John Scott-Railton **@jsrailton** *Sun Jul 18 16:11:54 +0000 2021*

BREAKING: massive, global leak of the targets of NSO Group's Pegasus spyware. *huge deal.*

Forensic investigation by **@AmnestyTech**
in collaboration with **@FbdnStories** reporters.

We **@citizenlab** conducted peer review.

Here's an explainer THREAD.
https://t.co/TasFCy5EGW https://t.co/rGGKAkfSry

2. Background: the already-notorious NSO Group makes mercenary spyware to silently & remotely hack iPhones & Androids.

Many of their government customers are authoritarians.

Most cannot resist the temptation to target their critics, reporters, human rights groups etc. **https://t.co/97oHA6fsV9**

3. More about leaked numbers & targets in a sec, but first you need to know:

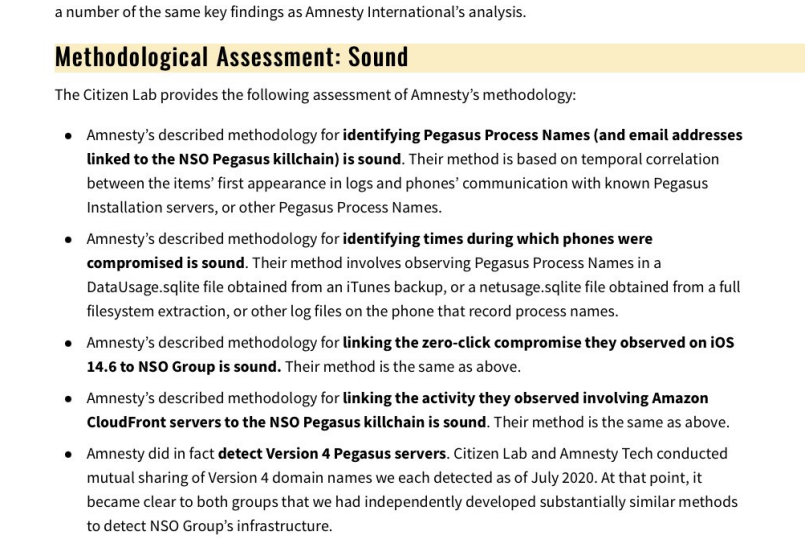
@AmnestyTech just released a report with technical analysis of NSO's infrastructure... & analysis validating w/forensics that some phones were infected with Pegasus.

https://t.co/WCl5rDvpv7

4. We @citizenlab independently peer reviewed @AmnestyTech's forensic methodology, including how they identify an infected phone.

Our review, led by my colleague @billmarczak, judged their forensics & research methodology to be SOUND.

https://t.co/YTTqFdx7AI https://t.co/d8whUyioEJ



a number of the same key findings as Amnesty International's analysis.

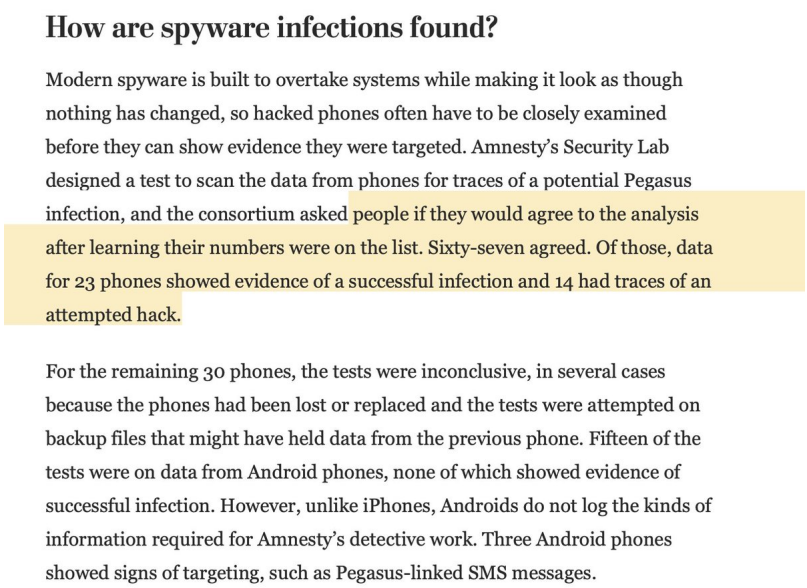
Methodological Assessment: Sound

The Citizen Lab provides the following assessment of Amnesty's methodology:

- Amnesty's described methodology for **identifying Pegasus Process Names (and email addresses linked to the NSO Pegasus killchain) is sound**. Their method is based on temporal correlation between the items' first appearance in logs and phones' communication with known Pegasus Installation servers, or other Pegasus Process Names.
- Amnesty's described methodology for **identifying times during which phones were compromised is sound**. Their method involves observing Pegasus Process Names in a DataUsage.sqlite file obtained from an iTunes backup, or a netusage.sqlite file obtained from a full filesystem extraction, or other log files on the phone that record process names.
- Amnesty's described methodology for **linking the zero-click compromise they observed on iOS 14.6 to NSO Group is sound.** Their method is the same as above.
- Amnesty's described methodology for **linking the activity they observed involving Amazon CloudFront servers to the NSO Pegasus killchain is sound**. Their method is the same as above.
- Amnesty did in fact **detect Version 4 Pegasus servers**. Citizen Lab and Amnesty Tech conducted mutual sharing of Version 4 domain names we each detected as of July 2020. At that point, it became clear to both groups that we had independently developed substantially similar methods to detect NSO Group's infrastructure.

