EJÉRCITO ESPÍA

Red en Defensa de los Derechos Digitales, ARTICLE 19 Mexico and Central America, and SocialTIC, with the support of the Citizen Lab of the University of Toronto ─ and alongside the media outlets: *Animal Político, Aristegui Noticias* and *Proceso*─ reveal three new cases of espionage against journalists and human rights defenders in Mexico.

These attacks all have something in common: they were all spied on using the Pegasus malware during this government administration, and while they carried out work and investigations related to human rights violations committed by the Armed Forces.

This investigation has collected evidence that shows that, contrary to promises made by the current President, during this government the Ministry of National Defense (SEDENA) acquired a remote information monitoring system from the company that exclusively represents the sale of Pegasus in Mexico. The evidence further shows how SEDENA has systematically lied before various institutions in order to conceal the existence of this contract.

The findings of this investigation show that the Federal Government has not fulfilled its commitment to end illegal espionage in Mexico, as well as refuting the thesis on which the current government has based the drive for militarization in the country.

We publish this collaborative work hoping that it contributes - once and for all - to the dismantling of the arbitrariness of intelligence mechanisms that operate without accountability, facilitating the violation of human rights violation and denying access to truth and justice for society.

1. How Pegasus works

Pegasus is spyware produced by the Israeli company **NSO Group**. Due to its exportation license, **it can only be sold to governments**.

The technological capabilities of Pegasus have grown in recent years. The malware takes advantage of unknown vulnerabilities ─ that is to say, vulnerabilities that are not known to the manufacturer of the device ─ to attack, infect and gain control of the device.

While the version of Pegasus that was documented in 2017 required user interaction, the most recent versions use zero-clic vulnerabilities for their attacks. This means that it is no longer necessary for the target to interact in any way ─ such as clicking on a link or opening a file─ to infect the device.

In recent years, how Pegasus has taken advantage of vulnerabilities within mobile phone applications has been documented, for example the use of WhatsApp (2019) to infect telephones through a missed video call. In 2021 it was discovered that Pegasus had used a vulnerability in iMessage to access Apple devices.

Once Pegasus manages to infect a device, **it can access practically everything on that device:** text messages, calls, instant messenger applications (including encrypted applications such as WhatsApp or Signal), contacts list, emails, notes, photographs, and generally files that are stored on the device.

Pegasus can also **access the telephone's microphone and camera,** as well as **passwords that are saved** on the device to access email and social media accounts. Once in total control of the device, **Pegasus can delete any trace of the infection,** becoming virtually undetectable.

Another significant change is that, given that it can attack a device at practically any time, it is no longer necessary for the infection to last for days or weeks. Similarly, the attacker can **access message logs**, through which they can obtain months of conversation history during one single attack.

Organizations including Citizen Lab of the University of Toronto and Amnesty International have developed forensic methodologies that allow them to identify if a device was attacked with Pegasus through a series of traces that the malware leaves in the device. This technical analysis allows them to link a device with, for example, the NSO Group infrastructure.

Based on forensic analysis, Citizen Lab has confirmed the detection of Pegasus on the devices of **at least three people.**

CASES

1. Case: Raymundo Ramos Vázquez

Raymundo Ramos Vázquez is a human rights defender who has documented serious human rights violations in the state of Tamaulipas for more than 20 years. He is President of the Nuevo Laredo Human Rights Committee.

Since 2010, through his work Raymundo has denounced forced disappearances, torture, extrajudicial executions, among other abuses perpetrated by the Armed Forces in the state.

Pegasus attacks

Forensic analysis by the University of Toronto's Citizen Lab found that Raymundo Ramos' devices were compromised with Pegasus malware on the following dates:

- Around 28 August 2020
- Around 2 September 2020
- Around 3 September 2020

Citizen Lab clarifies that these findings do not exclude the possibility that the device may have been infected on previous occasions.

Context of the attacks

Raymundo Ramos has systematically documented human rights violations committed by the Army and Navy in Tamaulipas. In the activist's own words, the accumulation of serious cases during this six-year [government] term and the fear that the reports could reach the international arena could have been the reason for the espionage against him.

In recent years, Ramos has accompanied at least three major cases involving the Armed Forces: in 2018, the forced disappearance of 56 people in Nuevo Laredo; in 2019, the extrajudicial execution of eight people; and in 2020, the murder of three civilians during a chase.

The attacks against Raymundo Ramos occurred days after the newspaper El Universal published a video showing a group of soldiers firing at a pickup truck allegedly carrying members of organized crime. The soldiers reported that there were no survivors in the confrontation and 12 people were killed.

The video refutes the Army's version by showing one person still alive after the shots were fired. Upon realizing this, a soldier orders the killing of this person. The newspaper revealed that among the alleged criminals there were also three kidnapped civilians, bound hand and foot, who were executed in the operation: two of them were shot in the thorax and one in the skull.

Between 16 and 19 August, Ramos was visiting Mexico City. On the 18th, the activist visited the editorial office of El Universal; that same day he held meetings with the Secretary of the Navy and the Office of the United Nations High Commissioner for Human Rights.

On 24 August, the same day of the El Universal publication, Ramos criticized the actions of the military authorities in Tamaulipas in a column in the Washington Post.

Ramos was again in Mexico City between 25 and 27 August. On that occasion, he met again with the Secretary of the Navy, as well as the National Human Rights Commission (CNDH) and the media outlet Animal Político. On August 29 —the day he was attacked with Pegasus— the activist held a meeting with personnel from the Secretariat of National Defense (SEDENA).

Subsequently, Ramos returned to Tamaulipas for the first anniversary of the extrajudicial executions in Valles de Anahuac, Nuevo Laredo, at the hands of the State Police and SEDENA. Citizen Lab confirmed in its analysis that Raymundo's phone was tapped with Pegasus around 2 and 3 September.

Over the years, the human rights defender has been the target of defamation and harassment campaigns for his work. Around the time of the Pegasus attacks, a text was also published in which he was falsely accused of defending the house of a leader of the Northwest Cartel.

Ramos states that on numerous occasions he has been singled out by members of the Armed Forces for "defending criminals" and has even been called their "enemy" for documenting abuses.

"The espionage puts my life, my integrity and my family at risk," says the defender, who adds that this administration "is feeding the impunity" of the military authorities.

Currently, Ramos is accompanying the murder case of Heidi, a five-year-old girl who was killed in September 2022 by an alleged stray bullet during an Army chase in Nuevo Laredo.

