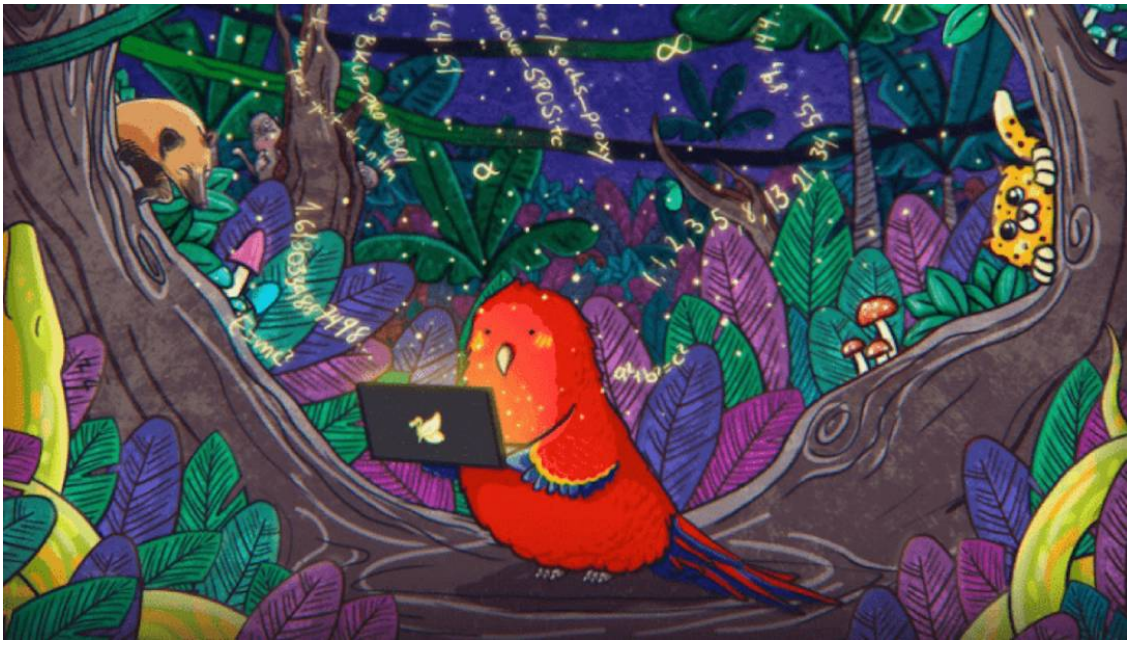
# Internal documents show Mexican army used spyware against civilians

therecord.media/mexican-army-spyware



A still image from one of the unusual hacking videos released by hacktivist group Guacamaya.

## Internal documents show Mexican army used spyware against civilians, set up secret military intelligence unit

*Two digital rights groups, Mexico's R3D and the University of Toronto's Citizen Lab, have just released an update to their "Ejército Espía" ("Spying Government") report from late last year. In October 2022, they revealed that the Mexican army bought spyware and deployed it against at least two Mexican journalists and a human rights advocate between 2019 and 2021. While they had compelling circumstantial evidence, there was no smoking gun. The newly-released internal classified documents appear to prove it.*

*Luis Fernando Garcia, a lawyer and executive director of R3D, told Click Here in an interview that a roster of freedom of information requests and internal Ministry of Defense documents – released as part of last year's massive hack-and-leak operation by the hacktivist group Guacamaya – connect officials at the highest levels of the Mexican army to the purchase of Pegasus spyware. R3D found a 2019 acceptance letter that links the military to a company with the exclusive right to sell licenses for the NSO Group's Pegasus spyware in Mexico.*

*NSO Group created Pegasus in 2011 and it has been linked to everything from the capture of the drug lord El Chapo to the murder of journalist Jamal Khashoggi. Pegasus' super power is its ability to infect smartphones without a user knowing — the phone becomes a spy in their pocket, capturing their location, their communications, and information on their friends.*

*Among the new revelations are documents from the Mexican Secretariat of National Defense , or SEDENA, that discuss a previously unknown military intelligence agency in charge of the nation's surveillance programs. The leaked files show the agency, referred to as CMI or the Military Intelligence Center, spied on a human rights advocate named Raymundo Ramos who has been investigating a suspected extrajudicial killing by the Army that occurred in July 2020 in a border town called Nuevo Laredo.*

*The interview has been edited for space and clarity. A fuller version of the story can be heard on the Click Here podcast.*

**CLICK HERE: For people who don't know, can you explain the mission of R3D (The Digital Rights Defense Network)?**

**LUIS FERNANDO GARCIA:** The Digital Rights Defense Network is a NGO that works on issues related to human rights and technology. Since the beginning we've been working to uncover and to investigate and pushback against the surveillance apparatus in Mexico.

