PEGASUS and the Killing of Jamal Khashoggi

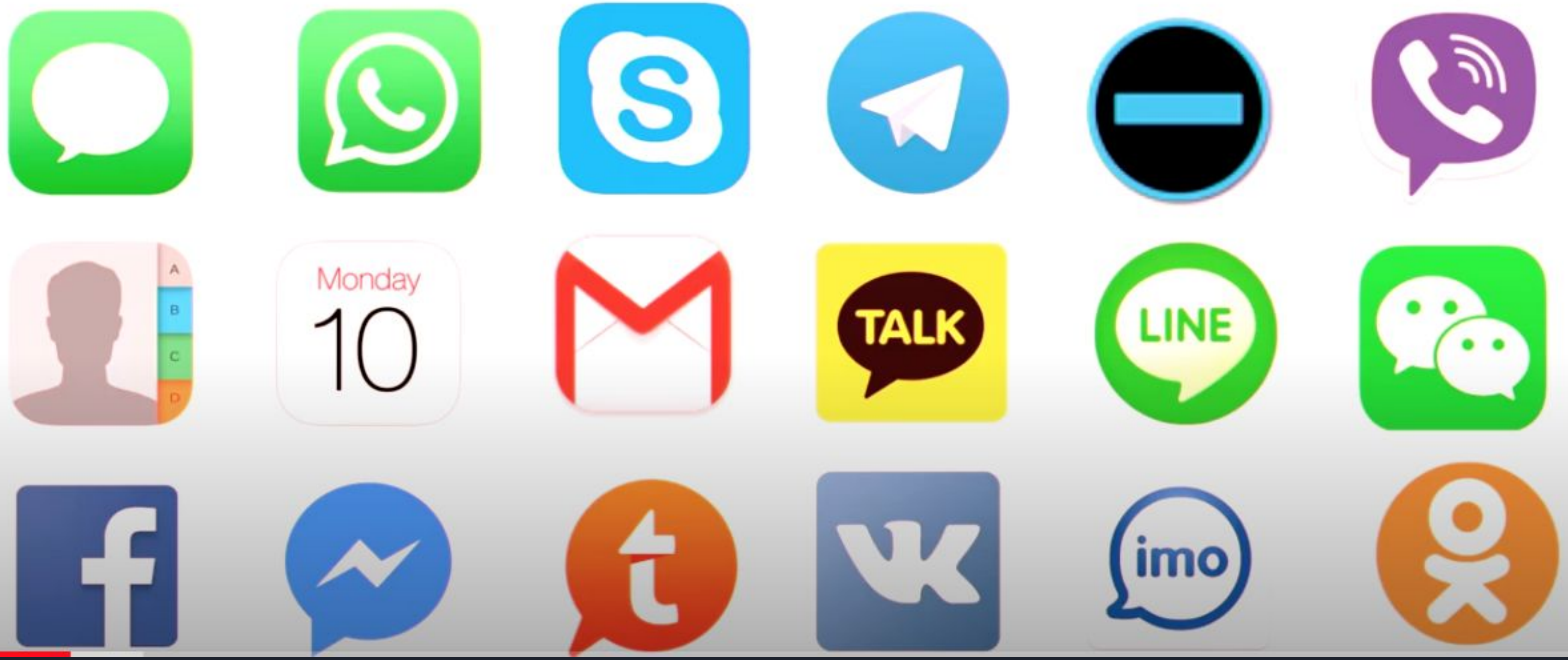
Ariel Allensworth
Phillip Garver
Laura Lamoureux
Fayick Suleman