2. Case: Ricardo Raphael

Ricardo Raphael es un periodista, analista político, investigador y escritor. Colabora en diversos espacios informativos en radio y televisión, y es columnista en *Proceso* y *Milenio Diario*. Es autor de la novela *Hijo de la Guerra,* la biografía periodística *Los socios de Elba Esther,* entre otros títulos. Actualmente es conductor del noticiario matutino en el canal ADN40.

Raphael escribe habitualmente acerca del acontecer nacional. Sus columnas proporcionan información y ofrecen contexto relevante al debate público, en especial en torno a escándalos políticos, investigaciones periodísticas y casos judiciales.

Ricardo Raphael is a journalist, political analyst, researcher and writer. He collaborates in several radio and television news programs, and is a columnist for *Proceso* and *Milenio* Diario. He is the author of the novel *Hijo de la Guerra*, the journalistic biography and *Los*

socios de Elba Esther, among other titles. He is currently the host of the morning newscast on channel ADN40.

Raphael writes regularly about national events. His columns provide information and offer relevant context to the public debate, especially on political scandals, journalistic investigations and court cases.

Pegasus attacks

Ricardo Raphael's device was attacked on the following dates:

- Around 30 October 2019
- Around 7 November 2019
- Around 16 November 2019
- Around 27 December 2020

In addition, forensic analysis of his mobile device found that Raphael had previously been targeted by Pegasus from 26 May 2016 through 25 August 2016.

Context of the attacks

Since the first Pegasus attacks against him in 2016, Ricardo Raphael has consistently addressed issues related to human rights violations by the Armed Forces in his media spaces.

For example, between May and August 2016 ─the period in which he was spied on under the Peña Nieto government─ the columnist reported on the discovery of skeletal remains, presumably of the Ayotzinapa normalista students, six kilometers from Cocula. Days later, he exposed the dissatisfaction of the president of the IACHR with "the unsustainable version" of the PGR regarding the Ayotzinapa case.

In October 2019, Raphael presented *Hijo de la Guerra* (Son of War), a book based on a series of interviews with an individual who presents himself as Galdino Mellado Cruz, one of the founders of the Zetas criminal group. Mellado Cruz died in May 2014, according to the official version. However, the author claims to have spoken with him in a prison in Chiconautla, Mexico State.

Raphael points out that the attacks with Pegasus coincide with the dates when he went on a media tour to promote his book. The articles that were published in those days about the book refer to the military origin of Los Zetas and the importance of that time for the subsequent violence in the country.

In addition, the week prior to the attacks, Ricardo held meetings with figures such as Francisco Cox, from the Interdisciplinary Group of Independent Experts (GIEI) of the Ayotzinapa case; and with Jan Jarab, Representative in Mexico of the UN High Commissioner for Human Rights.

In 2020, Ricardo Raphael also published in The Washington Post about the violence of the Armed Forces in Tamaulipas, where he attributed the escalation to a collaboration agreement between the local governor and the authorities. Likewise, the journalist closely followed the judicial process against General Salvador Cienfuegos in the United States, as well as his subsequent extradition to Mexico.

On 13 December 2020, Raphael published an article in *Proceso* where he reported that José Luis Abarca, the municipal president of Iguala accused of being the mastermind in the Ayotzinapa case, would be released due to lack of evidence. A day before the last attack registered against Ricardo, on 26 December, a report published in Aristegui Noticias ─ titled "The end of the 'historical truth about Ayotzinapa'─ cited the information published in *Proceso* about Abarca.

The espionage against Raphael has been used as part of a smear campaign orchestrated by Isabel Miranda de Wallace. In July 2022, Raphael reported having received a series of files obtained through wiretaps, with decontextualized fragments of a conversation he had at the end of 2019. These audios were also presented to the FGR to report an unfounded allegation of corruption.

That same month, his 12-year-old son received an unusual phone call, in which a man with a deep voice asked about his father and grandfather. "That's when I realized that they were… following me - spying on me," he says.

3. Case: *Animal Político*

Animal Político is a digital media outlet that covers issues related to human rights, corruption, accountability, among others. It has been the author of high-level journalistic investigations such as La Estafa Maestra (The Master Swindle) and Las empresas fantasma de Javier Duarte (Javier Duarte's ghost companies).

During this government administration, the media has been falsely accused by the Presidency of having alleged links with foreign financiers in order to criticize the current government.

Pegasus attacks

Forensic analysis by the Citizen Lab at the University of Toronto confirmed that an *Animal Político* journalist ─whose identity is kept anonymous for security reasons─ was attacked with Pegasus in 2021.

Again, Citizen Lab clarifies that these findings do not exclude the possibility that the device could have been infected on other previous occasions.

Context of the attacks

The attack on the *Animal Político* journalist occurred on the same day that the digital media outlet published a story related to human rights violations perpetrated by the Armed Forces and on days in which it met with sources linked to such violations.

During the current administration, *Animal Político* has provided critical coverage of human rights violations committed by the Armed Forces in Mexico. The media outlet has followed cases of forced disappearance and extrajudicial executions, among others, perpetrated by members of the Army and the Navy.

For Daniel Moreno, Director of *Animal Político*, these attacks are especially serious because the intervention of a journalist's device implies a vulnerability for the entire newsroom, especially after the media outlet moved its operations to a remote work model due to the pandemic.

The spying on the *Animal Político* journalist put not only the person attacked at risk, but the entire newsroom of the media outlet. At the time of the attack, the journalist was in at least 25 chats involving colleagues and staff, topics and even sources of information.

Furthermore, the attacks are also an indication that there has been no substantial change in the use of spying technologies against journalists and human rights defenders.

EVIDENCE

1. NSO Group only sells to governments

NSO Group has repeatedly stated that it **only sells its products to governments**.

Shalev Hulio, President of NSO Group, has declared under oath before court in the United States on a number of occasions that the company only sells its technology to governments and their agencies for the purposes of national security and justice.

This is because sales of Pegasus are monitored and regulated by the Israeli government through an export control law. To export its technology, NSO Group must register with the Israeli Ministry of Defense.

According to Hulio, NSO Group's contracts require its customers to **prove** that they are foreign governments or national security and/or law enforcement agencies authorized by a foreign government. In addition, the company assured the courts that it does not market or sell its technologies for use by private entities.

In an appearance before the European Parliament, NSO Group maintained its position: the company only sells to governments. "NSO's products are licensed for sale with the approval of the Israeli Export Control Authority and are provided exclusively to government, intelligence and law enforcement agencies," the Israeli firm's General Counsel stated under oath.