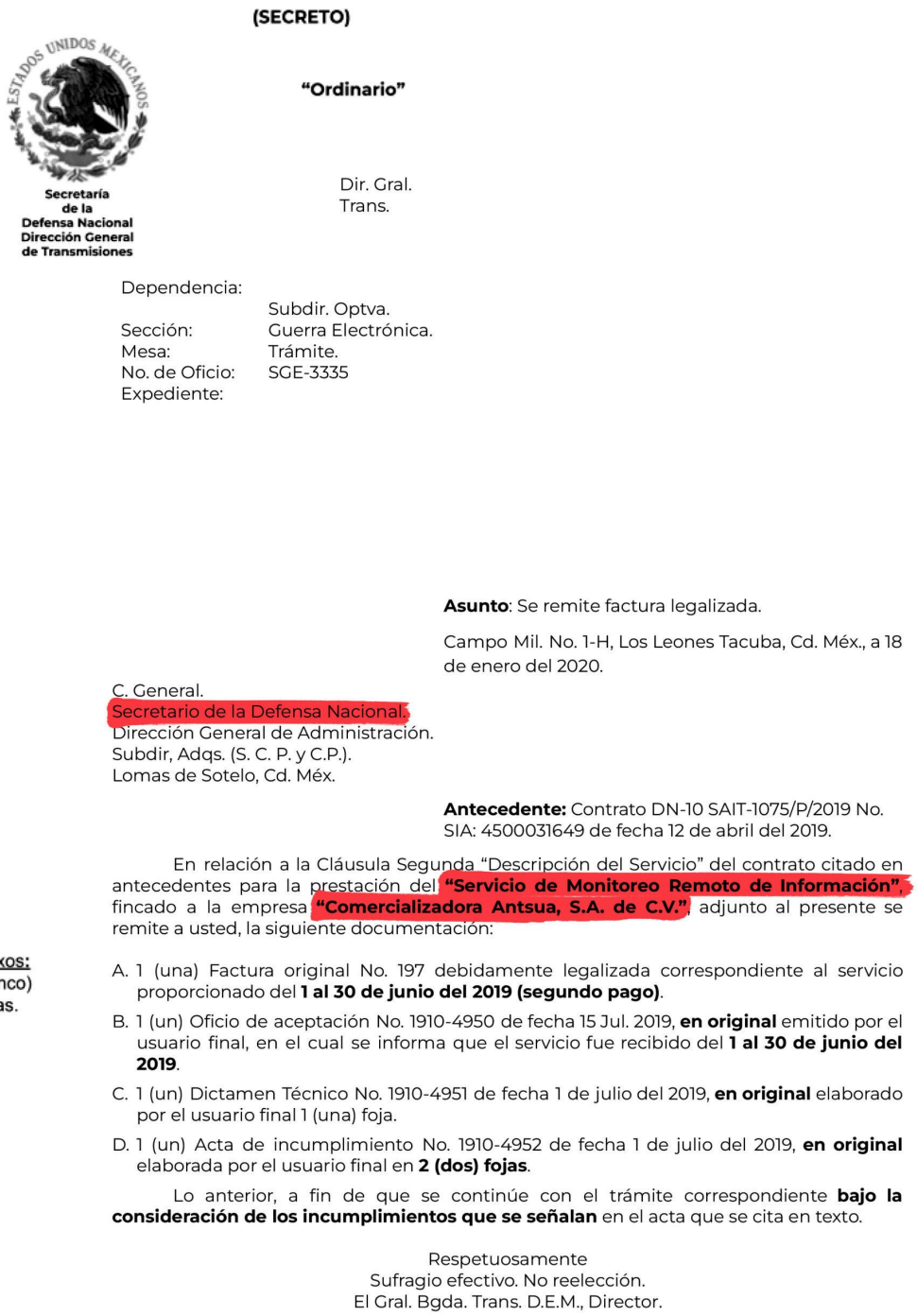
**CH: You started your latest investigation into government surveillance in collaboration with the University of Toronto's Citizen Lab in early 2022. What did the initial investigation [published last October] reveal?**

**LG:** We started checking phones of human rights defenders, journalists, trying to see if we could find forensic evidence of Pegasus in Mexico. We started to document cases of people who were infected in 2019, 2020, and 2021, which means [it was deployed] during the current government, not the previous government.