IST 623
Summer 2020

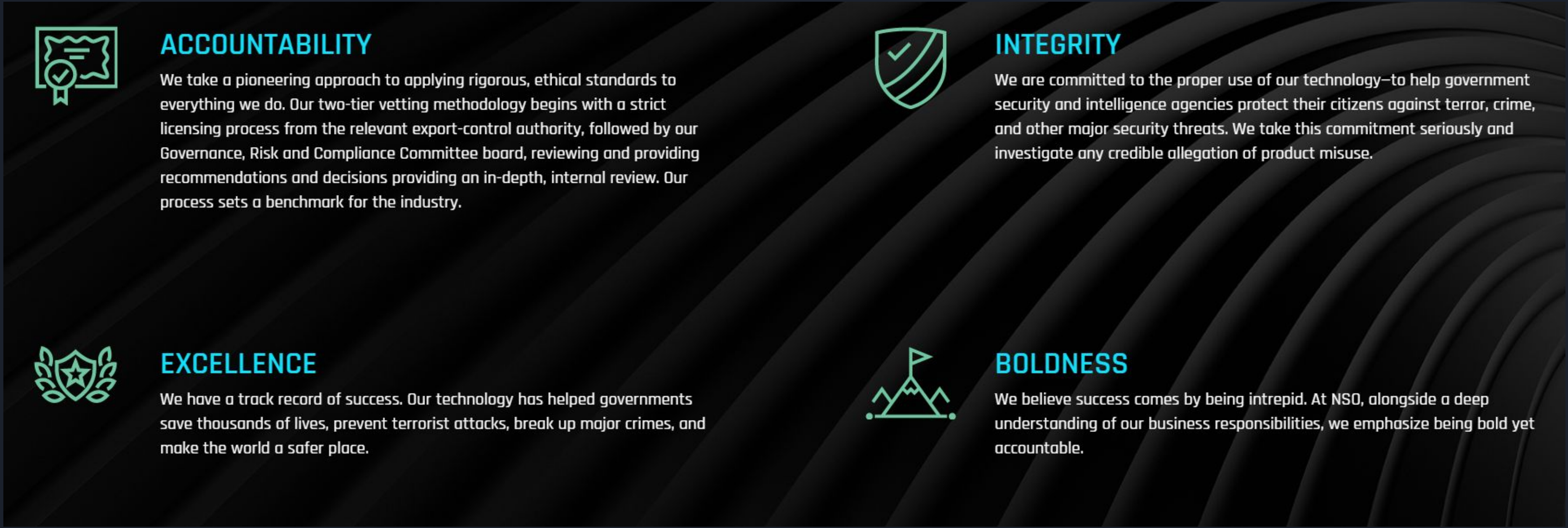
Background & History

- NSO Group
  - “Developing Technology to Prevent and Investigate Terror and Crime”
  - Went up for sale in 2017 for $1 Billion (sold back to original owners)
- International Customers
  - Mexican Government
  - Panamanian Government
  - Saudi Arabian Government
  - *attempted to sell services to U.S. Secret Service
- Jamal Khashoggi
  - Saudi Arabian dissident
  - Washington Post journalist
  - Inner circle was targeted (allegedly)

Targeted apps



NSO Group - Values



ACCOUNTABILITY

We take a pioneering approach to applying rigorous, ethical standards to everything we do. Our two-tier vetting methodology begins with a strict licensing process from the relevant export-control authority, followed by our Governance, Risk and Compliance Committee board, reviewing and providing recommendations and decisions providing an in-depth, internal review. Our process sets a benchmark for the industry.

INTEGRITY

We are committed to the proper use of our technology–to help government security and intelligence agencies protect their citizens against terror, crime, and other major security threats. We take this commitment seriously and investigate any credible allegation of product misuse.

EXCELLENCE

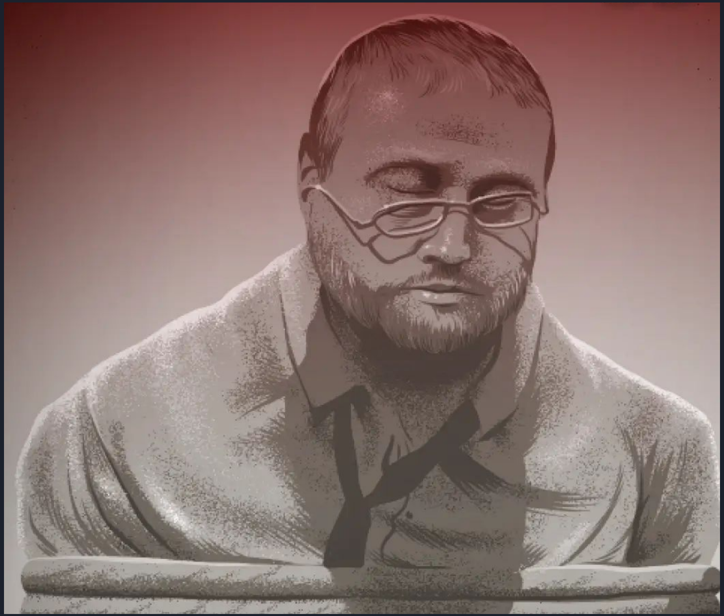
We have a track record of success. Our technology has helped governments save thousands of lives, prevent terrorist attacks, break up major crimes, and make the world a safer place.