5. Now, to the findings: >50k numbers were leaked that are reportedly part of the infection & targeting workflow with Pegasus.

To help validate the relationship between these numbers & infections @AmnestyTech got consent to forensically examine a subset of the devices. **https://t.co/Vd2rMz2ARf**



How are spyware infections found?

Modern spyware is built to overtake systems while making it look as though nothing has changed, so hacked phones often have to be closely examined before they can show evidence they were targeted. Amnesty's Security Lab designed a test to scan the data from phones for traces of a potential Pegasus infection, and the consortium asked people if they would agree to the analysis after learning their numbers were on the list. Sixty-seven agreed. Of those, data for 23 phones showed evidence of a successful infection and 14 had traces of an attempted hack.

For the remaining 30 phones, the tests were inconclusive, in several cases because the phones had been lost or replaced and the tests were attempted on backup files that might have held data from the previous phone. Fifteen of the tests were on data from Android phones, none of which showed evidence of successful infection. However, unlike iPhones, Androids do not log the kinds of information required for Amnesty's detective work. Three Android phones showed signs of targeting, such as Pegasus-linked SMS messages.

6. The @FbdnStories consortium worked w/the leaked phone numbers... what they found reveals 10 of NSO Group's customers insatiable intent to snoop.

And the massive scale of the operation.

- Mexico customer > 15,000
- Morocco > 10,000
- UAE > 10,00

Etc. **https://t.co/MPxtS9ihW3**

The consortium's analysis of the leaked data identified at least 10 governments believed to be NSO customers who were entering numbers into a system: Azerbaijan, Bahrain, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, Hungary, India, and the United Arab Emirates (UAE).

Analysis of the data suggests the NSO client country that selected the most numbers - more than 15,000 - was Mexico, where multiple different government agencies are known to have bought Pegasus. Both Morocco and the UAE selected more than 10,000 numbers, according to the analysis suggested.

The phone numbers which were selected, possibly ahead of a surveillance attack, spanned more than 45 countries across four continents. There were more than 1,000 numbers in European countries that, the analysis indicated, were selected by NSO clients.

7. #SaudiArabia ■■ murdered & dismembered Jamal Khashoggi.

Jamal's wife was targeted with Pegasus spyware before the killing...

Then his fiancee was hacked multiple times just days after.

@citizenlab independently confirmed findings.

#PegasusProject
https://t.co/FYcDwr7rAn https://t.co/MfSDEc3Nj2

The Android phone of his wife, Hanan Elatr, was targeted by a Pegasus user six months before his killing, but the analysis could not determine whether the hack was successful. The iPhone of his fiancee, Hatice Cengiz, was penetrated by spyware days after the murder, the forensics showed.

When Cengiz was told of the breach in an interview in Istanbul, she replied: "I was expecting that, but I am upset. I want to be a normal person, as anyone. All these things make me sad and scared. My phone could be attacked again in the future, and I feel I don't have any way to protect myself from this."

Whether Khashoggi's cellphone was also hacked is not known. He left his phone with Cengiz when he entered the consulate. She gave it to Turkish authorities. Authorities have kept it and have declined to say whether it had been hacked, citing the ongoing homicide investigation.

Agnès Callamard, the former United Nations rapporteur who investigated the murder and is now secretary general of Amnesty International, said the use of Pegasus against Khashoggi's inner circle and investigators "indicates an attempt to be on top of what may be revealed [by the Turkish investigation]."

8. #HUNGARY ■■

Ask the government for comment... get hacked.

Hungary's far-right PM Viktor Orbán is using Pegasus spyware to surveil & attack Hungary's independent media, like @direkt36, @panyiszabolcs, and many more.

Story: @shaunwalker7 **https://t.co/FuXWoylRul https://t.co/yM1KHbjRej**

intelligence. One day later, Panyi's phone was infected with Pegasus.

There were 11 occasions when a Pegasus infection was confirmed within a few days of a comment request from Panyi to the government, according to Amnesty's analysis.

More than half the comment requests he sent to various government offices during a seven-month period were followed up with an attack. The tactic, he assumes, was for the government to get ahead of the story,

Another Hungarian journalist selected as a candidate for possible surveillance was Dávid Dercsényi, who edits a newspaper put out by the authority of Budapest's opposition-run eighth district and previously worked for five years for the website of the independent outlet HVG.

Three numbers linked to Dercsényi, including one belonging to his ex-wife that had been registered in his name, were found in the data.

Over wine and finger food on Varga's expansive terrace, the men discussed creating a new foundation that among other things would investigate and expose corruption among Hungary's ruling elite. "It was a friendly conversation, it wasn't a coup," said Varga.

Two weeks later he met a government-linked acquaintance for coffee and she demonstratively referenced the dinner, suggesting such meetings could be "dangerous" for him. Varga suspected Orbán's circle had somehow put the meeting under surveillance.

Indeed, the records show all seven people at the dinner were selected as potential candidates for surveillance. Forensic analysis carried out on the handset of one of those present showed clear evidence of a confirmed infection at the time of the dinner. The phone of another participant showed signs of Pegasus activity but not of compromise.

9. #INDIA■■ Over 40 reporters, major opposition figures, serving ministers in the #Modi government, members of the security services and beyond are in the list.

Story to watch as the scandal unfolds there.