NSO Group also told the European Parliament that it has put in place new security measures that prevent its systems from being moved or operated by unauthorized personnel. The company also obliges its clients to sign a government-to-government certificate in which they agree not to transfer the technology to third parties.

2. The Armed Forces have a system for "intelligence work".

On 3 August 2021, President Andrés Manuel López Obrador was questioned in his morning conference about the use of Pegasus by the Army. When asked about the status of the malware in SEDENA, the president responded:

> *Andrés Manuel López Obrador: — At present there are no longer contracts with these companies. There is a service provided by the Ministry of Defense, as well as other ministries, such as the Navy, to carry out intelligence work…*
>
> *Journalist: — With Pegasus?*
>
> *AMLO: — No, a relationship with that company no longer exists*

López Obrador also pledged to release more details. "We are going to inform, we are going to have the Secretary of Defense inform us in due time," he said. As of the date of publication of this text, neither the Presidency nor the SEDENA have clarified this intelligence system.

3. The current government — including the Army — continues to buy from Pegasus suppliers

Although the Federal Government has denied continuing to use Pegasus or having any relationship with the companies that marketed it in past administrations, there is evidence that the current administration has signed contracts during this six-year term with companies linked to the sale of Pegasus malware during the administration of Enrique Peña Nieto.

As a result of Project Pegasus, a network of intermediary companies headed by **KBH Track** was revealed, which includes several companies such as **Proyectos y Diseños VME**, BLITZ Corp, Grupo Comercial Vicra, **Air Cap**, BSD Applied Technologies and **Comercializadora Antsua**, among others.

These companies share key names among their legal representatives and shareholders. One of them is **Marco Antonio Suárez Cedillo**, who appears as legal representative of the company **Diseños y Proyectos VME**, which signed contracts and received payments related to Pegasus from CISEN, PGR and SEDENA during the previous government.

Suárez Cedillo also states that he is the legal representative of **Comercializadora Antsua**, a company that received a direct award of contract from the **National Migration Institute** in December 2019 for "leasing and technical support of computer equipment." The contract is reserved for five years under alleged national security reasons.

According to information obtained by the Guacamaya hacktivist group's leak, SEDENA has continued to request quotes from companies in the Pegasus network. For example, in November 2020, SEDENA requested a quote from Comercializadora Antsua; in March 2021, from Proyectos y Diseños VME; and in April 2022 (months after the Project Pegasus scandal), from KBH Track, to mention a few cases.

4. Comercializadora Antsua was authorized by NSO Group to sell Pegasus to SEDENA

On 20 July 2021, the Attorney General's Office of Mexico reported a series of investigations and searches carried out at the company KBH Track. As per journalistic reports, during these investigations several documents were recovered, including two letters accrediting **Comercializadora Antsua** as an entity authorized to offer Pegasus in Mexico.

The first letter, signed by NSO Group director Shalev Hulio, grants Comercializadora Anstua "**rights and representation in Mexico**" as of March 2018. The letter also mentions Air Cap —a company that participated in the renewal of Pegasus licenses to the PGR in 2017— as its representative until February 2018. Comercializadora Antsua and Air Cap are companies with a close relationship in the Pegasus intermediary network: the legal representative of Air Cap, Yaraví Yunuén Reséndiz Villalobos, was also part of the board of Comercializadora Antsua (Proceso, November 14, 2011).

The second letter, dated January 2018, authorizes Comercializadora Antsua to "**exclusively represent NSO Group**" before the **Ministry of National Defense** until 31 December 2019. During the search, several documents with the letterhead of the SEDENA were also recovered.

5. La SEDENA acquired a “remote monitoring service” from Comercializadora Antsua in 2019

The leak of Army documents by the hacker group Guacamaya has revealed that SEDENA acquired a "**Remote Information Monitoring Service**" from **Comercializadora Antsua** in April 2019, under contract DN-10 SAIT-1075/P/2019.

In a email sent by the Electronic Warfare Section of the General Directorate of Transmissions of SEDENA with the subject "Oficios Mortales" (Deadly Trades), a letter dated 18 January 2020 is attached, where the existence of that contract is acknowledged and refers to an original invoice corresponding to a second payment for the service provided from 1 June to 30 June 2019.

(SECRETO)

Secretaría de la Defensa Nacional
Dirección General de Transmisiones

"2020, Año de Leona Vicario, Benemérita Madre de la Patria".

"Ordinario"

Dependencia:	Dir. Gral. Trans. Subdir. Optva.
Sección:	Guerra Electrónica.
Mesa:	Trámite.
No. de Oficio:	SGE-3335
Expediente:	

Asunto: Se remite factura legalizada.

Campo Mil. No. 1-H, Los Leones Tacuba, Cd. Méx., a 18 de enero del 2020.

C. General.
Secretario de la Defensa Nacional.
Dirección General de Administración.
Subdir, Adqs. (S. C. P. y C.P.).
Lomas de Sotelo, Cd. Méx.

Antecedente: Contrato DN-10 SAIT-1075/P/2019 No. SIA: 4500031649 de fecha 12 de abril del 2019.

En relación a la Cláusula Segunda "Descripción del Servicio" del contrato citado en antecedentes para la prestación del **"Servicio de Monitoreo Remoto de Información"**, fincado a la empresa **"Comercializadora Antsua, S.A. de C.V."**, adjunto al presente se remite a usted, la siguiente documentación:

Anexos:
5 (cinco) fojas.

A. 1 (una) Factura original No. 197 debidamente legalizada correspondiente al servicio proporcionado del **1 al 30 de junio del 2019 (segundo pago)**.

B. 1 (un) Oficio de aceptación No. 1910-4950 de fecha 15 Jul. 2019, **en original** emitido por el usuario final, en el cual se informa que el servicio fue recibido del **1 al 30 de junio del 2019**.

C. 1 (un) Dictamen Técnico No. 1910-4951 de fecha 1 de julio del 2019, **en original** elaborado por el usuario final 1 (una) foja.

D. 1 (un) Acta de incumplimiento No. 1910-4952 de fecha 1 de julio del 2019, **en original** elaborada por el usuario final en **2 (dos) fojas**.

Lo anterior, a fin de que se continúe con el trámite correspondiente **bajo la consideración de los incumplimientos que se señalan** en el acta que se cita en texto.

Respetuosamente
Sufragio efectivo. No reelección.
El Gral. Bgda. Trans. D.E.M., Director.