BOLDNESS

We believe success comes by being intrepid. At NSO, alongside a deep understanding of our business responsibilities, we emphasize being bold yet accountable.

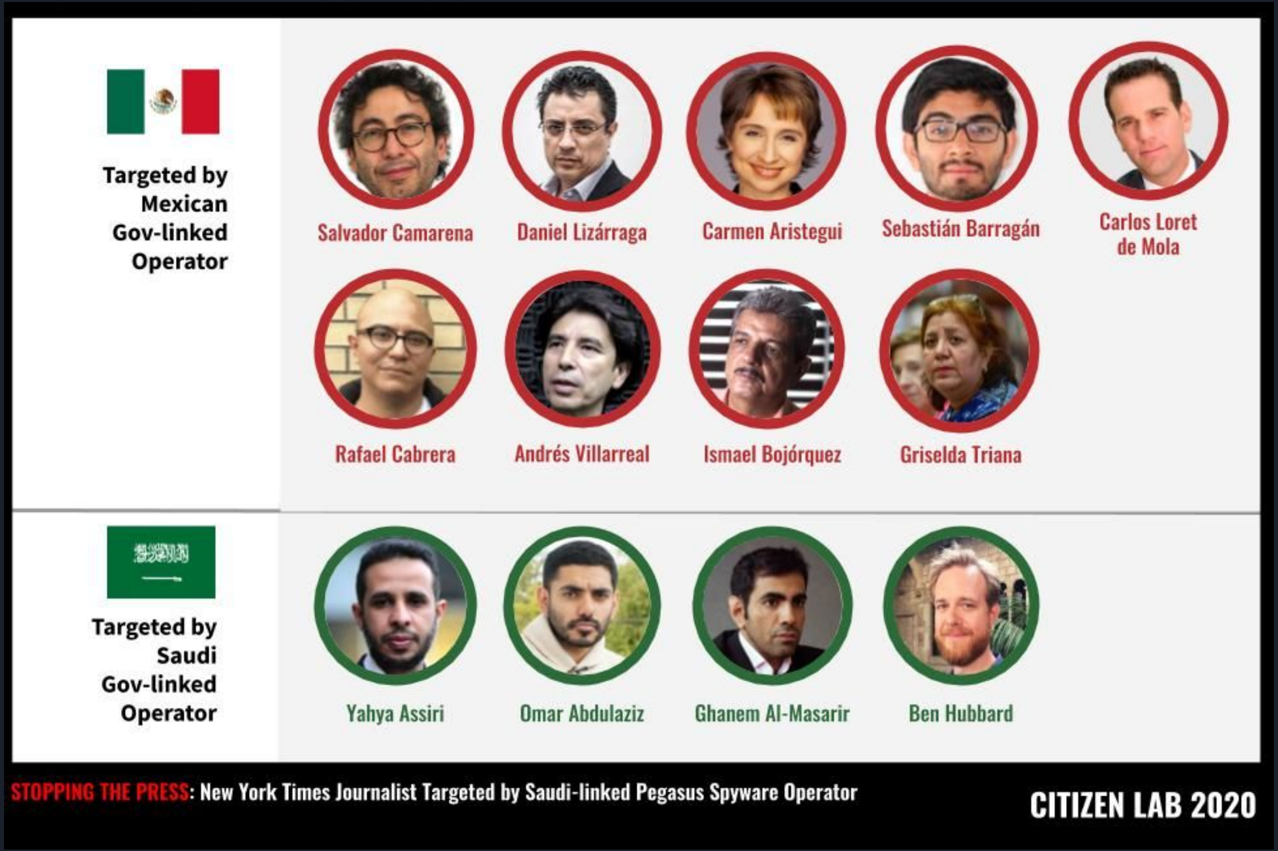
NSO Group. (2020). About Us. Retrieved August 20, 2020, from https://www.nsogroup.com/about-us/

