UNIVERSITY OF TORONTO

OFFICE OF THE VICE-PRESIDENT,
RESEARCH AND INNOVATION

May 13, 2022

Confidential

Mr. Jordi Cañas, MEP
Parlement européen
Bât. WILLY BRANDT
05M073
60, rue Wiertz / Wiertzstraat 60
B-1047 Bruxelles/Brussel

Email only: jordi.canas@europarl.europa.eu

Dear Mr. Cañas:

Re: Letter to the University of Toronto - Citizen Lab report "CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru"

I am writing to acknowledge receipt of your correspondence of May 11, 2022, and I am responding on behalf of the University Toronto.

The questions you posed in your letter to the University were put to Citizen Lab, and Professor Deibert's detailed responses to those questions are attached to this letter. Should you have any further questions or comments regarding Professor Deibert's responses, please let me know.

Sincerely,

Professor Lorraine E. Ferris
Associate Vice President, Research Oversight and Compliance

cc:
Professor Ron Deibert, University of Toronto
Mr. Luis Garicano, MEP
President Meric Gertler, University of Toronto
Professor Peter Loewen, University of Toronto
Mr. Alex Matos, University of Toronto

Simcoe Hall, 27 King's College Circle, Room 109, Toronto, ON Canada
Tel: +1 416 978-4984 • Fax: +1 416 971-2647 • www.research.utoronto.ca

Ms. Maite Pagazaurtundúa, MEP
Ms. Susana Solís Pérez, MEP
Ms. María Soraya Rodríguez Ramos, MEP
Mr. Adrián Vázquez Lázara, MEP
Dr. Rachel Zand, University of Toronto

UNIVERSITY OF TORONTO

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

May 13, 2022

Dear Members of the European Parliament,

MEP Jordi Cañas, Cs Europa - Renew Europe

MEP Luis Garicano, Cs Europa - Renew Europe

MEP Susana Solís, Cs Europa - Renew Europe

MEP Adrián Vázquez, Cs Europa - Renew Europe

MEP Soraya Rodríguez, Cs Europa - Renew Europe

MEP Maite Pagazaurtundúa, Cs Europa - Renew Europe

Thank you for your letter dated 11 May 2022. In this communication, you asked us to respond to questions regarding our report titled "CatalanGate: Extensive Mercenary Spyware Operation Against Catalans Using Pegasus and Candiru" (herein referred to as the "**Report**").

We appreciate this opportunity to reassure you that there is no basis for the concerns raised in the letter. The Citizen Lab is an interdisciplinary research laboratory at the Munk School of Global Affairs & Public Policy at the University of Toronto. We have been conducting research at the intersection of human rights and digital technologies for over two decades.

I am the founder and the Principal Investigator at the Citizen Lab. The Citizen Lab employs staff, fellows, and contractors to assist in its research work. As a research laboratory based at the University of Toronto, our work is conducted independently and free of external direction from governments or companies. Where our research engages human subjects, it is conducted pursuant to a research ethics protocol that has been approved by the University of Toronto's Research Ethics Board.

Our research protocols limit the data that we can share without consent from research participants, and we may further limit what data we share to protect participants from reprisals by hostile parties, including governments.

With this context in mind, we have provided answers to the questions that you listed in your communication dated 11 May 2022 below:

munkschool.utoronto.ca

At Trinity College
1 Devonshire Place
Toronto, ON
Canada M5S 3K7
T: 416.946.8900 F: 416.946.8915

At the Observatory
315 Bloor Street West
Toronto, ON
Canada M5S 0A7
T: 416.946.8929 F: 416.946.8877

At the Canadiana Gallery
14 Queen's Park Crescent West
Toronto, ON
Canada M5S 3K9
T: 416.978.5120 F: 416.978.5079

- **Was the "CatalanGate" report peer-reviewed?**

A sample of the victims provided forensic artifacts to Amnesty Tech (which is part of Amnesty International) to validate the technical methods used to identify a Pegasus infection. Amnesty Tech examined the forensic artifacts and concluded that there was evidence of Pegasus infections using their independently developed methodology.

- **Are the results of the forensic analysis replicable? Is there any repository or are there samples that could be used by independent experts to validate the findings?**

The results of the forensic analysis in the Report are replicable given the forensic extractions of the targets' devices. We are constrained in sharing this data without the consent of research participants due to our research ethics protocol.

