European spyware investigators slam Israeli regime over sale of Pegasus

A logo adorns a wall on a branch of the Israeli NSO Group company near the town of Sapir, Aug. 24, 2021. (AP File Photo)

Warsaw, September 24 (RHC)-- The European Parliament, which is investigating the use of Israeli spyware by EU governments, has slammed the Tel Aviv regime for a lack of transparency in allowing the sale of Pegasus to European governments to use it against critics.

European lawmakers condemned the approach of the Polish government for refusing to meet and talk with them during the meeting of the fact-finding committee in Warsaw. “It is regrettable and we condemn the fact that the Polish authorities did not want to cooperate with our investigation committee,” Jeroen Lenaers, the head of the delegation, said at a news conference in Warsaw. “We think it also is a telling sign of the complete lack of importance this government attaches to checks and balances, to democratic scrutiny, and to dialog with elected representatives.”

The European Union's fact-finding committee is investigating the use of Israel's Pegasus spyware and other invasive surveillance tools by the European governments, saying the technology poses a serious threat to democracy in European countries.

Pegasus is Israeli spyware that was designed and developed by Israel's NSO group and is used to break into mobile phones and spy on a large part of personal information including text messages, passwords, locations, and microphone and camera receivers.

The Israeli company marketed this technology as a tool to target its desired targets in the world. Many European governments have used this controversial software to suppress dissidents, journalists, and political opponents around the world.

In Europe, some cyber detectives have found traces of the use of Pegasus or some other spyware in Poland, Hungary, Spain, and Greece.

Sophie in ’t Veld, the rapporteur of the inquiry, said the committee found out in its research that the NSO group sold this spyware to 14 European Union member states with official permission from Tel Aviv.

According to reports, Poland and Hungary are not allowed to buy this spyware from NSO due to some political issues, details of which remain unclear. “Why can we not say with certainty that Poland was one of the two countries of which the contract has been terminated?” she said. “Why is it that NSO is allowed to operate in the European Union, conduct its finances through Luxembourg, sell its products to now 12 member states, products that have been used to violate the rights of European citizens and to attack democracy of the European Union?”

Recently, Greece revealed that Nikos Androulakis, a member of the European Parliament and the head of the third largest political party in Greece, was monitored using Predator software last year when he was running for the leadership of the PASOK party. It is said that a journalist from Mali was also under surveillance.

Recently, it was revealed that Poland, Hungary, and some Catalan separatists in Spain were using this software to suppress their critics and opponents. The 10-member delegation of the EU's fact-finding committee during its trip that began on Monday met with Poles targeted by the Pegasus spyware, including a prosecutor and a senator, and some members of the opposition-controlled Senate.

A report of the obtained results as well as some recommendations and solutions are supposed to be published on November 8th of this year.

UN Secretary-General Antonio Guterres has warned of the threat posed by spying programs such as the Pegasus spyware to UN human rights activists in a report to be released next week. In recent days, Pegasus and some other spyware have threatened a group of UN human rights activists.

Guterres warned that the increase in digital surveillance by governments and some non-governmental sources has affected the activities of civil society activists in providing reliable information to the world body and has made them vulnerable to fear and threats of retaliation.

“United Nations actors have pointed to growing and concerning evidence of online surveillance, privacy intrusion, and cyberattacks by state and non-state actors of victims and civil society communications and activities,” the UN chief noted. “The lack of trust in the digital sphere among those sharing information and testimony with the United Nations on sensitive issues can discourage future cooperation.”

The findings are part of an annual report that tracks the challenges facing those seeking to work with the organization and focuses on April 2021 to May 2022. During this period, much of the UN's activities following the Covid-19 pandemic have gone digital, and at the same time, espionage threats have increased.

According to UN officials, this software has also spied on the activities of Palestinian, Bahraini, and Moroccan organizations and some human rights activists of the UN during this period. In his recent report, Guterres warned that in 2021, the mobile phones of employees of three prominent Palestinian NGOs - Addameer, Al-Haq, and Bisan Center for Research and Development - were hacked using Pegasus spyware.

The Israeli NSO Group has earned notoriety for trying to have its spy apparatuses maintain an edge over their international counterparts. The regime makes extensive use of Pegasus and other locally-made spyware for espionage.

According to observers, Tel Aviv has treated NSO as a de-facto arm of the regime, granting licenses for the sale of the spyware to countries to forge stronger security and diplomatic ties. In January, the New York Times reported that the FBI had purchased Pegasus software in 2019.

It also stated that in 2018 the CIA had purchased Pegasus for the government of Djibouti to conduct counterterrorism operations, despite that country’s record of torturing political opposition figures and imprisoning journalists.

---

https://www.radiohc.cu/en/noticias/internacionales/300194-european-spyware-investigators-slam-israeli-regime-over-sale-of-pegasus

Radio Habana Cuba