Pegasus and Jamal Khashoggi

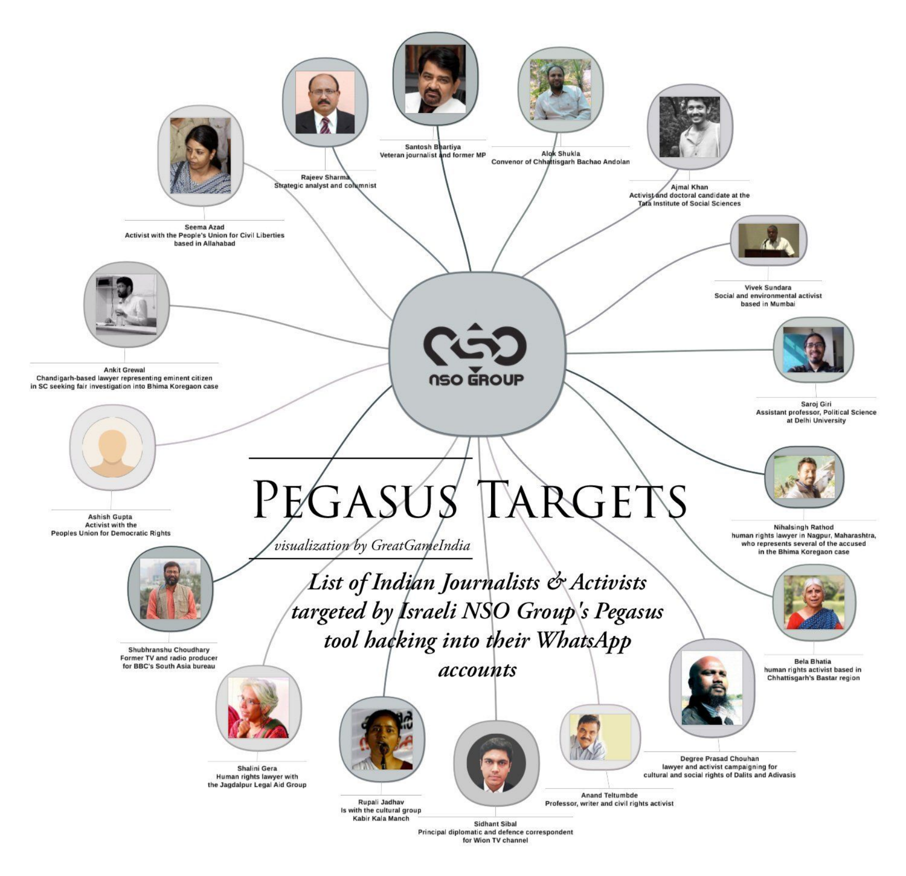


The Broader Overview

- ➔ Jamal BEFORE the Incident
- ➔ Lead-Up to the Incident
- ➔ The Incident Itself
- ➔ Follow-Up to the Incident
- ➔ The Continuing Story



JOURNALISTS AND MEDIA PERSONALITIES FROM MEXICO AND SAUDI ARABIA



Pegasus Targets

visualization by GreatGameIndia

List of Indian Journalists & Activists targeted by Israeli NSO Group's Pegasus tool hacking into their WhatsApp accounts

NSO GROUP

Seema Azad
Activist with the People's Union for Civil Liberties
based in Allahabad

Rajeev Sharma
Strategic analyst and columnist

Santosh Bhartiya
Veteran journalist and former MP

Alok Shukla
Convenor of Chhattisgarh Bachao Andolan

Ajmal Khan
Activist and doctoral candidate at the
Tata Institute of Social Sciences

Vivek Sundara
Social and environmental activist
based in Mumbai

Ankit Grewal
Chandigarh-based lawyer representing eminent citizen
in SC seeking fair investigation into Bhima Koregaon case