[redacted]

c.c.p. El C. Gral. Srio. Def. Nal., Subjfas., Admtva. y Log. e Intl.; S-4 (Log.) Ss. P. y E., para su superior conocimiento.- Lomas de Sotelo, Cd. Méx.
c.c.p. El C. Gral. Srio. Def. Nal., Oflía. Myr. esta Sría. (Coord. Adqs. y Ppto.), mismo fin.- Lomas de Sotelo, Cd. Méx.
c.c.p. El C. Gral. Srio. Def. Nal., Insp. y Ctlría. Gral. Ejto. y F.A., igual fin.- Lomas de Sotelo, Cd. Méx.
c.c.p. El C. Gral. Srio. Def. Nal., Dir. Gral. Admón. Subdir. Adqs. (S.A.I.T.), idéntico fin, **anexándole copias** de los documentos citados en texto.- Lomas de Sotelo, Cd. Méx.
c.c.p. El C. Cor. I.C.E. D.E.M., Dir. C.M.I. del E.M.D.N., para su conocimiento, en relación a su Oficio No. 1910-4950 de fecha 15 de julio del 2019.- Campo Militar No.1-A, Cd. Méx.
c.c.p. El C. Cap. 1/o. I.C.E., Enc. Coord. Adqs. esta Dir. Gral., para su conocimiento.- Presente.

HMZ-RLM-NOCM.

(SECRETO)

Another document referring to this contracting indicates that the company Fianzas y Cauciones Atlas S.A. granted a guarantee for 12 million pesos to Comercializadora Antsua for contract DN-10 SAIT-1075/P/2019, with a compliance date of 31 December 2020.

During the period in which this monitoring system was acquired from Antsua, the intermediary company **was authorized by NSO Group** to offer its products to SEDENA.

6. NSO Group has marketed Pegasus under other names

Faced with the bad reputation that Pegasus has gained from spying scandals around the world, **NSO Group** has resorted to using aliases to try to evade public scrutiny of its malware.

The Israeli company, for example, uses the name **Q Cyber Technologies** to try to go undetected and refers to its product simply as **Q Suite**.

Alternate names for Pegasus that have been identified include Minotaur in Thailand, used to spy on pro-democracy movement activists in the Asian country.

NSO Group also tried to sell Pegasus to the U.S. Federal Bureau of Investigation (FBI) in 2019, under the name **Phantom**, a report in The New York Times revealed.

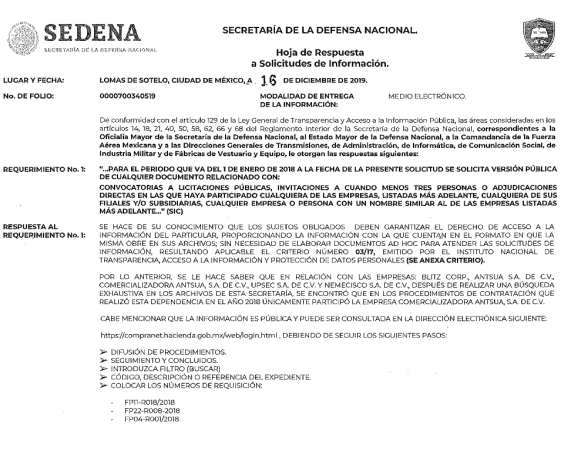
Pegasus' multiple identities make it more difficult to detect through contract searches or information access requests, and also allow governments to conceal the fact that they have the malware.

7. The Federal Government has concealed its links to Comercializadora Antsua

Following the revelations made by the Pegasus Project in 2021, the federal government published information about the network of companies that sold the malware during the administration of Enrique Peña Nieto. However, **Comercializadora Antsua**'s membership in this network has been **inexplicably omitted**.

On 21 July, the then Head of the Secretariat of Finance and Public Credit's **Financial Investigations Unit**, Santiago Nieto, presented a list of companies linked to the network of intermediaries that sold Pegasus during the previous government. However, in his presentation he omitted Comercializadora Antsua, despite the fact that it shared the same "fronts" with companies such as Proyectos y Diseños VME or KBH Track, which were mentioned.

Apart from the omissions, **the Army has systematically denied** having contracts with this company. For example, in response to requests for access to information made by R3D in late 2019, SEDENA responded in December 2019 that "after conducting an exhaustive search in the files of the Secretariat, **no documentary evidence was found**," despite the fact that as has been demonstrated above, SEDENA contracted a "Remote Information Monitoring Service" from Comercializadora Antsua in April 2019.



SEDENA
SECRETARÍA DE LA DEFENSA NACIONAL

SECRETARÍA DE LA DEFENSA NACIONAL.

Hoja de Respuesta a Solicitudes de Información.

LUGAR Y FECHA: LOMAS DE SOTELO, CIUDAD DE MÉXICO, A 16 DE DICIEMBRE DE 2019.

No. DE FOLIO: 0000700340519 **MODALIDAD DE ENTREGA DE LA INFORMACIÓN:** MEDIO ELECTRÓNICO.

De conformidad con el artículo 129 de la Ley General de Transparencia y Acceso a la Información Pública, las áreas consideradas en los artículos 14, 18, 21, 40, 50, 58, 62, 66 y 68 del Reglamento Interior de la Secretaría de la Defensa Nacional, **correspondientes a la Oficialía Mayor de la Secretaría de la Defensa Nacional, al Estado Mayor de la Defensa Nacional, a la Comandancia de la Fuerza Aérea Mexicana y a las Direcciones Generales de Transmisiones, de Administración, de Informática, de Comunicación Social, de Industria Militar y de Fábricas de Vestuario y Equipo, le otorgan las respuestas siguientes:**

REQUERIMIENTO No. 1: **"...PARA EL PERIODO QUE VA DEL 1 DE ENERO DE 2018 A LA FECHA DE LA PRESENTE SOLICITUD SE SOLICITA VERSIÓN PÚBLICA DE CUALQUIER DOCUMENTO RELACIONADO CON:**

CONVOCATORIAS A LICITACIONES PÚBLICAS, INVITACIONES A CUANDO MENOS TRES PERSONAS O ADJUDICACIONES DIRECTAS EN LAS QUE HAYA PARTICIPADO CUALQUIERA DE LAS EMPRESAS, LISTADAS MÁS ADELANTE, CUALQUIERA DE SUS FILIALES Y/O SUBSIDIARIAS, CUALQUIER EMPRESA O PERSONA CON UN NOMBRE SIMILAR AL DE LAS EMPRESAS LISTADAS MÁS ADELANTE..." (SIC)