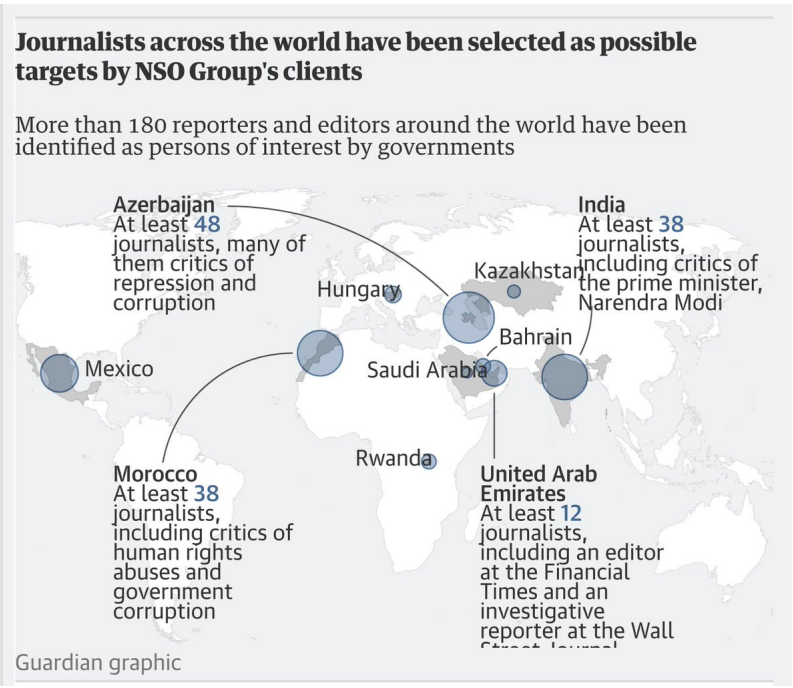
Story @svaradarajan @thewire_in
https://t.co/te9Fqwop38 https://t.co/Zutt1pia8l

The numbers of those in the database include over 40 journalists, three major opposition figures, one constitutional authority, two serving ministers in the Narendra Modi government, current and former heads and officials of security organisations and scores of businesspersons.

10. HUNDREDS of journalists around the globe are on the #PegasusProject list.

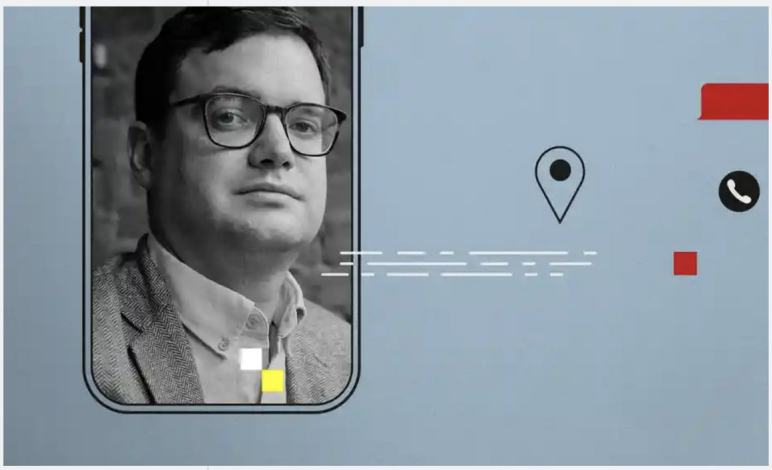
NSO Group's role in fueling the authoritarian assault on democratic values (like a free press) is coming into sharp focus

https://t.co/Akfdzw9MCX https://t.co/PQqKgq83lH



Other journalists who were selected as possible candidates for surveillance by NSO's clients work for some of the world's most prestigious media organisations. They include the Wall Street Journal, CNN, the New York Times, Al Jazeera, France 24, Radio Free Europe, Mediapart, El País, Associated Press, Le Monde, Bloomberg, Agence France-Presse, the Economist, Reuters and Voice of America.

Bradley Hope: 'Your phone is a potential surveillance device'



▲Investigative journalist Bradley Hope. Composite: David Levene/Guardian

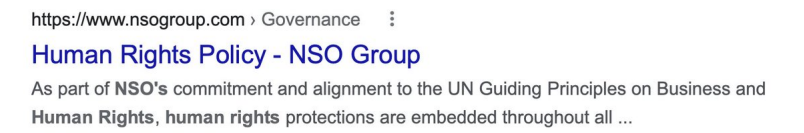
Also listed in the leaked records is a UK phone number belonging to the American investigative journalist Bradley Hope, who lives in London. At the time of his selection he was an employee at the Wall Street Journal.

11. NSO Group puts up a facade of caring about human rights, doing due diligence, etc.

This leak exposes the farce of that performance.

When your customers are dictators... they will do bad things. NSO knows this. We know it.

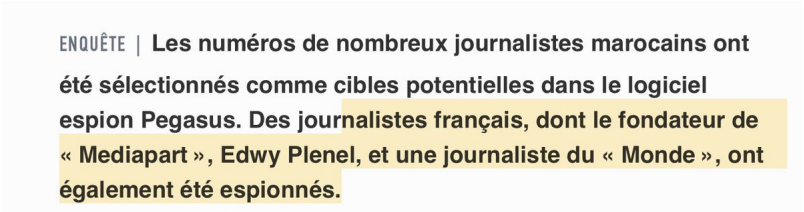
Now everybody knows it. **https://t.co/zapMzJvrUK**



12. Continuing with cases.... in #FRANCE ■■

#PegasusProject list includes @edwyplenel, founder of independent news site @Mediapart, a reporter from @lemondefr, etc..