A week or maybe less from our publication date, something really important happened. The army's email system was hacked and an activist group called Guacamaya was offering access to those emails to media organizations and to human rights organizations. And this gave us like the missing key that we needed to actually point the finger at the army and say we found these Pegasus cases [and connected them to the military].

**CH: Can you talk about some of the specific things you discovered in the Guacamaya documents?**

**LG:** We were able to find a kind of acceptance letter from the army, directed to the secretary, which is the head of the army — the General Secretary of National Defense in Mexico. And here it talks about a contract with Comercializadora Antsua, the same company that we already had a strong suspicion was the intermediary company that was being used by NSO Group to commercialize Pegasus in Mexico. This was proof that the contract existed and the head of the army knew about it because this was a document created for the head of the army.



(SECRETO)

"Ordinario"

Secretaría de la Defensa Nacional
Dirección General de Transmisiones

Dir. Gral.
Trans.

Dependencia: 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.

*An internal military document lays out details of a contract with Comercializadora Antsua, a company that sells licenses to Pegasus spyware in Mexico. (Image: R3D).*

**CH: And did you ever have any concerns that this might be a set-up or that the documents might be fake?**

**LG:** Not at all. The president himself [Andrés Manuel López Obrador] has said that the hack happened, that the documents are real, and we have verified some of the documents ourselves. We found an email directed to the Secretary

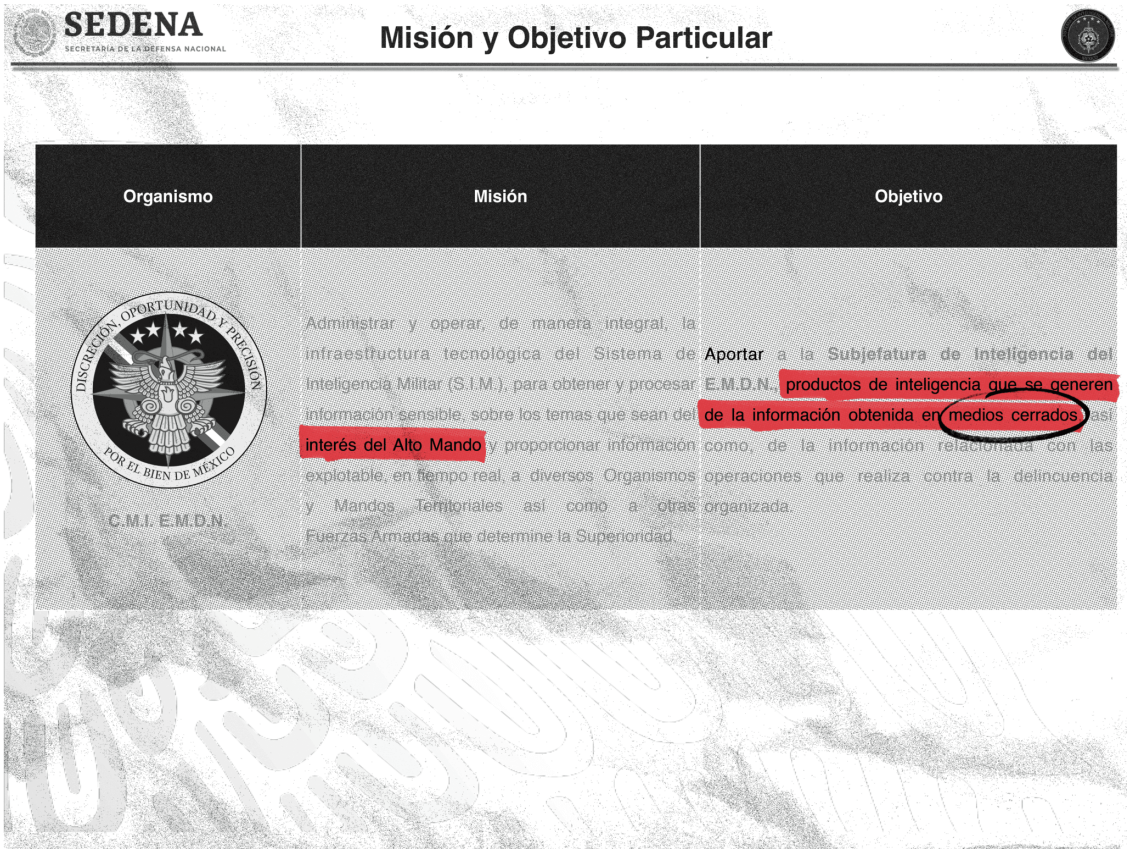
of the Army and we asked about that email through legal means, through an access information request, and they gave us the same email. And it hasn't been disputed by the government or the Army that the documents [in the hack] are fake.