Sample Sharing: Pegasus & Candiru

Pursuant to our vulnerability disclosure policy, we regularly provide samples to device and operating system manufacturers, and developers, allowing them to secure their users. For example, we shared samples of NSO Group's FORCEDENTRY exploit with Apple in 2021, leading them to issue the iOS 14.8 update, patching the vulnerability. Apple independently attributed the FORCEDENTRY exploit to NSO, and filed a lawsuit against NSO Group stemming from the incident.

Samples that the Citizen Lab shared with Apple have led to the assignment of multiple Common Vulnerabilities and Exposures (CVE) assignments: CVE-2021-30860, CVE-2016-4657, CVE-2016-4655, and CVE-2016-4656.

We also provided samples to Project Zero at Google, which then analyzed and wrote extensively in 2021 and 2022 on NSO Group's FORCEDENTRY exploit. Indeed, beginning with our very first investigations into Pegasus, we shared a sample with Lookout Security in 2016.

Similarly, we shared samples with Microsoft related to Candiru spyware discovered as part of our investigation described in the Report, leading to CVE-2021-31979 and CVE-2021-33771, and updates sent to all Windows devices.

Indicator Publication

The Citizen Lab regularly publishes indicators of compromise from our research, which can be used by experts to validate some of our technical findings. Our reports on NSO Group's Pegasus spyware are summarized in Appendix A. Research groups also regularly work with indicators published in Citizen Lab reports; for example, this 2021 report on Candiru by antivirus company ESET draws on the Citizen Lab's indicators.

Credibility of Testimony

In a recent decision, Sir Andrew McFarlane, the President of the Family Division of the High Court of Justice in England and Wales, accepted the expert testimony of Dr. Bill Marczak regarding the intrusion of certain devices with Pegasus spyware in that litigation. The Court appointed an independent expert, Professor Alastair Beresford, to review Dr. Marczak's findings. He concluded: "The overall approach taken appears sound and I have been able to confirm much of the technical detail." The judge found: "Dr. Marczak was, in short, an impressive witness who presented a detailed, logical account, supported by the core data that he had found, which led to the conclusion that there was strong evidence that the three principal phones [at issue in the litigation] had been hacked by

Pegasus." Dr. Marczak is a Senior Researcher at the Citizen Lab and the developer of the technical methodology used by the Citizen Lab for identifying Pegasus infections or attempted infections.

To date, no reputable technical analysis has contradicted our findings, nor have any specific concerns regarding our technical methodology for identifying Pegasus been substantiated.

- **Is disclosure of potential conflict of interest part of the research ethics protocols at the University of Toronto?**

Disclosure of conflicts of interest is part of the research ethics protocols at the University of Toronto.

- **Did Mr. Elies Campo, the coordinator of the fieldwork in Catalonia, disclose any conflict of interest to the Ethics Research Committee of the University of Toronto?**

As the Principal Investigator under the applicable research ethics protocol, all research work is conducted under my supervision and authority along with that of my co-investigator, Mr. Scott-Railton. While Mr. Campo assisted in coordinating outreach activities in Catalonia, all coordination activities took place under my direction, as well as that of Mr. Scott-Railton, and Mr. Campo did not work independently. There was no conflict of interest raised by Mr. Campo's work with the Citizen Lab and his role was specifically mentioned in the Report.

- **What was the participation of each of the other eight authors of the report in the fieldwork, write up of the report and communication strategy?**

As the Principal Investigator under the applicable research ethics protocol, all technical analysis, drafting, and communications strategy is developed under my direction and authority.

In this case, Dr. Marczak, Mr. Scott-Railton, and Mr. Bahr AbdulRazzak led the technical analysis for the Report. Mr. Campo assisted Mr. Scott-Railton and myself in identifying potential cases and helping to coordinate outreach with potential victims. I further conducted contextual analysis and background research along with Ms. Siena Anstis, and with the research assistance of Mr. Salvatore Solimano. Ms. Gözde Böcü provided further research assistance.

The Report was primarily drafted by Mr. Scott-Railton, Dr. Marczak, Ms. Anstis, and myself, with assistance from the other named authors.

- **When was Mr Elies Campo trusted with the investigation fieldwork in Catalonia?**

Mr. Campo worked with myself and my co-investigator, Mr. Scott-Railton, to provide outreach assistance for the Citizen Lab between 2020 and 2022. Mr. Campo's work was conducted under my supervision, as well as that of my co-investigator, Mr. Scott-Railton.