Story **https://t.co/695Gxl0eqL https://t.co/5AY3U8axaJ**



13. in #Mexico ■■ Journalist Cecilio Pineda Birto was getting death threats for reporting on official collusion with a cartel capo...

...then his number showed up on the #PegasusProject list.

Then he was assassinated.
https://t.co/AB49bJZ12z https://t.co/LKRCJSutCk

On 2 March 2017, Cecilio Pineda Birto made a broadcast about alleged corruption. Hours later he was dead

The hitmen came for Cecilio Pineda Birto as he swung in a hammock at a carwash, waiting for his pickup to be cleaned.

The 38-year-old freelance reporter was shot dead on 2 March 2017 in Ciudad Altamirano, a town in the southern Mexican region of Tierra Caliente - a battleground for rival organised crime factions.

A few hours earlier, Pineda had in a broadcast on Facebook Live accused state police and local politicians of colluding with a violent local capo known as El Tequilero.

In previous weeks, Pineda had received a string of anonymous death threats. At about the same time, his mobile phone number was selected as a possible target for surveillance by a Mexican client of the spyware company NSO Group.

▲ The carwash where Pineda was shot dead on 2 March 2017.

While the leak reveals phones that were selected as possible targets by NSO's government clients, it is not possible to say whether phones were successfully infected with spyware without forensic analysis of a device.

> Pineda frequently changed numbers because he feared his could be compromised, according to his colleagues and family. At one point, the transcript of a conversation between Pineda, a colleague and a source was published in a national newspaper.
>
> 
>
> ▲Pineda with his friend Agustín Hernández, right.

14. Bookmark this thread. Things are only getting started.

I'll be updating it with more cases & context as #PegasusProject revelations keep dropping.

15. REASON TO CARE #1

So, you didn't know today's #PegasusProject hacking victims personally.

But tomorrow? Who knows. You don't.

#NSOGROUP is aggressively pitching *local* cops, including in USA ■■

Pause. Think about the oversight at your local PD.

https://t.co/xSr7EEDLMZ https://t.co/gAOe9oU4zi

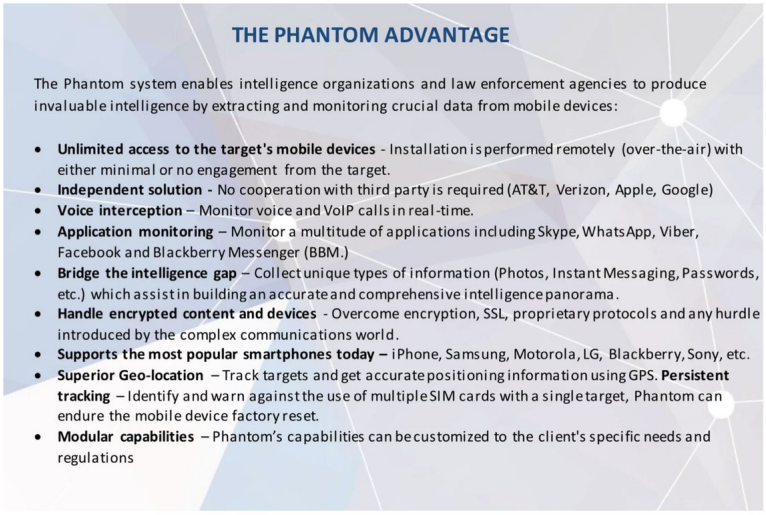
> In August 2016, a Westbridge employee emailed the San Diego Police Department (SDPD) offering more information on Phantom, "a mobile intelligence system that would be a great addition to your investigative and special support offices." After remotely hacking the phone, Phantom can siphon a target's emails, text messages, and contact list, as well track their location, turn on the device's microphone and take photos with its camera, according to the brochure.
>
> "I would like to thank you again for the product demo you put on for us at LAPD headquarters," Detective Mark Castillo, from the technical support unit of the LAPD's major crimes division, wrote to Westbridge, NSO's U.S.-arm, in a June 2016 email. Motherboard obtained the emails through a public records act request.

I would like to thank you again for the product demo you put on for us at LAPD headquarters. If you have any additional info regarding Landmark, phantom and hook I would like to go over it with my crew. Also, if my command allows, I would like to set up another demo with just my team.

Thanks again.

Detective Mark Castillo
Office: [redacted]
Cell: [redacted]
FAX: [redacted]
LAPD Major Crimes Division
Technical Support Unit
100 West First Street, 9th Fl
Los Angeles CA 90012

A SCREENSHOT OF AN EMAIL FROM THE LAPD TO WESTBRIDGE. IMAGE: MOTHERBOARD



A SECTION OF THE WESTBRIDGE BROCHURE. IMAGE: MOTHERBOARD

16. REASON TO CARE #2:

Since all phones are vulnerable, #Pegasus spyware lets its autocrat-users *export fear*

They want want *you* to be afraid to criticize them.

Yes, you. A continent away. In a democracy.

Think about the implications.

7. REASON TO CARE #3:

Think only human rights defenders & journalists get hacked with #Pegasus?

Wrong.

Good chance officials responsible for the national security of YOUR country have been / will be targeted.

Example pic: 2019 #NSOGroup WhatsApp hack.
https://t.co/0XYGbL07WD https://t.co/5oExzzxX6N

Sources familiar with WhatsApp's internal investigation into the breach said a "significant" portion of the known victims are high-profile government and military officials spread across at least 20 countries on five continents. Many of the nations are U.S. allies, they said.

