Nothing Sacred: Religious and Secular Voices for Reform in Togo Targeted with NSO Spyware - The Citizen Lab

By Authoritarianism, Violence & Surveillance in Togo

Archived: 2026-04-05 19:01:21 UTC

This Research Note identifies NSO Spyware targeting in Togo originating from the 2019 WhatsApp incident.

Key Points

- NSO spyware was used in 2019 to target Togolese civil society, including a Catholic bishop, priest, and opposition politicians.
- The targeting coincided with nationwide pro-reform protests which were forcibly dispersed, amidst violence and arrests.

Background

In May 2019, WhatsApp identified and shortly thereafter fixed a vulnerability that allowed attackers to inject NSO Group spyware onto phones with a missed WhatsApp video call. At least 1,400 WhatsApp users were targeted as part of this incident. WhatsApp attributes the attacks to NSO Group, an Israeli spyware developer.

The Citizen Lab volunteered to assist WhatsApp to investigate the 2019 Incident as part of the Citizen Lab's mandate to study digital threats against civil society. In the Fall of 2019 Citizen Lab's researchers reached out to more than 100 members of civil society among the targets to inform them of the attack and point them to resources to help them improve their digital security. On October 29th, 2019, WhatsApp sent messages to users targeted in the 2019 Incident. On the same day, WhatsApp filed a lawsuit against NSO Group in the United States.

NSO Spyware Attacks In Togo

During our investigation we identified multiple targets in Togo. These individuals were targeted between April and May, 2019. Four have now chosen to come forward. They include a bishop and a priest that have supported reform, as well as two members of Togo's political opposition. We believe the infection attempts would have led to the infection of most targeted devices with NSO's spyware.

Spyware Targets in the Catholic Church

Monseigneur Benoît Comlan Alowonou is the Bishop of Kpalimé, Togo. Bishop Alowonou is also the current president of the Conférence des Evêques du Togo ("Conference of Bishops in Togo"). The Catholic Church of Togo has been vocal in its support for human rights and democracy, and critical of abuses by the regime.

The Bishop has been the target of misinformation, and false reporting. For example, in 2015 he met with Pope Francis in Rome. During the *Ad Limina* visit, the Pope recognized the Togolese Bishops for their efforts for justice, peace and reconciliation, while cautioning about political entanglements. However, according to the Diocese, while the Bishop was in Rome it was falsely reported by a Togolese outlet that he had called on the opposition to "admit electoral defeat."

Father Pierre Marie-Chanel Affognon is a Togolese Catholic priest. He is the founder of a movement to promote constitutional, institutional, and electoral reform in Togo. Father Affognon describes his work as informing and encouraging Togolese citizens to hold their government to account. In the lead up to the 2020 elections, Father Affognon and other members of the campaign attempted to organize peaceful marches but their permits were denied by the government.

In 2018 and into 2019, Father Affognon was the target of a smear and disinformation campaign apparently intended to undermine his activities and those of the movement. Father Affognon speculates that the authors of this campaign may have had access to personal information only available on his phone.

Opposition Figures

Elliott Ohin is a prominent politician who has previously served in several senior cabinet roles, including Foreign Minister, and Minister for State Reform and Modernization. Ohin departed government in 2019. Ohin is also the former president of the opposition party *Union des Forces du Changement* ("Union of Forces for Change": UFC).

Raymond Houndjo was a mayoral candidate for the city of Lomé, and is currently a visible member of the opposition party *Alliance Nationale pour le Changement* ("National Alliance for Change": ANC).

Targeting Context

The targeting in April – May 2019 coincided with nationwide protests calling for presidential term limits. Planned demonstrations by the opposition Pan-African National Party (PNP) were largely banned by the government, which only permitted demonstrations in three cities. On April 13, 2019, protestors were violently dispersed by armed security forces, with one person killed and many others injured. Dozens of journalists, opposition leaders, and human rights defenders were detained. Detained in inhumane conditions, 19 were later sentenced to prison.

In May 2019, the National Assembly approved constitutional changes to reinstate presidential term limits in response to the protests. However, this restriction could not be applied retroactively, allowing President Gnassingbé (who has ruled Togo uninterrupted since 2005 after succeeding his father as President) to stay in

office until 2030. In addition to this, the amendments guarantee all former presidents immunity from prosecution for life "for acts committed during their presidential term."

In our 2018 *Hide and Seek* report, Citizen Lab identified a single Pegasus operator spying in Togo that we called REDLIONS. Because the operator appeared to be spying only in Togo, we suspected that REDLIONS was operated by an agency of the Togolese Government.

Two websites used by REDLIONS appeared to suggest politically motivated targeting, *nouveau-president[.]com* ("new president") and *politiques-infos[.]info* ("political information"), and four REDLIONS websites appeared to be designed to faciliate religiously focused targeting, including Christianity and Islam.

Religious-Themed Pegasus Domains Used By REDLIONS

chretiendaujoudhui[.]com ("Christian today")
viedechretien[.]org ("Christian life")
vie-en-islam[.]com ("life in Islam")
leprotestant[.]com ("the Protestant")

The first domains that we associated with REDLIONS were registered in January 2017, suggesting that the entity behind REDLIONS acquired the system prior to that point.

Togo has a history of authoritarian rule and serious human rights abuses. Faure Gnassingbé, Togo's President, has been in power since 2005. He succeeded his father, President Gnassingbé Eyadéma, who ruled Togo from 1967 until his death. Faure Gnassingbé has been re-elected four times, with each election deemed a sham by opposition members.