Saroj Giri
Assistant professor, Political Science
at Delhi University

Ashish Gupta
Activist with the
Peoples Union for Democratic Rights

Nihalsingh Rathod
human rights lawyer in Nagpur, Maharashtra,
who represents several of the accused
in the Bhima Koregaon case

Shubhranshu Choudhary
Former TV and radio producer
for BBC's South Asia bureau

Bela Bhatia
human rights activist based in
Chhattisgarh's Bastar region

Shalini Gera
Human rights lawyer with
the Jagdalpur Legal Aid Group

Rupali Jadhav
Is with the cultural group
Kabir Kala Manch

Sidhant Sibal
Principal diplomatic and defence correspondent
for Wion TV channel

Anand Teltumbde
Professor, writer and civil rights activist

Degree Prasad Chouhan
lawyer and activist campaigning for
cultural and social rights of Dalits and Adivasis

JOURNALISTS AND ACTIVISTS FROM INDIA

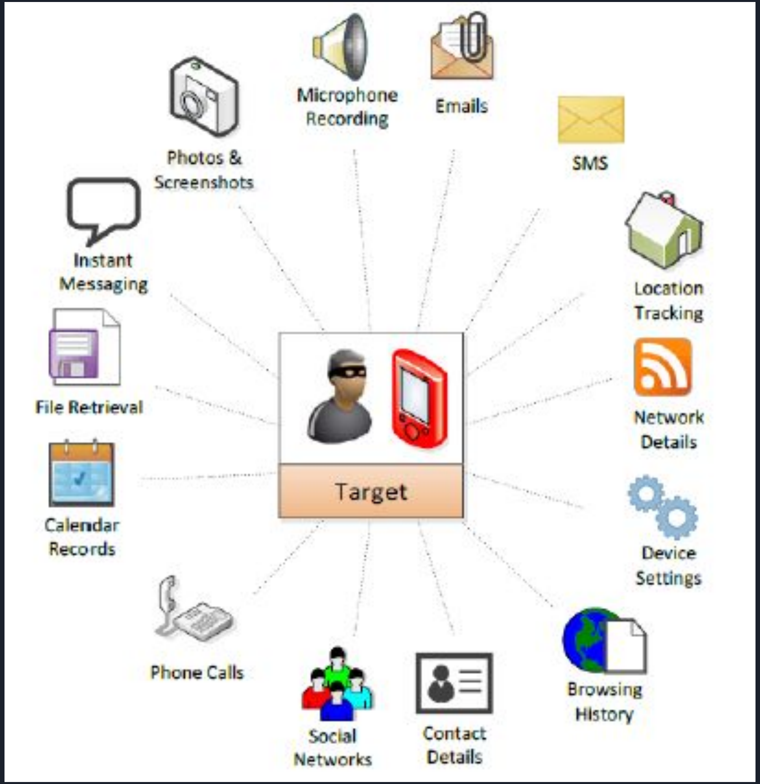
“When you find a Pegasus target, you find the fingerprints of a government.”