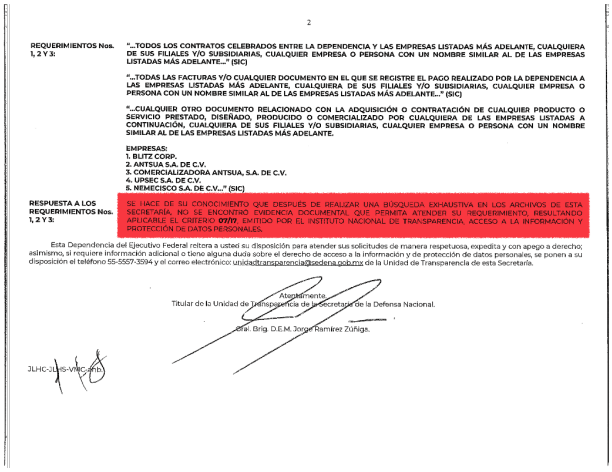
RESPUESTA AL REQUERIMIENTO No. 1: SE HACE DE SU CONOCIMIENTO QUE LOS SUJETOS OBLIGADOS DEBEN GARANTIZAR EL DERECHO DE ACCESO A LA INFORMACIÓN DEL PARTICULAR, PROPORCIONANDO LA INFORMACIÓN CON LA QUE CUENTAN EN EL FORMATO EN QUE LA MISMA OBRE EN SUS ARCHIVOS; SIN NECESIDAD DE ELABORAR DOCUMENTOS AD HOC PARA ATENDER LAS SOLICITUDES DE INFORMACIÓN, RESULTANDO APLICABLE EL CRITERIO NÚMERO **03/17**, EMITIDO POR EL INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES **(SE ANEXA CRITERIO).**

POR LO ANTERIOR, SE LE HACE SABER QUE EN RELACIÓN CON LAS EMPRESAS: BLITZ CORP., ANTSUA S.A. DE C.V., COMERCIALIZADORA ANTSUA, S.A. DE C.V., UPSEC S.A. DE C.V. Y NEMECISCO S.A. DE C.V., DESPUÉS DE REALIZAR UNA BÚSQUEDA EXHAUSTIVA EN LOS ARCHIVOS DE ESTA SECRETARÍA, SE ENCONTRÓ QUE EN LOS PROCEDIMIENTOS DE CONTRATACIÓN QUE REALIZÓ ESTA DEPENDENCIA EN EL AÑO 2018 ÚNICAMENTE PARTICIPÓ LA EMPRESA COMERCIALIZADORA ANTSUA, S.A. DE C.V.

CABE MENCIONAR QUE LA INFORMACIÓN ES PÚBLICA Y PUEDE SER CONSULTADA EN LA DIRECCIÓN ELECTRÓNICA SIGUIENTE:

https://compranet.hacienda.gob.mx/web/login.html , DEBIENDO DE SEGUIR LOS SIGUIENTES PASOS:

- DIFUSIÓN DE PROCEDIMIENTOS.
- SEGUIMIENTO Y CONCLUIDOS.
- INTRODUZCA FILTRO (BUSCAR)
- CÓDIGO, DESCRIPCIÓN O REFERENCIA DEL EXPEDIENTE.
- COLOCAR LOS NÚMEROS DE REQUISICIÓN:
  - FPT1-0018/2018
  - FP22-R008-2018
  - FP04-R001/2018



2

REQUERIMIENTOS Nos. 1, 2 Y 3: **"...TODOS LOS CONTRATOS CELEBRADOS ENTRE LA DEPENDENCIA Y LAS EMPRESAS LISTADAS MÁS ADELANTE, CUALQUIERA DE SUS FILIALES Y/O SUBSIDIARIAS, CUALQUIER EMPRESA O PERSONA CON UN NOMBRE SIMILAR AL DE LAS EMPRESAS LISTADAS MÁS ADELANTE..." (SIC)**

"...TODAS LAS FACTURAS Y/O CUALQUIER DOCUMENTO EN EL QUE SE REGISTRE EL PAGO REALIZADO POR LA DEPENDENCIA A LAS EMPRESAS LISTADAS MÁS ADELANTE, CUALQUIERA DE SUS FILIALES Y/O SUBSIDIARIAS, CUALQUIER EMPRESA O PERSONA CON UN NOMBRE SIMILAR AL DE LAS EMPRESAS LISTADAS MÁS ADELANTE..." (SIC)

"...CUALQUIER OTRO DOCUMENTO RELACIONADO CON LA ADQUISICIÓN O CONTRATACIÓN DE CUALQUIER PRODUCTO O SERVICIO PRESTADO, DISEÑADO, PRODUCIDO O COMERCIALIZADO POR CUALQUIERA DE LAS EMPRESAS LISTADAS A CONTINUACIÓN, CUALQUIERA DE SUS FILIALES Y/O SUBSIDIARIAS, CUALQUIER EMPRESA O PERSONA CON UN NOMBRE SIMILAR AL DE LAS EMPRESAS LISTADAS MÁS ADELANTE.

EMPRESAS:
1. BLITZ CORP.
2. ANTSUA S.A. DE C.V.
3. COMERCIALIZADORA ANTSUA, S.A. DE C.V.
4. UPSEC S.A. DE C.V.
5. NEMECISCO S.A. DE C.V..." (SIC)

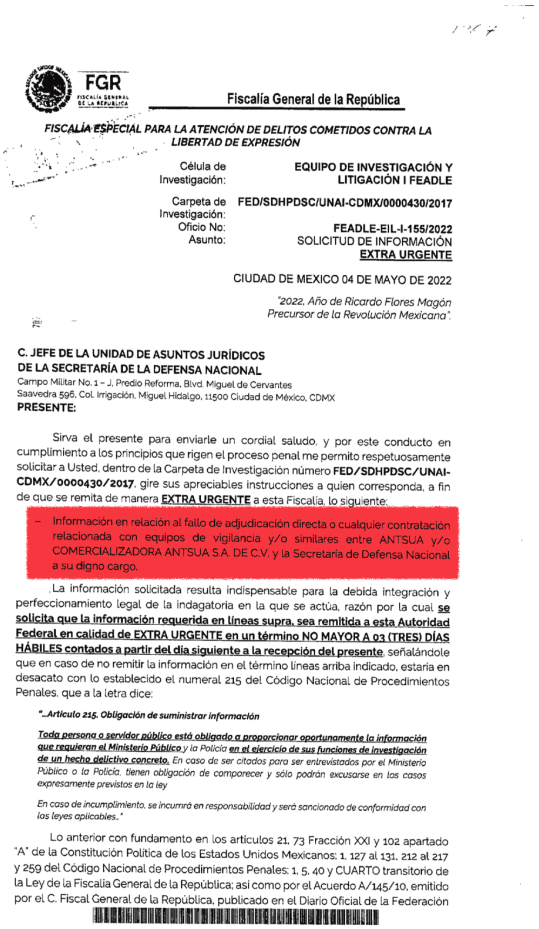
RESPUESTA A LOS REQUERIMIENTOS Nos. 1, 2 Y 3: SE HACE DE SU CONOCIMIENTO QUE DESPUÉS DE REALIZAR UNA BÚSQUEDA EXHAUSTIVA EN LOS ARCHIVOS DE ESTA SECRETARÍA, NO SE ENCONTRÓ EVIDENCIA DOCUMENTAL QUE PERMITA ATENDER SU REQUERIMIENTO, RESULTANDO APLICABLE EL CRITERIO **07/17**, EMITIDO POR EL INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES.