**CH: You'd been working on surveillance issues in Mexico for years, so how did this new information help with your research?**

**LG:** Now we have the number of the contract, the date of the contract, the amount paid for the contract — around 140 million pesos – so that solidifies our belief that the army was actively trying to hide the information related to this and lying to different authorities. [R3D had been requesting this document and they were told it didn't exist.]

**CH: Did you find anything in the documents that was surprising or presented new information entirely?**

**LG:** Yes. We didn't know about [a military intelligence unit called] CMI. If you Google CMI, you are not going to find much of anything. The objective of the CMI, the document says, is to give to the intelligence arm of the chief of staff intelligence products generated from information obtained through closed systems. In other words, it is not open source intelligence – they are talking about communications intercepts. Legally they don't have any powers to do interception of communications of civilians at any point.




*One of the Guacamaya leak documents shows the logo of a previously undisclosed military intelligence unit doing illegal surveillance. (Image: R3D)*

What's more, I looked and I couldn't find any formal, legal establishment of this institution. We did find a document that lays out an analysis of CMI's strengths, opportunities, weaknesses, and threats. One of the threats that they specifically identify is that the activities of this [CMI] center are made public. That's one of the main threats that they identify — that the people know that CMI exists and what it does.

**CH: Meaning they don't want people to know they exist or what they do…**

**LG:** Exactly.

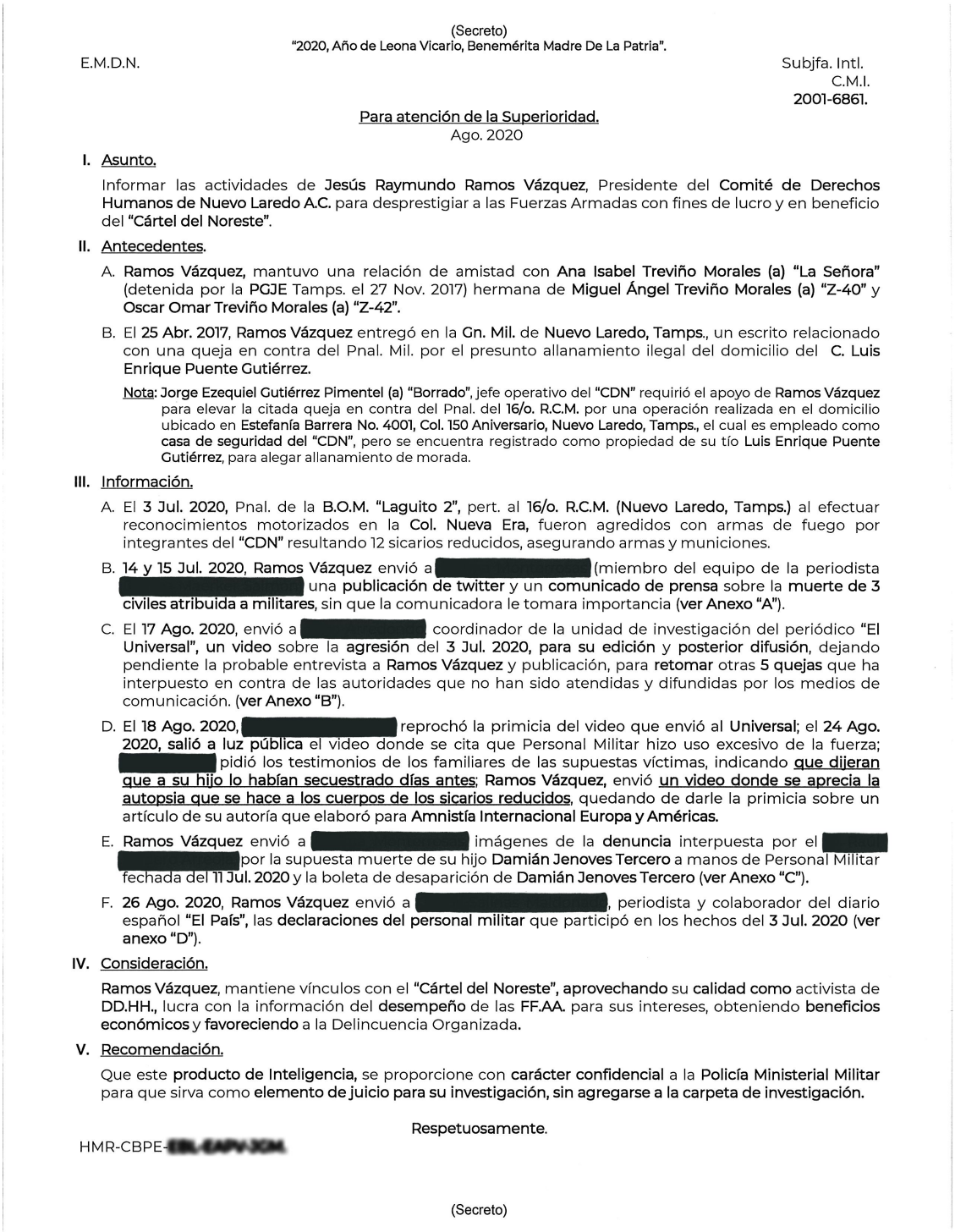
**CH: You found specific surveillance information on a human rights advocate named Raymundo Ramos, tell us about that?**