CITIZEN LAB RESEARCHER:
JOHN SCOTT-RAILTON

Pegasus Operation and Exploitation

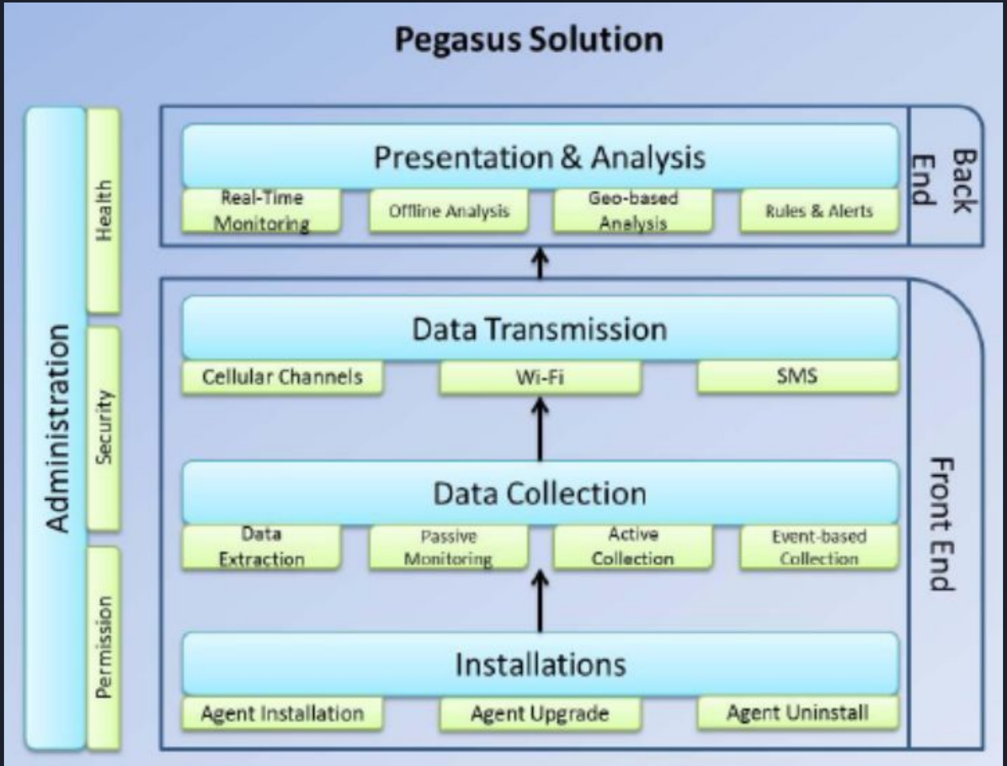
Mobile Intelligence/ Data Collection/Key Features

- User/Device Data
- Remotely Installed and Controlled
- Front-End Automation with Back-End Control
- Security threat/Stealth/Self destruct
- Highly sophisticated malware
- Multiple modes of installation
- IOS vs WhatsApp



Bazaliy, M., Flossman, M., Blaich, A., Hardy, S., Edwards, K., & Murray, M. (2017). *Technical Analysis of Pegasus Spyware* (Rep.). Retrieved August 3, 2020, from https://www.lookout.com/trident-pegasus-enterprise-discovery

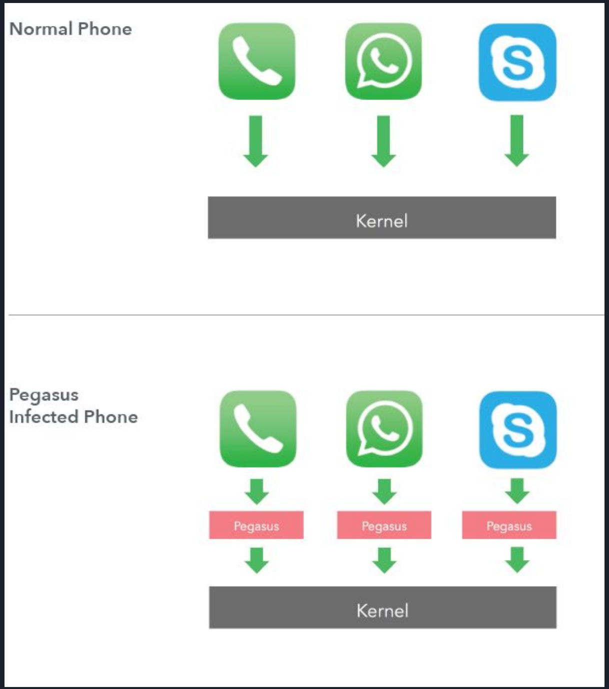
- Complete surveillance infrastructure
- Capable of self-administration and remote control
- Full package administration
- Flexible collection posture
- Flexible data transmission options