18. Know who else is saying #NSOGroup must be stopped?

Big tech.

These days they are hitting back hard against the mercenary spyware industry for hacking their products & users.

E.g. this thread by @wcathcart @WhatsApp's CEO.■
https://t.co/dyjZREqRmK
19. #INDIA■■ (2/)

She accused the Chief Justice of India's Supreme Court of sexual harassment.

Just days later:

Her phone. Her husband's phone. Their family members..

11 in total then showed up on the #PegasusProject list.

https://t.co/hi2gXVmqHp https://t.co/kNUxrrNwo2

> In other words, the legal strategy of a woman who said she was sexually harassed by India's top judge would have been known to whichever individual or agency was interested in surveilling her, placing them in a powerful position vis a vis not just the woman but,

Former CJI Ranjan Gogoi. Photo: PTI

> The leaked records show that eight other phone numbers belonging to her husband and two of his brothers were also marked as possible candidates for surveillance in the same week, when her allegations against the CJI were first reported.

20. #FRANCE ■■ Claude Mangin is campaigning for the release of her husband, a political activist, from a #moroccan prison.

She's in France.

Last month her iPhone 11 was silently hacked w/#Pegasus spyware. A second iPhone she borrowed? Also infected.
https://t.co/4LkbwnZ8Iq https://t.co/ri8aCpa392

Claude Mangin, shown at her home in suburban Paris, has been waging an international campaign to win the freedom of her husband, political activist Naama Asfari, who has been jailed in Morocco for more than a decade. Her iPhone 11 was hacked last month with Pegasus spyware. (Guillaume Herbaut/Agence VU for The Washington Post)

The text delivered last month to the iPhone 11 of Claude Mangin, the French wife of a political activist jailed in Morocco, made no sound. It produced no image. It offered no warning of any kind as an iMessage from somebody she didn't know delivered malware directly onto her phone — and past Apple's security systems.

> For years, Mangin has been waging an international campaign to win freedom for her husband, activist Naama Asfari, a member of the Sahrawi ethnic group and advocate of independence for the Western Sahara who was jailed in 2010 and allegedly tortured by Moroccan police, drawing an international outcry and condemnation from the United Nations.
>
> "When I was in Morocco, I knew policemen were following me everywhere," Mangin said in a video interview conducted in early July from her home in suburban Paris. "I never imagined this could be possible in France."
>
> Especially not through the Apple products that she believed would make her safe from spying, she said. The same week she sat for an interview about the hacking of her iPhone 11, a second smartphone she had borrowed — an iPhone 6s — also was infected with Pegasus, a later examination showed.

21. BREAKING: Americans ■■ including US. Gov. officials are on the #PegasusProject list...

...even the #Biden administration's lead Iran negotiator Robert Malley!

#NSOGroup is an urgent national security problem for the United States.
https://t.co/PDpKXWgoQq https://t.co/JxANkfcTGy

A list of more than 50,000 phone numbers that included some for documented surveillance targets also included the overseas phone numbers for about a dozen Americans, including journalists, aid workers, diplomats and others, according to an investigation by The W[redacted]shington Post and 16 other news organizations.

US OFFICIALS, JOURNALISTS, AID WORKERS

The investigation was unable to determine whether clients of NSO had delivered or attempted to deliver its Pegasus spyware to any of these numbers. But the presence of numbers used by American officials on the list highlighted questions about the national security threat posed by commercially available spyware.

CHIEF IRAN DEAL NEGOTIATOR!

In addition to the overseas phone numbers, the Washington-area cellphone number for the Biden administration's lead Iran negotiator, Robert Malley, appeared on the list, as did those of several United Nations diplomats based in the United States and Rwandan expatriates who oppose the government of President Paul Kagame and are living in exile here.

22. #MEXICO ■■: At least *50 people* close to the president ... are on the #PegasusProject spyware list.

They were put there while he was campaigning.

-His wife
-Family members, drivers, doctor
-Aides, chief of staff
-Doctor...

#PegasusProject
Story **https://t.co/bYasa114WO https://t.co/2YgzlvFJHt**

▲Andrés Manuel López Obrador and his wife, Beatriz Gutiérrez Müller. Photograph: Hector Vivas/Getty Images

As Amlo crisscrossed the country campaigning, however, NSO's Mexican clients selected almost everyone in his inner circle as persons of interest - including his wife, three sons, three brothers and two former chauffeurs, according to analysis of the leaked data. Amlo rarely used his own phone, relying instead on those of his assistant and communications chief - both of which were selected. His chief of staff, Alfonso Romo, his legal counsel, Julio Scherer Ibarra, and his communications coordinator, Jesús Ramírez Cuevas, were also selected.

Even the manager of the amateur baseball team Amlo plays in was selected - as was his cardiologist, Patricio Heriberto Ortíz Fernández.

Amlo had surgery in 2013 following a heart attack at the age of 60, after which his health became the subject of press speculation casting doubt over his ability to govern. "The only target was the candidate; I was a tool," said Ortíz, who added that he never discussed Amlo's health on the phone. "I think it's very serious, but it was the way things were going on in the country. Unfortunately, I'm not surprised."

23. Paul Rusesabagina inspired Hotel #Rwanda ■■

He's become a critic of the gov., and was recently thrown in jail.

His American ■■ daughter, while advocating for his release, has been incessantly surveilled w/ #Pegasus.

