiate his/her thoughts and beliefs;"

    b. Article 32 states that "everyone has the right to the inviolability of private life" and "the right for confidentiality of his/her private and family life;"

    c. Article 49 states that "everyone has the right to freely assemble together with others;"

    d. Article 58 ensures that "everyone is free to associate with others" and that "freedom of activity of all associations is guaranteed;"

    e. Article 60 ensures that "everyone is guaranteed protection of his/her rights and liberties through the administrative remedies and in court" and "may appeal against the actions and inaction of state bodies, political parties, legal entities, municipalities and their officials in administrative manner or in courts."

Pegasus phone hacking revelations

5. The submitting organisations are extremely concerned about the evident misuse by the government of Azerbaijan of a phone hacking product created by the Israeli surveillance company NSO Group. Known as "Pegasus," this spyware product can be secretly installed onto mobile phones and other devices often without the knowledge of the target and requiring no action from the user of the target device. For instance, it may not require clicking links, or opening software/apps. Once installed, it gives full access to the target phone, and gives complete control over the device. According to the NSO Group, the company only sells their product to states for the purpose of fighting terrorism and other serious crimes.[5]

6. Civil society organisations have been documenting the use of Pegasus against human rights defenders, journalists, lawyers, dissidents, and government critics around the world, from the

[4] President of the Republic of Azerbaijan Ilham Aliyev, The Constitution of the Republic of Azerbaijan, available at https://president.az/en/pages/view/azerbaijan/constitution.
[5] Le Monde, Pegasus Project: One year later, the twilight of NSO Group, , available at https://www.lemonde.fr/en/pixels/article/2022/07/19/pegasus-project-one-year-later-the-twilight-of-nso-group_5990692_13.html, 19 July 2022.

2016 Citizen Lab revelation of the hacking of Ahmed Mansoor,[6] to the targeting of the murdered jouranlist's Jamal Khashoggi's associates,[7] to the WhatsApp hacking scandal.[8]

7. In July 2021, a list of more than 50,000 phone numbers was shared with Amnesty International and Forbidden Stories, allegedly representing a list of "persons of interest" for targets of surveillance by NSO Group's customers. In response, a consortium of organisations, known as the "Pegasus Project," commenced a joint-journalistic investigation into this list. Organisations taking part in the investigation included *The Guardian* (UK), *Le Monde* and *Radio France* (France), *Die Zeit*, *Süddeutsche Zeitung*, *WDR* and *NDR* (Germany), *The Washington Post* and *Frontline* (USA), *Haaretz* (Israel), *Aristegui Noticias* and *Proceso* (Mexico), *Knack* and *Le Soir* (Belgium), *The Wire* (India), *Daraj* (Syria), *Direct* (Hungary) and OCCRP (Organized Crime and Corruption Reporting Project) (Serbia). [9]

8. On 18 July 2021, the Pegasus Project released the outcomes of its investigation. According to the consortium, the leaked list represents a list of those "selected for targeting" from clients of NSO Group, given the status of many of those whose numbers are on the list (including journalists, human rights defenders, and opposition figures), the timing of when the individuals were added to the list (some corresponding to real events such as elections or arrests), and most critically, that forensic analysis of a number of phones on the list showed that infection occurred within minutes of inclusion on the list.[10] The Pegasus Project list includes at least 180 journalists in 20 countries selected by at least 10 NSO clients.[11] The list itself does not prove whether a target's phone was actually hacked by Pegasus: this requires a forensic investigation of the phone itself. However, the July 2021 analysis by Amnesty International's Security Lab of 67 phones found that 23 phones were infected, and 14 showed signs of targeting. Many of these phones showed traces of Pegasus within minutes of being placed on the list.[12]

Pegasus in Azerbaijan

9. The available evidence strongly indicates that illegal surveillance has occurred through the use of Pegasus hacking software in Azerbaijan and that the authorities have not conducted an effective investigation into the matter.