Alliance), C. (2020, January 01). NSO Pegasus. Retrieved August 03, 2020, from https://www.documentcloud.org/documents/4599753-NSO-Pegasus.html

iOS Example

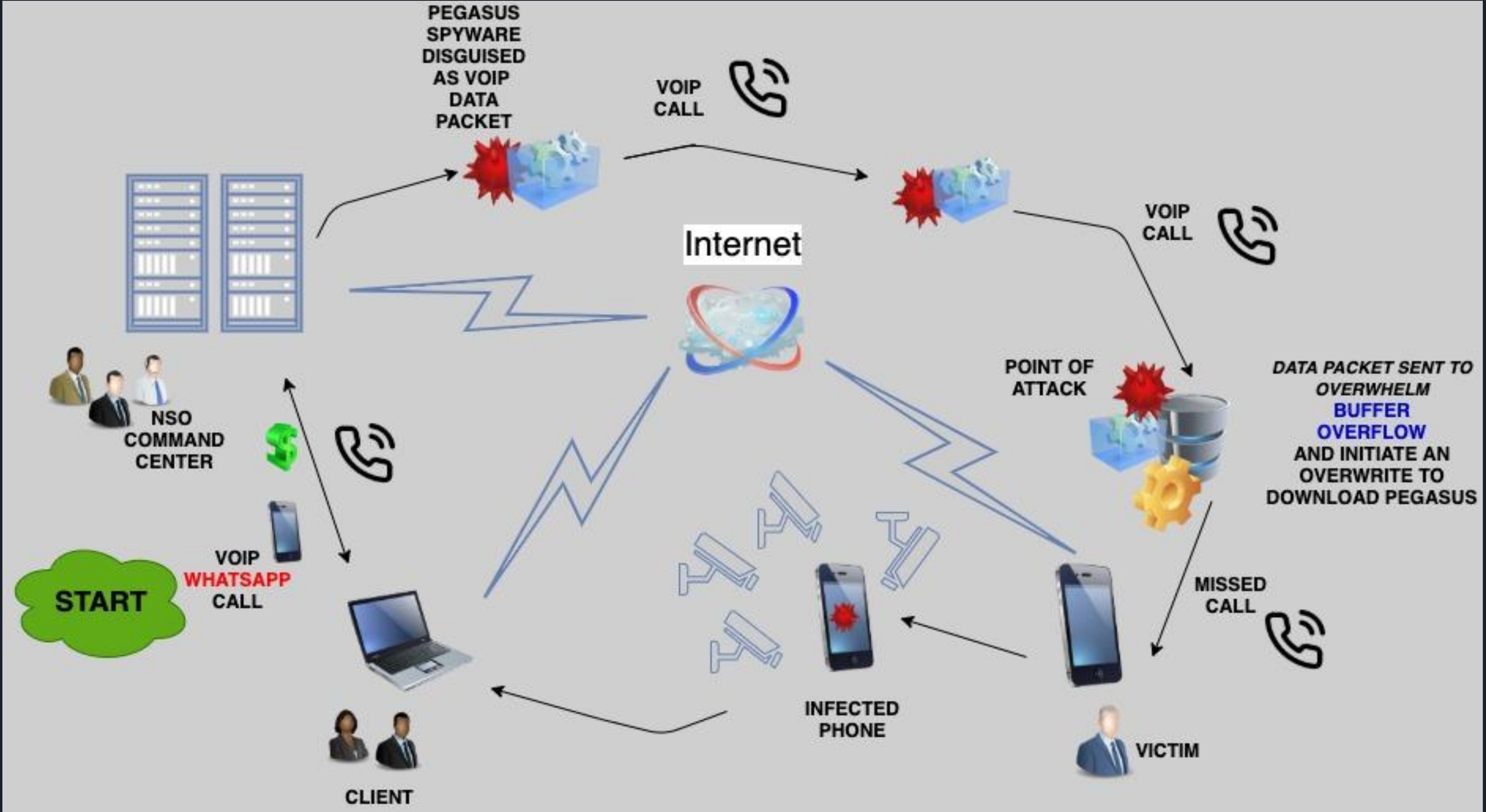
- Trident Vulnerabilities (iOS Specific)
  - Memory Corruption in Safari (allows arbitrary code execution)
  - Leaked Kernel Memory Location
  - Kernel Memory Corruption (allows jailbreak)
- User clicks the link
- Agent is installed
- Device is monitored