- **When did fieldwork take place? (could you provide an approximate timeline?)**

Outreach and research activities leading up to the Report began in Fall 2019 and continued until the time of publication.

- **Where were the exploratory and confirmatory forensic analyses of the devices of Catalan politicians conducted?**

To protect the privacy of research participants, I cannot provide information regarding where the technical analysis for the Report was conducted. All analysis was validated by Dr. Marczak.

- **What other institutions or groups were involved in the forensic analysis?**

No other institutions or groups were involved in the forensic analysis conducted for the Report.

As part of the peer review of the report, a sample of victims provided Amnesty Tech with forensic artifacts to validate the Citizen Lab's technical methods used to identify a Pegasus infection. As indicated above, Amnesty Tech examined the forensic artifacts and concluded that there was evidence of Pegasus infections using their independently developed methodology.

- **The report states that at least 65 individuals were targeted or infected by Pegasus or Candiru, but could Citizen Lab reveal how many devices were investigated in total?**

To protect the privacy of research subjects under the applicable research ethics protocol, the Citizen Lab does not typically comment on cases that are not published or publicly disclosed.

- **Did Citizen Lab analyse also devices of non-secessionist leaders or activists?**

To protect the privacy of research subjects under the applicable research ethics protocol, the Citizen Lab does not typically comment on cases that are not published or publicly disclosed.

- **How did you decide the four cases out of 65 positives that were submitted to Amnesty Tech to external validation?**

Cases were selected to include multiple types of indicators (SMS infection attempts, infections), and accommodate Amnesty Tech's research mandate, which focuses on civil society cases.

- **Was Etienne Maynier the person who conducted the external validation at Amnesty Tech?**

The technical analysis conducted by Amnesty Tech was undertaken independently. The Citizen Lab is not aware of the specific individuals who conducted the technical analysis at Amnesty Tech. Further, we note that it has been incorrectly stated that Mr. Maynier was employed or affiliated with Citizen Lab when Amnesty Tech conducted its independent review. Mr. Maynier's fellowship at Citizen Lab ended in April 2021, while the independent review conducted by Amnesty Tech occurred almost one year later in March-April 2022. Furthermore, Mr. Maynier was not involved in the Citizen Lab investigation of these cases at any time.

- **Can Citizen Lab reliably distinguish Pegasus infection attempts from other spywares attacks?**

The Citizen Lab can reliably distinguish Pegasus infection attempts from other spyware attacks.

The Citizen Lab's technical methods for identifying Pegasus infections or infection attempts are supported by six years of published research, as well as independent validations. Our attribution to Pegasus is further bolstered by the decision by Apple to sue NSO Group over the FORCEDENTRY exploit, which we disclosed to Apple and attributed to NSO Group.

We are confident in our ability to distinguish between Pegasus and other infections and infection attempts with other types of spyware. For your reference, we have published technical reports documenting other spyware, such as tools made by vendors like Candiru, Cytrox, FinFisher, Cyberbit, Hacking Team, and many other types of spyware such as Stealth Falcon, DroidJack, Cybergate, XtremeRAT, Netwire, AlienSpy, njRAT, Adzok, PlugX, GH0st RAT, ShadowNet, Conime, Duojeen, GLASSES, cxpid, Enfal, Surtur, Vidgrab, PosionIvy, nAspyUpdate, Revir/IMuler, MacControl, Olyx / Lamdai / PubSab, among others.

- **What type of expertise or skills served as basis for choosing Mr Elies Campo as coordinator of the fieldwork in Catalonia?**

The Citizen Lab regularly works with individuals who are trusted within targeted communities to contact and help coordinate outreach to high-risk groups. No special technical expertise is required for this activity.

As the Principal Investigator under the applicable research ethics protocol, all research work is conducted under my supervision and authority along with that of my co-investigator, Mr. Scott-Railton. While Mr. Campo assisted in coordinating outreach activities in Catalonia, it is incorrect to imply that he was the sole coordinator of these activities. All activities took place under my direction, as well as that of Mr. Scott-Railton.

- **When Citizen Lab trusted field work to Mr Elies Campo, did they already know that he was being monitored by Spanish intelligence services for his alleged implication in several illegal secessionist activities?**

The Citizen Lab only became aware of allegations made against Mr. Campo after the publication of the Report.