[6] The Citizen Lab, The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender, available at https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/, 24 August 2016.
[7] See, e.g., The Citizen Lab, The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil, available at https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/, 1 October 2018.
[8] The Citizen Lab, NSO Group / Q Cyber Technologies: Over One Hundred New Abuse Cases, available at https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/, 29 October 2019.
[9] The Forbidden Stories, About the Pegasus Project, https://forbiddenstories.org/about-the-pegasus-project/, 2021.
[10] OCCRP, About the Project, available at https://www.occrp.org/en/the-pegasus-project/about-the-project#2-what-does-selected-for-targeting-mean-were-these-people-actually-hacked, 18 July 2021.
[11] Forbidden Stories, Pegasus: The New Global Weapon for Silencing Journalists, available at https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/, 18 July 2021.
[12] OCCRP, About the Project, available at https://www.occrp.org/en/the-pegasus-project/about-the-project, 18 July 2021.

10. The Pegasus Project identified more than 1,000 Azerbaijani numbers in the list. Of these, the Pegasus Project was able to link 245 of these to Azerbaijani individuals.[13] A fifth of these were reporters, editors, or media company owners. 40 Azerbaijani activists and their families are on the list.[14] Other persons identified on the list include human rights defenders, lawyers, opposition figures, businesspersons, and academics.[15]

11. To date, the government of Azerbaijan has not publicly admitted or denied using Pegasus spyware or spying on the persons contained in the list, and NSO Group does not disclose who its clients are. However, given the number of Azerbaijani phone numbers on the list (more than 1,000) and that a number of individuals on this list have had the infections on their phones forensically confirmed by Amnesty International's Amnesty Tech team, it is highly likely that the Azerbaijani government was a client of NSO Group and is behind the attacks.

12. A number of individuals who were on this list have complained to the Azerbaijani Prosecutor's Office requesting an investigation into the incident. However, in the instances where the Prosecutor has responded, the Prosecutor has passed the matter onto the State Security Services (SSS). The SSS does not have jurisdiction to investigate this matter, and is not independent as it was likely the very agency that conducted the surveillance in question. Thus, the complainants launched judicial review proceedings to bring the investigation back to the Prosecutor's office, which was unsuccessful. While some complainants have been asked to give statements to the SSS, the submitting organisations are not aware of any other further investigative steps undertaken by the Azerbaijani authorities.

13. Nine individuals, represented by EHRAC and individual Azerbaijani lawyers Emin Abbasov, Samed Rahimli and Shahla Humbatova, have filed complaints to the European Court of Human Rights (ECrHR), submitting that their rights to private life (Article 8 of the European Convention on Human Rights) and freedom of expression (Article 10, in case of three journalist victims) were violated; that they had no effective domestic remedies to challenge it (Article 13); and that their rights were violated with ulterior purpose as a means of repression for their activism and criticism (Article 18).

14. In addition, Media Defense, also submitted a case with the ECrHR on behalf of four Azerbaijani journalists - Sevinj Abbasova, Aynur Ganbarova, Natig Javadli, and Gular Mehdizade, alleging violations of their rights under Articles 6, 8, 10, 13, 17 and 18 of the European Convention on Human Rights.[16]

[13] OCCPR, Life in Azerbaijan's Digital Autocracy: 'They Want to be in Control of Everything," available at https://www.occrp.org/en/the-pegasus-project/life-in-azerbaijans-digital-autocracy-they-want-to-be-in-control-of-everything, 18 July 2021.
[14] Id.
[15] OCCPR, Who's on the List - The Pegasus Project: Azerbaijan, available at https://cdn.occrp.org/projects/project-p/?_gl=1*vv4hwz*_ga*ODYxNzg2ODg4LjE2MjY0NDA5MzM.*_ga_NHCZV5EYYY*MTYyNjYyNDYzNy41LjEuMTYyNjYyNTg2NS42MA..#/countries/AZ, 2021.
[16] Media Defence, Media Defence files four cases at the ECtHR concerning use of Pegasus spyware by the Azerbaijan government, available at https://www.mediadefence.org/news/pegasus-spyware-azerbaijan/, 3 October 2022.