**LG:** [One of the documents talks] about communications between Raymundo Ramos and journalists around the time a controversial video was released that seemed to capture an extrajudicial killing by the military in [the border town] of Nuevo Laredo.

Ramos was investigating the shooting. All his conversations with journalists at that time were on encrypted apps, so the only way they could have captured the conversations was with something like Pegasus. Espionage carried out by

the Military Intelligence Center is absolutely illegal since the Army lacks the legal authority to intervene in the private communications of civilians.

The document also suggests that the military has secret information that shows Ramos had a relationship with the cartel in Nuevo Laredo. They have never proved anything, and they have never charged him of being involved with the cartels at any point.



(Secreto)
"2020, Año de Leona Vicario, Benemérita Madre De La Patria".

E.M.D.N.

Subjfa. Intl.
C.M.I.
2001-6861.

Para atención de la Superioridad.
Ago. 2020

**I.** Asunto.

Informar las actividades de **Jesús Raymundo Ramos Vázquez**, Presidente del **Comité de Derechos Humanos de Nuevo Laredo A.C.** para desprestigiar a las Fuerzas Armadas con fines de lucro y en beneficio del **"Cártel del Noreste"**.

**II.** Antecedentes.

A. **Ramos Vázquez,** mantuvo una relación de amistad con **Ana Isabel Treviño Morales (a) "La Señora"** (detenida por la **PGJE** Tamps. el 27 Nov. 2017) hermana de **Miguel Ángel Treviño Morales (a) "Z-40"** y **Oscar Omar Treviño Morales (a) "Z-42".**

B. El **25 Abr. 2017, Ramos Vázquez** entregó en la **Gn. Mil.** de **Nuevo Laredo, Tamps.**, un escrito relacionado con una queja en contra del Pnal. Mil. por el presunto allanamiento ilegal del domicilio del **C. Luis Enrique Puente Gutiérrez.**

Nota: **Jorge Ezequiel Gutiérrez Pimentel (a) "Borrado"**, jefe operativo del **"CDN"** requirió el apoyo de **Ramos Vázquez** para elevar la citada queja en contra del Pnal. del **16/o. R.C.M.** por una operación realizada en el domicilio ubicado en **Estefanía Barrera No. 4001, Col. 150 Aniversario, Nuevo Laredo, Tamps.**, el cual es empleado como **casa de seguridad del "CDN"**, pero se encuentra registrado como propiedad de su tío **Luis Enrique Puente Gutiérrez**, para alegar allanamiento de morada.

**III.** Información.

A. El **3 Jul. 2020,** Pnal. de la **B.O.M. "Laguito 2",** pert. al **16/o. R.C.M. (Nuevo Laredo, Tamps.)** al efectuar reconocimientos motorizados en la **Col. Nueva Era,** fueron agredidos con armas de fuego por integrantes del **"CDN"** resultando 12 sicarios reducidos, asegurando armas y municiones.

B. **14 y 15 Jul. 2020, Ramos Vázquez** envió a [redacted] (miembro del equipo de la periodista [redacted] una **publicación de twitter** y un **comunicado de prensa** sobre la **muerte de 3 civiles atribuida a militares,** sin que la comunicadora le tomara importancia (**ver Anexo "A"**).