- **When did Mr Elies Campo first contact Citizen Lab?**

Mr. Campo first contacted the Citizen Lab in 2020.

- **Did WhatsApp/Microsoft suggest launching a specific investigation about Pegasus in Spain? Why did Citizen Lab choose Spain out of more than 20 countries affected in the spyware attacks revealed by the 2019 WhatsApp dossier?**

No company suggested to the Citizen Lab that it should launch a specific investigation into the use of Pegasus in Spain. The Citizen Lab is an independent research laboratory based at the University of Toronto and it does not take research direction from companies or governments.

The second part of this question is unclear. To our knowledge, there is no such thing as a "2019 WhatsApp dossier."

The 2019 WhatsApp breach by NSO Group's spyware prompted multiple published investigations by the Citizen Lab and other organizations into the use of Pegasus spyware against human rights defenders, civil society and political opposition in multiple countries, including Spain, Togo, and Rwanda, among others. It has also triggered multiple ongoing Citizen Lab investigations. In addition, Citizen Lab has supported victims in multiple other countries to take steps to be more secure online, and when requested by a victim, provided confirmations to the media that the victim was targeted or infected with spyware.

- **In July 2020 when fieldwork in Catalonia began, was Citizen Lab already commissioned by Apple to find evidence for a lawsuit against NSO?**

The Citizen Lab has never been commissioned to find evidence for a lawsuit by any parties to any litigation, including Apple. Under no circumstances would we undertake commissioned research.

- **Has Citizen Lab or its employees received payments or donations from Apple and WhatsApp/Facebook?**

The Citizen Lab has never received payments or donations from Apple, WhatsApp, or Facebook.

Mr. Scott-Railton, in his personal capacity, was paid by Facebook to advise a one-day event on responding to internet infrastructure disruptions held at Facebook in 2016.

- **According to the University of Toronto research ethics code, can external researchers without any contractual or honorary affiliation conduct research on behalf of the University of Toronto or Citizen Lab? If so, would these researchers be bound by the University of Toronto research ethics protocol?**

All researchers with the Citizen Lab are required to follow applicable research ethics protocols.

- **Has Citizen Lab or the Munk School of Global Affairs received any funding, donation, or sponsorship from any Spanish organisation since 2019? If so, could you reveal the origin of such economic support?**

The Citizen Lab has not received any funding from Spanish organizations.

- **How was the fieldwork in Catalonia funded? Was it funded by Citizen Lab or by any other external public or private organisation?**

The Citizen Lab's funding sources are publicly listed on our website. All participation in our research program by victims of Pegasus spyware, and civil society organizations, is voluntary and non-remunerated.

- **How were the professional infographics of the report funded?**

The visual story that accompanied the Report was paid for by the Citizen Lab.

- **Did anyone in Citizen Lab receive any payment or other perks (e.g., free flights, accommodation) from any external organisation not listed in the list of Citizen Lab donors, during the field research in Catalonia?**

No person in the Citizen Lab received payments or other perks from external organizations while conducting research and technical analysis for the Report.

- **Was any Catalan political party (such as *Junts per Catalunya*, ERC or CUP) or secessionist organisations such as, *Assemblea Nacional Catalana* (ANC), *Omnium*, involved in the sampling process or the write up of the report?**

No Catalan political party or secessionist organization was involved in writing the Report or in the technical analysis conducted by the Citizen Lab for this Report.

Pursuant to the research ethics protocol approved by the Research Ethics Board, the Citizen Lab recruits research participants based on a specific criteria and using a snowball sampling methodology. Research participants or

related organizations may refer other persons in the community who they believe meet the research criteria to the Citizen Lab and/or provide some support to community members by helping them share data with the Citizen Lab.

- **Was the research ethics board aware that two Catalan secessionist parties (ERC and Junts per Catalunya) were collecting and filtering the suspicious messages that Mr Elies Campo forwarded to Citizen Lab?**

Pursuant to the research ethics protocol approved by the Research Ethics Board, the Citizen Lab recruits research participants based on a specific criteria and using a snowball sampling methodology. Research participants or related organizations may refer other persons in the community who they believe meet the research criteria to the Citizen Lab and/or provide some support to community members by helping them share data with the Citizen Lab.