Esta Dependencia del Ejecutivo Federal reitera a usted su disposición para atender sus solicitudes de manera respetuosa, expedita y con apego a derecho; asimismo, si requiere información adicional o tiene alguna duda sobre el derecho de acceso a la información y de protección de datos personales, se ponen a su disposición el teléfono 55-5557-3594 y el correo electrónico: unidadtransparencia@sedena.gob.mx de la Unidad de Transparencia de esta Secretaría.

Atentamente,
Titular de la Unidad de Transparencia de la Secretaría de la Defensa Nacional.
Gral. Brig. D.E.M. Jorge Ramírez Zúñiga.

JLHC-JLGS-VMC-MTO

The SEDENA even falsified statements before the Attorney General's Office (FGR) within the investigation file related to the spying with Pegasus during the government of Enrique Peña Nieto. In response to a request from the FGR addressed to SEDENA asking for "information (...) related to surveillance and/or similar equipment between ANTSUA and the Ministry of National Defense", the military agency responded on 31 May 2022 that "it has not formalized any contractual instrument (...) with Comercializadora Antsua, S.A. de C.V.".



FGR
FISCALÍA GENERAL DE LA REPÚBLICA

Fiscalía General de la República

FISCALÍA ESPECIAL PARA LA ATENCIÓN DE DELITOS COMETIDOS CONTRA LA LIBERTAD DE EXPRESIÓN

Célula de Investigación: **EQUIPO DE INVESTIGACIÓN Y LITIGACIÓN I FEADLE**

Carpeta de Investigación: **FED/SDHPDSC/UNAI-CDMX/0000430/2017**

Oficio No: **FEADLE-EIL-I-155/2022**

Asunto: SOLICITUD DE INFORMACIÓN **EXTRA URGENTE**

CIUDAD DE MEXICO 04 DE MAYO DE 2022

"2022, Año de Ricardo Flores Magón Precursor de la Revolución Mexicana".

C. JEFE DE LA UNIDAD DE ASUNTOS JURÍDICOS DE LA SECRETARÍA DE LA DEFENSA NACIONAL
Campo Militar No. 1 – J, Predio Reforma, Blvd. Miguel de Cervantes Saavedra 596, Col. Irrigación, Miguel Hidalgo, 11500 Ciudad de México, CDMX
PRESENTE:

Sirva el presente para enviarle un cordial saludo, y por este conducto en cumplimiento a los principios que rigen el proceso penal me permito respetuosamente solicitar a Usted, dentro de la Carpeta de Investigación número **FED/SDHPDSC/UNAI-CDMX/0000430/2017**, gire sus apreciables instrucciones a quien corresponda, a fin de que se remita de manera **EXTRA URGENTE** a esta Fiscalía, lo siguiente:

- Información en relación al fallo de adjudicación directa o cualquier contratación relacionada con equipos de vigilancia y/o similares entre ANTSUA y/o COMERCIALIZADORA ANTSUA S.A. DE C.V. y la Secretaría de Defensa Nacional a su digno cargo.

La información solicitada resulta indispensable para la debida integración y perfeccionamiento legal de la indagatoria en la que se actúa, razón por la cual **se solicita que la información requerida en líneas supra, sea remitida a esta Autoridad Federal en calidad de EXTRA URGENTE en un término NO MAYOR A 03 (TRES) DÍAS HÁBILES contados a partir del día siguiente a la recepción del presente**, señalándole que en caso de no remitir la información en el término líneas arriba indicado, estaría en desacato con lo establecido el numeral 215 del Código Nacional de Procedimientos Penales, que a la letra dice:

"...Artículo 215. Obligación de suministrar información

Toda persona o servidor público está obligado a proporcionar oportunamente la información que requieran el Ministerio Público y la Policía en el ejercicio de sus funciones de investigación de un hecho delictivo concreto. *En caso de ser citados para ser entrevistados por el Ministerio Público o la Policía, tienen obligación de comparecer y sólo podrán excusarse en los casos expresamente previstos en la ley.*

En caso de incumplimiento, se incurrirá en responsabilidad y será sancionado de conformidad con las leyes aplicables."

Lo anterior con fundamento en los artículos 21, 73 Fracción XXI y 102 apartado "A" de la Constitución Política de los Estados Unidos Mexicanos; 1, 127 al 131, 212 al 217 y 259 del Código Nacional de Procedimientos Penales; 1, 5, 40 y CUARTO transitorio de la Ley de la Fiscalía General de la República; así como por el Acuerdo A/145/10, emitido por el C. Fiscal General de la República, publicado en el Diario Oficial de la Federación el 05 de julio de 2010, por el que se crea la Fiscalía Especializada para la Atención de Delitos cometidos contra la Libertad de Expresión, en relación con el Acuerdo A/109/2012 publicado en el Diario Oficial de la Federación el 25 de mayo de 2012, que reforma entre otros, el artículo PRIMERO del acuerdo A/145/10, estableciendo que esta Fiscalía Especializada, se adscribe a la Subprocuraduría de Derechos Humanos, Atención a Víctimas y Servicios a la Comunidad.