#PegasusProject

By @skirchy **https://t.co/3nQb2B6aIa https://t.co/7hyuGea5wM**

The American daughter of Paul Rusesabagina, the imprisoned Rwandan activist who inspired the film Hotel Rwanda, has been the victim of a near-constant surveillance campaign, according to a forensic analysis of her mobile phone that found evidence of multiple attacks using NSO Group spyware.

Carine Kanimba, a US-Belgian dual citizen, has been leading her family's effort to free her father from prison following Rusesabagina's abduction and forced return to Kigali last year by the government of the Rwandan president, Paul Kagame.

> Rusesabagina is a Belgian national widely credited with saving more than 1,000 people in the Rwandan genocide. He became a vocal critic of Kagame and was living in the US and Belgium until his arrest by the Rwandan government last year. He is facing life in prison after being accused of terror-related charges, including murder and staging attacks in Rwanda. The 67-year-old's family staunchly deny the allegations.

24. Policies to stop the global spyware catastrophe?

Experts @davidakaye & @MarietjeSchaake say:

- Immediate moratorium on sale & transfer
-Rule-of-law requirements on users
-Victims must be able to sue
-Global principles of conduct

#PegasusProject
https://t.co/60JBvg8qrS https://t.co/d8225HcIfu

> The international community should take action to constrain the global spyware industry. The effort should include the following.
>
> First, governments should implement a moratorium on the sale and transfer of spyware technology until a global export regime can identify and place these tools under global restraint.
>
> During this pause, governments should negotiate a regime that, among other things, carefully defines the technologies at issue; requires transparent human-rights assessments for the development and transfer of any such tools; involves a public registry of tools, companies and clients: and enables public comment in the case of any application for export.
>
> It is essential that Israel reins in its spyware sector and joins democratic nations in pushing back against the proliferation of technologies that operate like commercial intelligence services.
>
> Second, export control is not the only tool available to constrain the spread of spyware. Governments using these technologies must put in place transparent, rule-of-law based requirements for any use of spyware. Any government that fails to develop such requirements — or that has a pattern of abuse — should be on a global no-transfer list. Democracies and authoritarian states will probably part ways quickly.
>
> Third, the victims of spyware must be granted the ability to sue governments and companies involved in the surveillance industry. The persistence of transnational repression is such that individuals often are harmed by actors operating beyond their borders, but domestic law often presents barriers to accountability. Those barriers should be removed.

Finally, the companies themselves need to be subject to multi-stakeholder constraint. The NSO Group claims to adhere to the United Nations Guiding Principles on Business and Human Rights, a global standard for corporate human rights practice. But it does not subject its policy to any independent scrutiny.

Taking a page from the effort to restrict the private mercenary industry, the international community should work toward a global code of conduct and stop the proliferation of spyware for repression.

25. #INDIA ■■ (3/) Rahul Gandhi was Prime Minister #Modi's main opponent in the 2019 nat'l elections.

During the campaign, 2 of his phones were put on the #PegasusProject list, and 5 of his friends & fellow Congress party officials.

https://t.co/niZcPPKgR3 https://t.co/RfoyPTJlC8

Rahul Gandhi with his sister Priyanka Gandhi in Kalpetta in southern India in 2019. Rahul Gandhi, the country's main opposition leader and the great-grandson of India's first prime minister, is one of the most prominent Indians to appear on a list that includes numbers selected for surveillance by an NSO Group client. (Atul Loke/Getty Images)

26. #NSOGroup & #Pegasus spyware customers are issuing panicky, fairy-tale denials.

Here's my take.

#PegasusProject
https://t.co/M6tpDpyqe1

27. BREAKING: 10 prime ministers, 3 presidents & a king on the #PegasusProject spyware list.

Included, French president @EmmanuelMacron
■■

Crystal clear: #NSOGroup is a global national security threat.

Story: **https://t.co/qW4paLz7IF https://t.co/npvridrwkp**

But here's who's on the list: Three sitting presidents, France's Emmanuel Macron, Iraq's Barham Salih and South Africa's Cyril Ramaphosa. Three current prime ministers, Pakistan's Imran Khan, Egypt's Mostafa Madbouly and Morocco's Saad-Eddine El Othmani.

Seven former prime ministers, who according to time stamps on the list were placed there while they were still in office, including Lebanon's Saad Hariri, Uganda's Ruhakana Rugunda, and Belgium's Charles Michel.

And one king: Morocco's Mohammed VI.

28. #NSOGroup, after courting a lot of press, is suddenly not interested in talking....

So begins the hope-this-dies-down phase of crisis management?
#PegasusProject
https://t.co/Qvdi6XIOMT

29. NEW "there's gotta be some accountability for spies-for-hire"

Senator @RonWyden to Senate Intelligence Committee yesterday in light of #PegasusProject revelations about #NSOGroup spyware.
Full: **https://t.co/uiqatzUWcN https://t.co/CqBteOTfnS**

30. NEW: 1st legal complaint from #Pegasus victims over latest spyware revelations has landed in France ■■

Brought by 2 journalists, supported by press freedom org @RSF_inter

Their statement says more complaints inbound.
#PegasusProject
https://t.co/iw3U54P09d https://t.co/osRN6HPgz4

In the wake of yesterday's revelations about the Pegasus spyware, Reporters Without Borders (RSF) and two journalists with French and Moroccan dual nationality, Omar Brouksy and Maati Monjib, filed a joint complaint with prosecutors in Paris today calling on them to "identify those responsible, and their accomplices," for targeted harassment of the journalists.

The complaint does not name NSO Group, the Israeli company that makes Pegasus, but it targets the company and was filed in response to yesterday's revelations that Pegasus has been used to spy on at least 180 journalists in 20 countries, including 30 in France.