- **Was any of these organisations involved in deciding the date of publication date and the communication strategy?**

Along with Citizen Lab staff, we decided to co-time the publication date of the Report with the publication of an article by Ronan Farrow in the *New Yorker*, which had informed us of their publication date. It is standard practice at the Citizen Lab – when it will facilitate public understanding of a case – to co-time a research report with journalistic reporting.

The Citizen Lab's communications strategy was decided by Citizen Lab staff, under my direction.

- **Were Mr. Elies Campo and Mr. John Scott-Railton working on the final report (in 2020) in collaboration with an American communication agency? If so, why did they do so? What is the name of this communication company?**

No research report regarding the use of Pegasus spyware in Spain was written by the Citizen Lab in 2020. The Report was written in 2022.

The Citizen Lab did not collaborate with an "American communication agency" in writing the Report.

- **Did any of these parties or organizations exert pressure on Citizen Lab to name the report "CatalanGate"? (The website "https//CatalanGate.cat" that accuses Spain of this espionage was registered by ANC in January 2022)**

The Citizen Lab took no external direction in naming the Report. I decided, along with staff at the Citizen Lab, to include the term in the title after learning, shortly prior to publication, that victims were using the term to refer to the case.

- **Have you initiated or are you planning to initiate any internal investigation on this report?**

The Citizen Lab's research is conducted under the scope of an approved research ethics protocol. As the Principal Investigator at the Citizen Lab, I – along with the Citizen Lab's researchers – regularly review our research protocols and practices.

- **Where the members of Citizen Lab aware of the allegations published by NY Times, Político, Washington Post, concerning the collaboration of Catalan secessionist leaders with Russian security services when they contacted these same leaders and informed them that Spain may be monitoring their phones?**

The Citizen Lab became aware of these reported allegations in the fall of 2021, after many of the infections described in the Report had been identified and confirmed to victims.

Sincerely,

Professor Ronald J. Deibert
Professor Political Science
Director, The Citizen Lab at the Munk School of Global Affairs & Public Policy,
University of Toronto

Appendix A

Date	Report name	URL	Authors	Excerpt
August 24, 2016	Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender	https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/	Bill Marczak and John Scott-Railton	This report describes how a government targeted an internationally recognized human rights defender, Ahmed Mansoor, with the Trident, a chain of zero-day exploits designed to infect his iPhone with sophisticated commercial spyware.
February 11, 2017	Bitter Sweet: Supporters of Mexico's Soda Tax Targeted	https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/	John Scott-Railton, Bill Marczak, Claudio	This report describes an espionage operation using

	With NSO Exploit Links		Guarnieri, and Masashi Crete-Nishihata	government-exclusive spyware to target Mexican government food scientists and two public health advocates.
June 19, 2017	Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware	https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/	John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert	Uncovering an operation using NSO Group's Pegasus spyware and Trident exploit framework to target Mexican journalists, lawyers, and even a minor child.
June 29, 2017	Reckless Redux: Senior Mexican Legislators and Politicians Targeted with NSO Spyware	https://citizenlab.ca/2017/06/more-mexican-nso-targets/	John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert	NSO Group's Pegasus spyware and exploit framework were used in infection attempts against Mexican senators and senior politicians in June and July 2016.
July 10, 2017	Reckless III: Investigation Into Mexican Mass Disappearance Targeted with NSO Spyware	https://citizenlab.ca/2017/07/mexico-disappearances-nso/	John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert	The international investigation into the 2014 Iguala Mass Disappearance was targeted with infection attempts using spyware developed by the NSO group.
August 2, 2017	Reckless IV: Lawyers for Murdered Mexican Women's Families Targeted with NSO Spyware	https://citizenlab.ca/2017/08/lawyers-murdered-women-nso-group/	John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert	Lawyers representing the families of three slain Mexican women were sent infection attempts with NSO Group's Pegasus spyware after questioning