Over the past five decades the Gnassingbé family and their supporters have suppressed and modified democratic processes to ensure their hold on power. Mass protests have repeatedly sought electoral reform and his resignation, but are typically met with repression and violence. Togo remains one of the poorest countries of the world. It is ranked 167/189 in the 2019 United Nations Human Development Index.

Violence and Repression

The Gnassingbé government makes extensive use of force against opposition groups and human rights defenders, and its rule is marked by arbitrary detentions, torture, inhumane prison conditions, and killings by security forces. Legal and constitutional measures are regularly used to curtail rights to freedom of expression and peaceful assembly.

The 2020 Election

Ahead of the February 2020 national election, two opposition-friendly newspapers were suspended for two months for "discourteous, insulting and defamatory words." By election time, the primary election observation group was barred from monitoring the voting, as were monitors from the Catholic Church; the government claimed that these measures were taken to prevent interference. The election's results were met with accusations of extensive irregularities and voter fraud. The government placed the retired Archbishop of

Lomé under house arrest after he questioned the results. In July 2020, Togo's government issued an arrest warrant for the primary opposition candidate.

Digital Repression

The Togolese government uses technical means to curb dissent. Authorities have disrupted mobile phone and internet service during protests and on election days to suppress protest and to curtail press coverage. In June 2020, the Economic Community of West African States (ECOWAS) Community Court of Justice ruled that the nine-day internet shutdown in September 2017 by the Togolese government during anti-government protests was illegal. The Court ordered the government of Togo to pay compensation to the applicants, and enact safeguards to meet international human rights law.

In 2018, the National Assembly passed a cybersecurity law which includes provisions to criminalize the publication of "false" information, breaches of public morality, and "the production, diffusion or sharing of data which undermine 'order, public security or breach human dignity.'" Police are also granted greater authority to conduct electronic surveillance without adequate judicial oversight.

NSO Group & Abuses of Its Spyware

NSO Group is majority-owned by Novalpina Capital, a European private equity firm based in London. While NSO Group's spyware (often called "Pegasus") is marketed as used for crime fighting, there are over 130 cases in which NSO Group's hacking technology has been used to conduct abusive surveillance against civil society around the globe.

NSO Group claims it sells its spyware strictly to government clients and that all of its exports are undertaken in accordance with Israeli government export laws and oversight mechanisms. NSO Group also claims to abide by a human rights policy and governance framework. However, the number of documented cases in which their technology is used abusively to target civil society continues to grow. Most recently, Amnesty International confirmed in June 2020 that Pegasus was used to target a Moroccan journalist. That targeting took place just three days after NSO Group had implemented its new human rights policy.

For more information on NSO Group, a summary of key public reporting is here. The Business and Human Rights Resource Center's website for both NSO Group and Novalpina Capital has additional resources. Further, exhibits filed in the ongoing litigation between WhatsApp/Facebook and NSO Group in the United States provide insight into Pegasus' functions and NSO Group's operations (see, in particular, Exhibit 10 of the complaint).

What An NSO Spyware Infection Can Do

NSO's spyware product is most commonly known as Pegasus, however in specific cases it may be given different codenames. Pegasus is a mobile phone hacking tool that provides its operator complete access to a target's mobile device. Pegasus allows the operator to extract passwords, files, photos, web history, contacts, as well as identity data (such as information about the mobile device).

Pegasus can take screen captures, monitor user inputs and activate a telephone's microphone and camera. These features enable attackers to monitor all activity on the device and in the vicinity of the device, such as conversations conducted in a room.

Pegasus also allows the operator to record chat messages (including messages sent through some "encrypted" texting apps), as well as regular phone and encrypted VoIP calls.

Pegasus also allows the operator to track the target's location. As with any infection, spyware may also allow for the modification or manipulation of data on a device.

A Global List of Abuses

Pegasus has been linked to at least 130 cases of abusive targeting of human rights defenders and journalists in dozens of countries in Asia, Europe, the Middle East, and North America. Research groups, including Amnesty International, have identified additional cases.

Canada & Europe

In Canada and Europe, targets include critics of the Saudi government, and specifically individuals who believe that they were targeted as part of the surveillance of Jamal Khashoggi just prior to his murder. Other targets include the staff of international human rights organizations. In addition, a number of individuals critical of president Paul Kagame were targeted in Europe and Africa.

Mexico

In Mexico, at least 25 members of civil society were targeted, ranging from prominent journalists and critics of then-President Enrique Peña Nieto, like Carmen Aristegui, to the President of Mexico's Senate, anti-corruption organizations, such as Mexicanos Contra la Corrupción y la Impunidad, and public health officials. Troublingly, several targets working in media were targeted shortly after their colleague was assassinated in a cartel-linked killing. The wife of the slain journalist, a reporter herself, was also targeted.

Middle East & North Africa

Government critics and human rights defenders in Gulf countries, as well as journalists and other pro-reform voices in Morocco are among those targeted.

India

In India, at least two dozen lawyers, journalists, and other members of civil society, including defenders of ethnic and cultural minorities, were extensively targeted with NSO spyware.

Acknowledgements

We thank the many targets of NSO Spyware, including those mentioned in this report, who continue to come forward. Their courageous choice not to stay silent in the face of digital attacks makes such investigations

possible.

Thanks to Citizen Lab staff for additional logistical assistance with this investigation.
