AMNESTY INTERNATIONAL

-Check Against Delivery-

ORAL STATEMENT BY AMNESTY INTERNATIONAL

Index: AFR 01/5506/2022

71st Ordinary Session of the African Commission on Human and Peoples' Rights

Agenda Item 6(xiii): Activity report of the Special Rapporteur on human rights defenders and focal point on reprisals in Africa

Honourable Chairperson,

Amnesty International welcomes this opportunity to address the African Commission on Human and Peoples' Rights (African Commission) on the occasion of its 71st ordinary session.

Almost a year ago, as part of the Pegasus Project[1], media outlets, with the technical partnership of Amnesty International's Security Lab, revealed how Pegasus spyware produced by cyber-surveillance company NSO Group has been systematically used to facilitate human rights violations around the world on a massive scale. Amnesty International's Security Lab conducted forensic confirmations of the targeting and infections on the phones of scores of journalists, human rights defenders, and others around the world.

Based on this mounting evidence, it is abundantly clear that we are looking at a human rights crisis posed by the cyber-surveillance industry and states who misuse their tools. In particular, the scale and breadth of abuse facilitated by one of the industry's most prominent participants, NSO Group, and its state clients, is utterly out of control, destabilizing, and threatening to individuals' human rights, and the digital ecosystem as a whole. NSO Group is complicit in these human rights violations.[2]

In the African continent, the Pegasus Project revealed that **Togo, Rwanda, and Morocco** were potential clients of NSO Group.[3] Amnesty International and others have documented multiple instances of the unlawful targeted surveillance of journalists and civil society in all three countries. Aside from NSO Group's spyware, in 2021 we published on technology transfers from Israel of surveillance equipment to **South Sudan**, which was coupled with state-run physical surveillance and an atmosphere of fear and intimidation amongst civil society in the country.[4] In

[1] Amnesty International, 'Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally', June 2021, (Press Release)
[2] Amnesty International, Scale of secretive cyber surveillance 'an international human rights crisis' in which NSO Group is complicit, July 2021, (Press Release)
[3] Amnesty International, 'Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally', June 2021, (Press Release)/
[4] Amnesty International, 'South Sudan: "These walls have ears": The chilling effect of surveillance in South Sudan), February 2021 (AFR 65/3577/2021)

2021, Amnesty International also uncovered a separate targeted digital attack campaign against a human rights defender in **Togo.**[5]

These instances of surveillance have posed a serious threat to human rights protected under the African Charter on Human and Peoples' Rights, including the right to privacy, freedom of expression, freedom of association and peaceful assembly. Unlawful targeted surveillance has devastating consequences for those targeted, including to their physical safety and mental well-being. It also places their sources, colleagues, and loved ones in harm's way.

Many of those known to be targeted and/or infected by Pegasus have faced a history of repression at the hands of governments, including harassment, smear campaigns, and imprisonment. For women human rights defenders, the threat of surveillance is graver still. Information obtained through unlawful surveillance can be weaponized against them through smear campaigns, doxing, and other digital attacks. Even where the presence of surveillance cannot be proven, the mere suspicion that it exists causes civil society to self-censor, imposing a chilling effect on human rights work.

These examples we mention are only a tip of the iceberg and are not exhaustive. Due to the secrecy of the industry and state practice, there are likely to be numerous other instances of states deploying these tools in the African continent.

It is important to underscore that the problem is bigger than that of one bad actor. For years, the private surveillance industry has been allowed to operate unchecked. States have failed not only in their obligations to protect people from human rights violations, but have themselves failed in their own human rights obligations, clearly letting these invasive surveillance weapons loose on people worldwide for no other reason than exercising their human rights.

This is an unaccountable industry, and an unaccountable sphere of state practice, that must not continue to operate in their current forms.

Amnesty International therefore calls on the African Commission to urge state parties to the African Charter on Human and Peoples' Rights to:

1. Publicly support and implement an immediate moratorium on the export, sale, transfer and use of surveillance technology until robust human rights safeguards are in place.
2. Conduct an immediate, independent, transparent, and impartial investigations into cases of unlawful targeted surveillance.
3. Adopt and enforce a legal framework requiring private surveillance companies and their investors to conduct human rights due diligence in their global operations, supply chains and in relation to the end use of their products and services.
4. Disclose information about all previous, current and future contracts with private surveillance companies by responding to requests for information or by making proactive disclosures.

[5] Amnesty International, Togo: Hackers-for-hire in West Africa: Activist in Togo attacked with Indian-made spyware, October 2021 (AFR 57/4756/2021)

5. Implement domestic legislation that imposes safeguards against human rights violations and buses through digital surveillance and establishes accountability mechanisms designed to provide victims of surveillance abuses a pathway to remedy.

Amnesty International also calls on the African Commission to urge African National Human Rights Institutions to publicly support an immediate moratorium on the export, sale, transfer, and use of surveillance technology until robust human rights safeguards are in place and document instances of unlawful targeted surveillance by states.

Thank you.