				official accounts of the killings.
August 30, 2017	Reckless V: Director of Mexican Anti-Corruption Group Targeted with NSO Group's Spyware	https://citizenlab.ca/2017/08/nso-spyware-mexico-corruption/	John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert	Claudio X. González, the director of Mexicanos Contra la Corrupción y la Impunidad (MCCI: Mexicans Against Impunity and Corruption), becomes the 22nd known individual abusively targeted with NSO's spyware technology in Mexico.
July 31, 2018	NSO Group Infrastructure Linked to Targeting of Amnesty International and Saudi Dissident	https://citizenlab.ca/2018/07/nso-spyware-targeting-amnesty-international/	Bill Marczak, John Scott-Railton, and Ron Deibert	Citizen Lab validates Amnesty International investigation showing targeting of staff member and Saudi activist with NSO Group's technology.
September 18, 2018	HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries	https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/	Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert	In this post, we develop new Internet scanning techniques to identify 45 countries in which operators of NSO Group's Pegasus spyware may be conducting operations.
October 1, 2018	The Kingdom Came to Canada: How Saudi-Linked Digital Espionage	https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/	Bill Marczak, John Scott-Railton, Adam Senft,	In this report, we describe how Canadian permanent resident and

	Reached Canadian Soil		Bahr Abdul Razzak, and Ron Deibert	Saudi dissident Omar Abdulaziz was targeted with a fake package delivery notification. We assess with high confidence that Abdulaziz's phone was infected with NSO's Pegasus spyware. We attribute this infection to a Pegasus operator linked to Saudi Arabia.
November 27, 2018	Reckless VI: Mexican Journalists Investigating Cartels Targeted with NSO Spyware Following Assassination of Colleague	https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague/	John Scott-Railton, Bill Marczak, Siena Anstis, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert	Two days after the murder of award-winning Mexican journalist Javier Valdez Cárdenas, two of his colleagues began receiving text messages laden with NSO Group's Pegasus spyware. To date, 24 targets of Pegasus have been identified in Mexico. This case additionally illustrates an alarming trend of spyware attacks around the world specifically aimed at journalists.
March 20, 2019	Reckless VII: Wife of Journalist Slain in Cartel-Linked Killing Targeted with NSO Group's Spyware	https://citizenlab.ca/2019/03/nso-spyware-slain-journalists-wife/	John Scott-Railton, Bill Marczak, Siena Anstis, Bahr Abdul Razzak, Masashi	This research brief details how Griselda Triana, journalist and the wife of slain journalist Javier Valdez Cárdenas, was

			Crete-Nishihata, and Ron Deibert	targeted with NSO Group's Pegasus spyware in the days after his killing.
January 28, 2020	Stopping the Press: New York Times Journalist Targeted by Saudi-linked Pegasus Spyware Operator	https://citizenlab.ca/2020/01/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator/	Bill Marczak, Siena Anstis, Masashi Crete-Nishihata, John Scott-Railton, and Ron Deibert	New York Times journalist Ben Hubbard was targeted with NSO Group's Pegasus spyware via a June 2018 SMS message promising details about "Ben Hubbard and the story of the Saudi Royal Family." The SMS contained a hyperlink to a website used by a Pegasus operator that we call KINGDOM. We have linked KINGDOM to Saudi Arabia. In 2018, KINGDOM also targeted Saudi dissidents including Omar Abdulaziz, Ghanem al-Masarir, and Yahya Assiri, as well as a staff member at Amnesty International.
August 3, 2020	Nothing Sacred: Religious and Secular Voices for Reform in Togo Targeted with NSO Spyware	https://citizenlab.ca/2020/08/nothing-sacred-nso-sypware-in-togo/	John Scott-Railton, Siena Anstis, Sharly Chan, Bill Marczak, and Ron Deibert	Amidst calls for reform in Togo, NSO Group's spyware was used to target voices for change including a bishop, priest, and opposition politicians.

December 20, 2020	The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit	https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/	Bill Marczak, John Scott-Railton, Noura Al-Jizawi, Siena Anstis, and Ron Deibert	Government operatives used NSO Group's Pegasus spyware to hack 36 personal phones belonging to journalists, producers, anchors, and executives at Al Jazeera. The journalists were hacked by four Pegasus operators, including one operator MONARCHY that we attribute to Saudi Arabia, and one operator SNEAKY KESTREL that we attribute to the United Arab Emirates.
July 18, 2021	Independent Peer Review of Amnesty International's Forensic Methods for Identifying Pegasus Spyware	https://citizenlab.ca/2021/07/amnesty-peer-review/	Bill Marczak, John Scott-Railton, Siena Anstis, and Ron Deibert	Forbidden Stories and Amnesty International requested that the Citizen Lab undertake an independent peer review of a sample of their forensic evidence and their general forensic methodology. We were provided with iTunes backups of several devices and a separate methodology brief, and independently validated that Amnesty