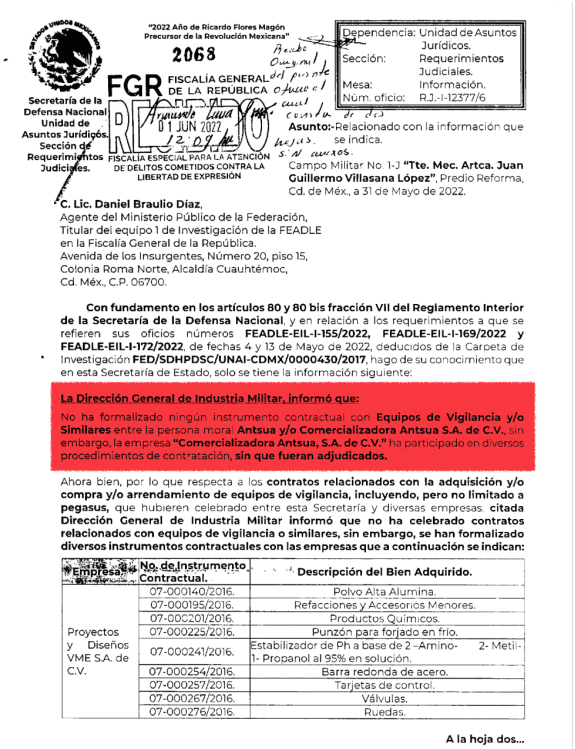
No omito señalar que el contenido de la información solicitada tiene el carácter de confidencial para la Fiscalía General de la República, por lo que su contenido no debe ser divulgado por los servidores públicos, a fin de salvaguardar dicha secrecía que respecto de las actuaciones imponen, por lo que es importante destacar que la transgresión a lo anterior, puede constituir alguno de los ilícitos contemplados en el Código Penal Federal en sus numerales 210, 214 fracción IV y 225 fracción XXVIII.

Haciendo de su conocimiento que las instalaciones que ocupa esta Fiscalía Especial para la Atención de Delitos cometidos contra la Libertad de Expresión, se encuentran ubicadas en Avenida Insurgentes 20, piso 15, Colonia Roma Norte, Delegación Cuauhtémoc, C.P. 06700, Ciudad de México, teléfono (55) 53464238 y correo electrónico daniel.braulio@pgr.gob.mx, datos que proporcionan para cualquier duda o aclaración.

Sin otro particular, en espera de su amable colaboración, le reitero las seguridades de mi atenta y distinguida consideración.

ATENTAMENTE
EL AGENTE DEL MINISTERIO PÚBLICO DE LA FEDERACIÓN, TITULAR DEL EQUIPO 1 DE INVESTIGACIÓN DE LA FEADLE

LIC. DANIEL BRAULIO DIAZ
FISCAL EN JEFE



"2022 Año de Ricardo Flores Magón
Precursor de la Revolución Mexicana"

2068

Secretaría de la Defensa Nacional
Unidad de Asuntos Jurídicos.
Sección de Requerimientos Judiciales.

FGR FISCALÍA GENERAL DE LA REPÚBLICA
FISCALÍA ESPECIAL PARA LA ATENCIÓN DE DELITOS COMETIDOS CONTRA LA LIBERTAD DE EXPRESION

RECIBIDO
01 JUN 2022
12:07 hrs

Dependencia:	Unidad de Asuntos Jurídicos.
Sección:	Requerimientos Judiciales.
Mesa:	Información.
Núm. oficio:	R.J.-I-12377/6

Asunto:-Relacionado con la información que se indica.

Campo Militar No. 1-J **"Tte. Mec. Artca. Juan Guillermo Villasana López"**, Predio Reforma, Cd. de Méx., a 31 de Mayo de 2022.

C. Lic. Daniel Braulio Díaz.
Agente del Ministerio Público de la Federación,
Titular del equipo 1 de Investigación de la FEADLE
en la Fiscalía General de la República.
Avenida de los Insurgentes, Número 20, piso 15,
Colonia Roma Norte, Alcaldía Cuauhtémoc,
Cd. Méx., C.P. 06700.

Con fundamento en los artículos 80 y 80 bis fracción VII del Reglamento Interior de la Secretaría de la Defensa Nacional, y en relación a los requerimientos a que se refieren sus oficios números **FEADLE-EIL-I-155/2022, FEADLE-EIL-I-169/2022 y FEADLE-EIL-I-172/2022**, de fechas 4 y 13 de Mayo de 2022, deducidos de la Carpeta de Investigación **FED/SDHPDSC/UNAI-CDMX/0000430/2017**, hago de su conocimiento que en esta Secretaría de Estado, solo se tiene la información siguiente:

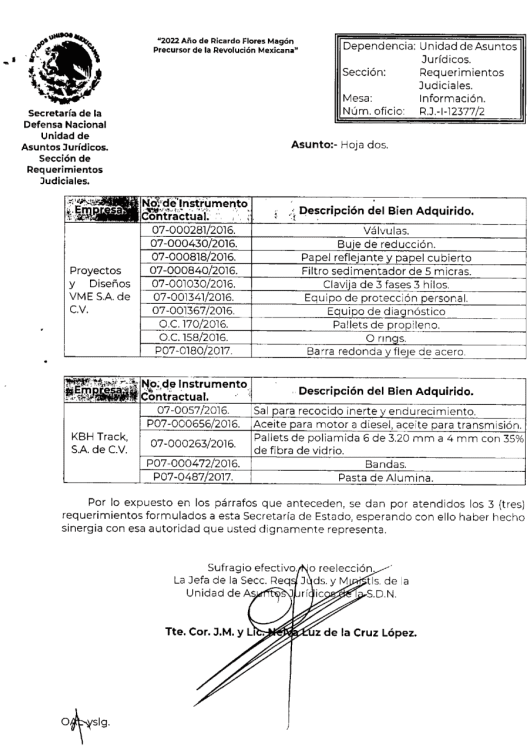
La Dirección General de Industria Militar, informó que:

No ha formalizado ningún instrumento contractual con **Equipos de Vigilancia y/o Similares** entre la persona moral **Antsua y/o Comercializadora Antsua S.A. de C.V.**, sin embargo, la empresa **"Comercializadora Antsua, S.A. de C.V."** ha participado en diversos procedimientos de contratación, **sin que fueran adjudicados.**

Ahora bien, por lo que respecta a los **contratos relacionados con la adquisición y/o compra y/o arrendamiento de equipos de vigilancia, incluyendo, pero no limitado a pegasus,** que hubieren celebrado entre esta Secretaría y diversas empresas **citada Dirección General de Industria Militar informó que no ha celebrado contratos relacionados con equipos de vigilancia o similares, sin embargo, se han formalizado diversos instrumentos contractuales con las empresas que a continuación se indican:**

Empresa	No. de Instrumento Contractual.	Descripción del Bien Adquirido.
Proyectos y Diseños VME S.A. de C.V.	07-000140/2016.	Polvo Alta Alumina.
	07-000195/2016.	Refacciones y Accesorios Menores.
	07-000201/2016.	Productos Químicos.
	07-000225/2016.	Punzón para forjado en frío.
	07-000241/2016.	Estabilizador de Ph a base de 2 -Amino- 2- Metil-1- Propanol al 95% en solución.
	07-000254/2016.	Barra redonda de acero.
	07-000257/2016.	Tarjetas de control.
	07-000267/2016.	Válvulas.
	07-000276/2016.	Ruedas.