Drafted by RSF lawyers William Bourdon and Vincent Brengarth, the complaint cites invasion of privacy (article 216-1 of the French penal code), violation of the secrecy of correspondence (article 226-15), fraudulent collection of personal data (article 226- 18), fraudulent data introduction and extraction and access to automated data systems (articles 323-1 and 3, and 462-2), and undue interference with the freedom of expression and breach of the confidentiality of sources (article 431-1).

This complaint is the first in a series that RSF intends to file in several countries together with journalists who were directly targeted.

The complaint makes it clear that NSO Group's spyware was used to target Brouksy and Monjib and other journalists the Moroccan authorities wanted to silence. The author of two books on the Moroccan monarchy and a former AFP correspondent, Brouksy is an active RSF ally in Morocco. Monjib, who was recently defended by RSF, was released by the Moroccan authorities on 23 March after a 20-day hunger strike, and continues to await trial.

"We will do everything to ensure that NSO Group is convicted for the crimes it has committed and for the tragedies it has made possible," RSF secretary-general Christophe Deloire said. "We have filed a complaint in France first because this country appears to be a prime target for NSO Group customers, and because RSF's international's headquarters are located here. Other complaints will follow in other countries. The scale of the violations that have been revealed calls for a major legal response."

31. NEW: Dalai Lama's inner circle on the #PegasusProject list. (He's not thought to carry a phone)

Happened in period before & after a private meeting with @BarackObama.

#India■■ suspected as #NSOGroup #spyware client responsible.

Report: **https://t.co/dVQt7KNfEj https://t.co/0DqpJteoIY**

any government that interfered with the selection process.

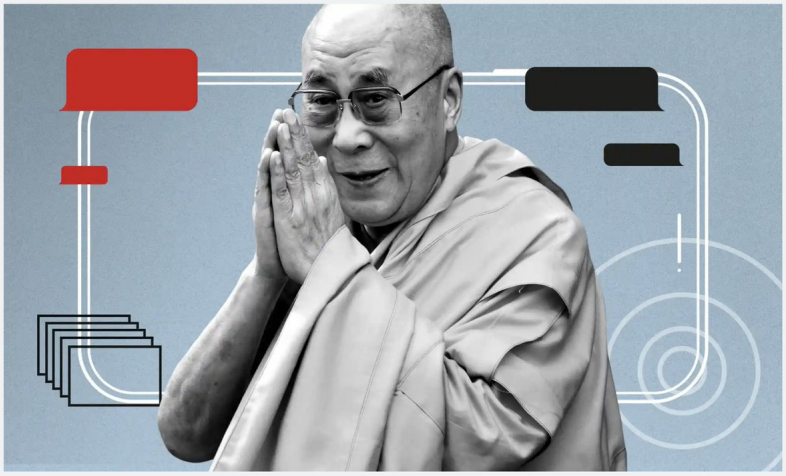
The records suggest Tibetan leaders were first selected in late 2017, in the period before and after the former US president Barack Obama met the Dalai Lama privately on a foreign tour that also included earlier stops in China.

Senior advisers to the Dalai Lama whose numbers appear in the data include Tempa Tsering, the spiritual leader's long-time envoy to Delhi, and the senior aides Tenzin Taklha and Chhimey Rigzen, as well as Samdhong Rinpoche, the head of the trust that has been tasked with overseeing the selection of the Buddhist leader's successor.

▲Tempa Tsering, right, the chief representative of the Dalai Lama in Delhi, speaks to the media alongside his wife, the Dalai Lama's sister Jetsun Pema. Photograph: Yoshikazu Tsuno/AFP/Getty Images

India could have several motives for possible spying on Tibetan leaders but some in Dharamsala have concluded the question of succession may be a driving force. Naming successors to the Dalai Lama has sometimes taken years after the death of the title holder, and is usually led by the monk's senior disciples, who interpret signs that lead them to the child next in line.

But China views the next Dalai Lama as a potential separatist leader who could weaken its authoritarian grip on Tibet. It has claimed the sole right to control the selection process, and analysts say it is already pressuring neighbours such as Nepal and Mongolia to rule out recognising any successor but its own.



▲The Dalai Lama is not thought to carry a personal phone, but numbers linked to his senior advisers appear in the data leak. Composite: Guardian/AP

32. NEW: While #NSOGroup is trying to distract you with a counter narrative...

Here are #Indian ■■ Police barging into the offices of one of the #PegasusProject media outlets. ■
https://t.co/YvK9lNHKKY

35. TODAY: @WhatsApp CEO @wcathcart rubbishes #NSOGroup's denials:

- #PegasusProject reporting consistent w/targeting in #NSOGroup's 2019 attack on WhatsApp users.
- Points out: in *only* 2 weeks 1.4k numbers were confirmed targeted in 2019. Do the math.

https://t.co/3odDQKBI0E https://t.co/0vBolNMN7d

"The reporting matches what we saw in the attack we defeated two years ago, it is very consistent with what we were loud about then," Cathcart said in an interview with the Guardian. In addition to the "senior government officials", WhatsApp found that journalists and human rights activists were targeted in the 2019 attack against its users. Many of the targets in the WhatsApp case, he said, had "no business being under surveillance in any way, shape, or form".

"This should be a wake up call for security on the internet ... mobile phones are either safe for everyone or they are not safe for everyone."