C. El **17 Ago. 2020,** envió a [redacted] coordinador de la unidad de investigación del periódico **"El Universal", un video** sobre la **agresión** del **3 Jul. 2020, para su edición** y **posterior difusión,** dejando pendiente la probable entrevista a **Ramos Vázquez** y publicación, para **retomar** otras **5 quejas** que ha interpuesto en contra de las autoridades que no han sido atendidas y difundidas por los medios de comunicación. (**ver Anexo "B"**).

D. El **18 Ago. 2020,** [redacted] reprochó la primicia del video que envió al **Universal**; el **24 Ago. 2020, salió a luz pública** el video donde se cita que Personal Militar hizo uso excesivo de la fuerza; [redacted] pidió los testimonios de los familiares de las supuestas víctimas, indicando **que dijeran que a su hijo lo habían secuestrado días antes**; **Ramos Vázquez,** envió **un video donde se aprecia la autopsia que se hace a los cuerpos de los sicarios reducidos**, quedando de darle la primicia sobre un artículo de su autoría que elaboró para **Amnistía Internacional Europa y Américas.**

E. **Ramos Vázquez** envió a [redacted] imágenes de la **denuncia** interpuesta por el [redacted] por la supuesta muerte de su hijo **Damián Jenoves Tercero** a manos de Personal Militar fechada del **11 Jul. 2020** y la boleta de desaparición de **Damián Jenoves Tercero** (**ver Anexo "C"**).

F. **26 Ago. 2020, Ramos Vázquez** envió a [redacted], periodista y colaborador del diario español **"El País",** las **declaraciones del personal militar** que participó en los hechos del **3 Jul. 2020** (**ver anexo "D"**).

**IV.** Consideración.

**Ramos Vázquez**, mantiene vínculos con el **"Cártel del Noreste", aprovechando** su **calidad como** activista de **DD.HH.,** lucra con la información del **desempeño** de las **FF.AA.** para sus intereses, obteniendo **beneficios económicos** y **favoreciendo** a la Delincuencia Organizada.

**V.** Recomendación.

Que este **producto de Inteligencia,** se proporcione con **carácter confidencial** a la **Policía Ministerial Militar** para que sirva como **elemento de juicio para su investigación, sin agregarse a la carpeta de investigación.**

Respetuosamente.

HMR-CBPE-[redacted]

(Secreto)

*An internal military document details the activities of Raymundo Ramos around the time he was found to have been infected with Pegasus spyware.*

But they repeat this accusation and in the document it says that this intelligence product is being given in a confidential manner to the military prosecutor police. So it's considered as an element of judgment in this investigation.

**CH: So connect the dots for us, why is it so important to see Ramos mentioned here? **

**LG:** So we determined last year [with the technical help of Citizen Lab] that Ramos' phone was infected with Pegasus. This document proves that it was the army who was spying on him because they wanted to find out his connection or alleged involvement in the publication of the Nuevo Laredo shooting video that was creating such a headache for the army.

**CH: Some people say the Guacamaya leaks were huge but haven't had the impact that some people had hoped for. Does today's news change that?**

**LG:** I think those assessments are premature. I think the volume of information is so great, it has posed technological challenges to those who might try to sort through the documents. It's not easy to find this information. It's not just control-f search, and you get all these results. You need to do a lot of methodic work and be strategic about what you look for and how.

And it's not only about information that comes from Guacamaya. You need to complement it with your own investigations. And here we have documents that we have obtained through freedom of information requests, forensic analysis that's been done with the help of Citizen Lab. There's a lot of legwork above and beyond the Guacamaya leaks that are part of this story. I don't think I'm the only one. I think there's a lot of people who are taking their time.

- Malware
- Nation-state
- News
- Technology


No previous article

No new articles

## Dina Temple-Raston

Dina Temple-Raston is the host and executive producer of the Click Here podcast as well as a senior correspondent at Recorded Future News. She previously served on NPR's Investigations team focusing on breaking news stories and national security, technology, and social justice and hosted and created the award-winning Audible Podcast "What Were You Thinking."

## Will Jarvis


Will Jarvis is a podcast producer for the Click Here podcast. Before joining Recorded Future News, he produced podcasts and worked on national news magazines at National Public Radio, including Weekend Edition, All Things Considered, The National Conversation and Pop Culture Happy Hour. His work has also been published in The Chronicle of Higher Education, Ad Age and ESPN.