A la hoja dos...



"2022 Año de Ricardo Flores Magón
Precursor de la Revolución Mexicana"

Secretaría de la Defensa Nacional
Unidad de Asuntos Jurídicos.
Sección de Requerimientos Judiciales.

Dependencia:	Unidad de Asuntos Jurídicos.
Sección:	Requerimientos Judiciales.
Mesa:	Información.
Núm. oficio:	R.J.-I-12377/2

Asunto:- Hoja dos.

Empresa	No. de Instrumento Contractual.	Descripción del Bien Adquirido.
Proyectos y Diseños VME S.A. de C.V.	07-000281/2016.	Válvulas.
	07-000430/2016.	Buje de reducción.
	07-000818/2016.	Papel reflejante y papel cubierto
	07-000840/2016.	Filtro sedimentador de 5 micras.
	07-001030/2016.	Clavija de 3 fases 3 hilos.
	07-001341/2016.	Equipo de protección personal.
	07-001367/2016.	Equipo de diagnóstico
	O.C. 170/2016.	Pallets de propileno.
	O.C. 158/2016.	O rings.
	P07-0180/2017.	Barra redonda y fleje de acero.

Empresa	No. de Instrumento Contractual.	Descripción del Bien Adquirido.
KBH Track, S.A. de C.V.	07-0057/2016.	Sal para recocido inerte y endurecimiento.
	P07-000656/2016.	Aceite para motor a diesel, aceite para transmisión.
	07-000263/2016.	Pallets de poliamida 6 de 3.20 mm a 4 mm con 35% de fibra de vidrio.
	P07-000472/2016.	Bandas.
	P07-0487/2017.	Pasta de Alumina.

Por lo expuesto en los párrafos que anteceden, se dan por atendidos los 3 (tres) requerimientos formulados a esta Secretaría de Estado, esperando con ello haber hecho sinergia con esa autoridad que usted dignamente representa.

Sufragio efectivo. No reelección.
La Jefa de la Secc. Reqs. Juds. y Minists. de la Unidad de Asuntos Jurídicos de la S.D.N.

Tte. Cor. J.M. y Lic. Nelda Luz de la Cruz López.

O/A-ysIg.

The Army has gone so far as to **deny the submission of information** to the **Superior Audit Office of the Federation**, as indicated in a communication signed by the General Directorate of Audit of Information Technology and Communications, obtained through the documents leaked by the hacktivist group Guacamaya.

In the email, the ASF confirms that the **SEDENA failed to comply** with the requirement to provide "[the] database with information on contracts and amending agreements in force in fiscal years 2019 and 2020 (including multi-year contracts from previous fiscal years), entered into between the SEDENA and Comercializadora Antsua, S.A. de C.V." The Army also failed to comply with the submission of existing contracts, technical annexes and amending agreements, invoices and credit notes that would have applied during fiscal years 2019 and 2020.

8. SEDENA has illegally spied in the past

Despite lacking legal powers to conduct communication surveillance, the **Ministry of National Defense** has carried out such surveillance in the past.

In October 2021, the Commission for Truth and Access to Justice in the Ayotzinapa case (COVAJ) made public that the SEDENA intercepted the communications of several actors involved in the disappearance of the normalista students.

This illegal surveillance was also taken up in the third report of the **Interdisciplinary Group of Independent Experts** (GIEI), presented in February 2022, where it states that the Army "had tapped the communications of relevant actors in the events even when they were occurring".

In fact, both the Report of the Presidency of the Commission for Truth and Access to Justice in the Ayotzinapa Case (COVAJ), published in August 2022, and the fourth report of the GIEI published in September 2022 affirm that the **SEDENA used the Pegasus system indiscriminately to intercept communications**, including those of relatives of the disappeared students.

The GIEI has also accused **SEDENA of continuing to deny that private communications were intercepted** despite the existence of documents in military archives that show such surveillance and that it continues to conceal documents related to surveillance linked to the Ayotzinapa case.

9. There is a link between the work of the people spied on with Pegasus and human rights violations committed by the Armed Forces.

The three individuals who have been spied on with Pegasus between 2019 and 2021 in the documented cases have systematically reported **human rights violations committed by the Armed Forces**, such as forced disappearances, extrajudicial executions, torture, among others.

In the case of **Raymundo Ramos**, his work has focused on reporting and on accompanying victims in Tamaulipas, where there has been an escalation in violence committed by the Army and Navy. Such abuses have also been addressed in journalistic investigations by both Ricardo Raphael and the ***Animal Político*** team.

In the case of **Ricardo Raphael**, the journalist considers that his approach to issues involving the Armed Forces could have led to an interest in spying on him. This includes cases such as the Ayotzinapa case, the coverage of human rights violations in Tamaulipas and the case of General Cienfuegos. The author also does not rule out that the surveillance around the time of the presentation of his book *El hijo de la Guerra* is related to the historical link between former members of the military and the Zetas criminal group.

All three have also been targets of defamation and harassment as a result of their work. Attempts have been made to discredit Raymundo Ramos' human rights work by falsely linking him to organized crime, while *Animal Político* and Ricardo Raphael have been accused without evidence during President López Obrador's morning conferences of addressing issues that are sensitive to the current government.

CONCLUSIONS

From all of the evidence obtained, the following conclusions can be drawn:

1. At least **three journalists and human rights defenders**, whose work and investigations are related to human rights violations committed by the Armed Forces **were spied on with the Pegasus malware** from NSO Group between 2019 and 2021.
2. **Comercializadora Antsua S.A. de C.V.** was authorized to exclusively represent **NSO Group** before the **Ministry of National Defense** from March 2018 to, at least, December 2019. In addition, this company is closely linked to other companies that are proven to have **sold Pegasus** to various federal government agencies during the government of Enrique Peña Nieto.
3. The Ministry of National Defense contracted **a "remote information monitoring system" in April 2019** from Comercializadora Antsua S.A. de C.V.
4. The Ministry of National Defense c**oncealed the existence of this contract** from the Attorney General's Office, the Federal Superior Audit Office and R3D through access to information requests.
5. The army **does not have the authority to intercept private communications of civilians**, however, it has carried out and continues to carry out interceptions of private communications in an illegal manner.
6. In Mexico, **the Army spies**. Multiple indications point to a high degree of probability that it is behind the Pegasus attacks on journalists and human rights defenders documented in this report.