▲Will Cathcart, the WhatsApp chief executive. Photograph: Facebook

But Cathcart questioned NSO's claim that the figure was in itself "exaggerated", saying that WhatsApp had recorded an attack against 1,400 users over a two-week period in 2019.

"That tells us that over a longer period of time, over a multi-year period of time, the numbers of people being attacked are very high," he said. "That's why we felt it was so important to raise the concern around this."

36. BIG DEAL: today @WhatsApp CEO @wcathcart *publicly confirmed* that senior national security officials of US allies■■ were targeted with #Pegasus spyware in 2019.

Clear message: #NSOGroup spyware is a national security threat.

By @skirchy **https://t.co/3odDQKBI0E https://t.co/gTvg80bL5z**

Senior government officials around the world - including individuals in high national security positions who are "allies of the US" - were targeted by governments with NSO Group spyware in a 2019 attack against 1,400 WhatsApp users, according to the messaging app's chief executive.

37. Taking #NSOGroup's denials at face value?

CEO: "you won't reach 50,000 #Pegasus targets since the company was founded"

FACT: there were >1,400 *confirmed* targets in just 2 weeks in 2019 per @WhatsApp.

At this rate NSO would have easily reached 50k+
https://t.co/WCNOnozLL0 https://t.co/DcYUOkh9lv

According to Hulio, "the average for our clients is 100 targets a year. If you take NSO's entire history, you won't reach 50,000 Pegasus targets since the company was founded. Pegasus has 45 clients, with around 100 targets per client a year. In addition, this list includes countries that aren't even our clients and NSO doesn't even have any list that includes all Pegasus targets - simply because the company itself doesn't know in real-time how its clients are using the system."

38. Not familiar with the 2019 #NSOGroup attack on @WhatsApp?

#Pegasus spyware was used to target people via WhatsApp in 2019. WhatsApp spotted it, quickly shut it down, notified all targets...and then *sued* NSO.

We @citizenlab helped investigate.
https://t.co/biMxFzJF9O

39. "A.Q. Khans of the cyber world"

■■ US lawmakers just came out swinging against mercenary hacking company #NSOGroup.

Statement: US Gov must impose consequences in light of latest revelations of spyware misuse.

Reps @Malinowski @RepKatiePorter @JoaquinCastrotx @RepAnnaEshoo **https://t.co/rVgMxc9M4o**

ENOUGH IS ENOUGH – JOINT STATEMENT FROM REPRESENTATIVES TOM MALINOWSKI, KATIE PORTER, JOAQUIN CASTRO AND ANNA G. ESHOO ON THE ABUSES LINKED TO THE NSO GROUP'S PEGASUS SPYWARE

July 26, 2021 | Press Release

(Washington, DC) Representatives Tom Malinowski (NJ-07), Katie Porter (CA-45), Joaquin Castro (TX-20), and Anna G. Eshoo (CA-18) issued the following statement today on reports that the NSO Group's sophisticated Pegasus spyware was used by authoritarian regimes against peaceful activists and journalists around the world.

"Enough is enough. The recent revelations regarding misuse of the NSO Group's software reinforce our conviction that the hacking for hire industry must be brought under control. Private companies should not be selling sophisticated cyber-intrusion tools on the open market, and the United States should work with its allies to regulate this trade. Companies that sell such incredibly sensitive tools to dictatorships are the A.Q. Khans of the cyber world. They should be sanctioned, and if necessary, shut down.

The NSO Group's denials are not credible, and show an arrogant disregard for concerns that elected officials, human rights activists, journalists, and cyber-security experts have repeatedly raised. The authoritarian governments purchasing spyware from private companies make no distinction between terrorism and peaceful dissent; if they say they are using these tools only against terrorists, any rational person should assume they are also using them against journalists and activists, including inside the United States. Selling cyber-intrusion technology to governments like Saudi Arabia, Kazakhstan, and Rwanda based on assurances of responsible use is like selling guns to the mafia and believing they will only be used for target practice.

The United States government and our allies often partner with private companies to develop and provide to our national security agencies sensitive technologies. But we would never tolerate a company that contracts with the Pentagon to develop drone, or missile, or laser technology, and then sells that technology on the open market to governments that might use it against us. If hacking for hire companies continue to exist, clear rules must be established to ensure they only do business with governments in rule of law states.

To that end, we call on the United States government to urgently:

1. Call out by name publicly and in reports provided to Congress private companies that sell cyber-intrusion tools to governments with a history of misusing them.
2. Consider the immediate addition of the NSO Group and any other company engaged in similar activities to the Entity List administered by the Commerce Department and consider the company's abusive clients for sanction under the Global Magnitsky Act.
3. Establish by legislation or executive order a sanctions regime to hold accountable individuals and companies that sell these tools to authoritarian states.
4. Ensure that the NSO Group and companies engaged in similar activities do not access American investors funds—including through a potential IPO—through SEC regulations that would protect non-securitized capital from funding their activities.
5. Accelerate efforts to finalize accession to the Wassenaar Arrangement's limited controls on cyber-intrusion tools, lead a multilateral initiative to impose strengthened controls with transparent human rights assessments on items with surveillance capabilities, and consider SEC regulations requiring companies to publicly disclose exports of technologies with surveillance capabilities and to carry out published human rights due diligence for any such exports.
6. Investigate and assess the possible targeting of American 'journalists, aid works, diplomats and others' with NSO Group's Pegasus spyware, determine whether America's national security was harmed, and take steps to protect all Americans, including federal employees, from the threat posed by the growing mercenary spyware industry."