				International's forensic methodology correctly identified infections with NSO's Pegasus spyware.
August 24, 2021	From Pearl to Pegasus: Bahraini Government Hacks Activists with NSO Group Zero-Click iPhone Exploits	https://citizenlab.ca/2021/08/bahrain-hacks-activists-with-nso-group-zero-click-iphone-exploits/	Bill Marczak, Ali Abdulemam, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, John Scott-Railton, and Ron Deibert	We identified nine Bahraini activists whose iPhones were successfully hacked with NSO Group's Pegasus spyware between June 2020 and February 2021. The hacked activists included three members of Waad (a secular Bahraini political society), three members of the Bahrain Center for Human Rights, two exiled Bahraini dissidents, and one member of Al Wefaq (a Shiite Bahraini political society).
September 13, 2021	FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild	https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/	Bill Marczak, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, and Ron Deibert	While analyzing the phone of a Saudi activist infected with NSO Group's Pegasus spyware, we discovered a zero-day zero-click exploit against iMessage. The exploit, which we call FORCEDENTRY, targets Apple's

				image rendering library, and was effective against Apple iOS, MacOS and WatchOS devices.
October 24, 2021	Breaking the News: New York Times Journalist Ben Hubbard Hacked with Pegasus after Reporting on Previous Hacking Attempts	https://citizenlab.ca/2021/10/breaking-news-new-york-times-journalist-ben-hubbard-pegasus/	Bill Marczak, John Scott-Railton, Siena Anstis, Bahr Abdul Razzak, and Ron Deibert	Our forensic analysis of two iPhones belonging to Hubbard found evidence of Pegasus infections in July 2020 and June 2021. Notably, these infections occurred after Hubbard reported in January 2020 that we found that he was targeted in 2018 by the Saudi Arabia-linked Pegasus operator that we call KINGDOM.
December 16, 2021	Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware	https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/	By Bill Marczak, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, and Ron Deibert	Two Egyptians—exiled politician Ayman Nour and the host of a popular news program (who wishes to remain anonymous)—were hacked with Predator spyware, built and sold by the previously little-known mercenary spyware developer Cytrox. The phone of Ayman Nour was simultaneously infected with both Cytrox's Predator

				and NSO Group's Pegasus spyware, operated by two different government clients.
January 12, 2022	Project Torogoz: Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware	https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/	By John Scott-Railton, Bill Marczak, Paolo Nigro Herrero, Bahr Abdul Razzak, Noura Al-Jizawi, Salvatore Solimano, and Ron Deibert	We confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. We shared a sample of forensic data with Amnesty International's Security Lab which independently confirms the findings.
February 18, 2022	Pearl 2 Pegasus: Bahraini Activists Hacked with Pegasus Just Days after a Report Confirming Other Victims	https://citizenlab.ca/2022/02/bahraini-activists-hacked-with-pegasus/	By Bill Marczak, Ali Abdulemam, John Scott-Railton, Bahr Abdul Razzak, Siena Anstis, Noura Al-Jizawi, and Ron Deibert	Our forensic analysis confirms that phones belonging to three individuals in Bahrain were hacked in 2021 with NSO Group's Pegasus spyware. Two have consented to be named.
April 5, 2022	Peace through Pegasus: Jordanian Human Rights Defenders and Journalists Hacked with Pegasus Spyware	https://citizenlab.ca/2022/04/peace-through-pegasus-jordanian-human-rights-defenders-and-journalists-hacked-with-pegasus-spyware/	By Mohammed Al-Maskati, Bill Marczak, Siena Anstis, and Ron Deibert	Phones belonging to four Jordanian human rights defenders, lawyers, and journalists were hacked with NSO Group's Pegasus

				spyware between August 2019 and December 2021.
April 18, 2022	CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru	https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/	By John Scott-Railton, Elies Campo, Bill Marczak, Bahr Abdul Razzak, Siena Anstis, Gözde Böcü, Salvatore Solimano, and Ron Deibert	The Citizen Lab, in collaboration with Catalan civil society groups, has identified at least 65 individuals targeted or infected with mercenary spyware. At least 63 were targeted or infected with Pegasus, and four others with Candiru. At least two were targeted or infected with both.