Pegasus hacking violates human rights

15. The use of spyware, such as Pegasus, threatens a wide range of fundamental human rights protected by the International Bill of Human Rights, including the rights to information (ICCPR Article 19(2)), peaceful assembly (ICCPR Article 21), association (ICCPR Article 22), family life (ICCPR Article 12), health (ICESCR Article 12), education (ICESCR Article 13), and work (ICESCR Article 6). Individuals who would otherwise use their 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. But the rights most directly and severely restricted by spyware are the rights to privacy (ICCPR Article 17) and to opinions and freedom of expression (ICCPR Article 19).

16. The misuse of the Pegasus technology to hack mobile phones and conduct covert surveillance by the government of Azerbaijan flagrantly violates all of these rights. Evidence suggests that Azerbaijani authorities are using a highly intrusive and sophisticated hacking product with the aim of spying on journalists, human rights defenders, lawyers, and activists. There is no evidence that these intrusions were authorised by court orders, as explicitly required by the domestic law, and that there is no evidence that the targets have committed any criminal offences. Given this, the hacking and surveillance was illegal, does not serve a legitimate aim, is a disproportionate interference, and the legislative framework provides insufficient safeguards against this misuse.

17. The use of this surveillance technology not only violates the rights of its targets, it leads to a chilling effect amongst civil society, given that individuals are unable to freely communicate and associate with others over telecommunications equipment, as their device may be unknowingly hacked and they may be under illegal surveillance.

18. Additionally, Article 2 of the ICCPR requires states under their positive obligations to investigate harm caused by private individuals and entities.[17] The UN Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Human Rights Violations require a duty to "investigate violations effectively, promptly, thoroughly and impartially and, where appropriate, take action against those allegedly responsible in accordance with domestic and international law."[18] In Azerbaijan, the authorities have not conducted an effective investigation of the government use of Pegasus spyware, as little to no investigative activities have been undertaken and, in most cases, prosecutors have passed on the complaint to the State Security Services, which has no jurisdiction to investigate these complaints and was likely the body that conducted the illegal surveillance.

[17] UN General Assembly, Human Rights Committee, General Comment No. 31: The Nature of the General Legal Obligation Imposed on State Parties to the Covenant, UN Doc. CCPR/C/21/Rev.1/Add.13, para. 8, available at https://www.refworld.org/docid/478b26ae2.html, 26 May 2004.

[18] UN General Assembly, Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law, UN Doc. A/RES/60/147, Article 3(b), available at https://www.ohchr.org/en/instruments-mechanisms/instruments/basic-principles-and-guidelines-right-remedy-and-reparation, 21 March 2006.

19. There is no indication that the government of Azerbaijan has any intention to curb these surveillance abuses. On the contrary, the complete lack of accountability points to their continued proliferation.

Recommendations

20. We urge that the right to privacy and data protection, the right to freedom of expression, the right to freedom of peaceful assembly and association, and the right to effective remedy on and offline are prominent issues in the upcoming UPR review cycle. We therefore recommend that Azerbaijan:

    a. *Adhere to international human rights standards, and uphold its commitments to promote and protect the right to privacy and data protection, freedom of expression, freedom of peaceful assembly and association, and the right to effective remedy, on- and offline;*

    b. *End the practice of illegal covert surveillance, particularly through the use of Pegasus hacking software, to target and harass journalists, civil society activists, lawyers, opposition figures, and human rights defenders;*

    c. *Ensure prompt, impartial, and independent investigation into the allegations of hacking through the use of Pegasus software, and hold individuals accountable for such illegal surveillance; and*

    d. *Cooperate with UN and international investigative bodies, and issue standing invitations to UN Special Procedures, including the UN Special Rapporteurs on freedom of opinion and expression, freedom of peaceful assembly and association, and the right to privacy to visit the country.*

21. The UPR is an important UN process aimed to address human rights issues worldwide. It is a rare mechanism through which citizens around the world get to work with the government to improve human rights and hold them accountable to international law.

22. *For more information, please contact:* **un@accessnow.org** or **ehrac@mdx.ac.uk**.