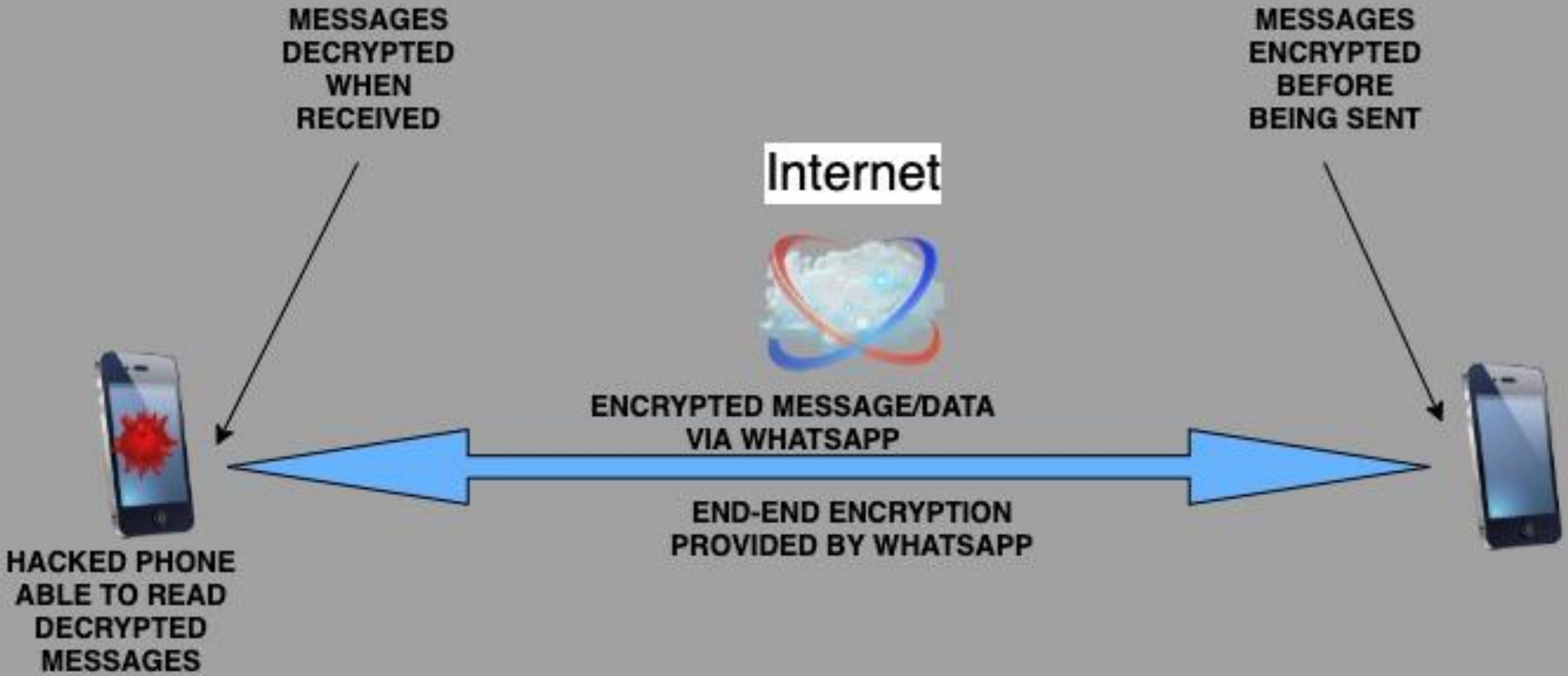
Bazaliy, M., Flossman, M., Blaich, A., Hardy, S., Edwards, K., & Murray, M. (2017). *Technical Analysis of Pegasus Spyware* (Rep.). Retrieved August 3, 2020, from https://www.lookout.com/trident-pegasus-enterprise-discovery

PEGASUS WHATSAPP ATTACK

- Over 1.5 billion users (size of Africa and Europe)
- Very popular in developing countries
- Facebook is the parent company
- Notable for its end-to-end encryption
- Most recent attack 2019
- 1400 affected mostly in India
- Attack is based on vulnerabilities in VoIP (Voice over Internet Protocol) calling system
- Buffer overflow attack overwhelms data holding cell of apps to cause a spill over of data into other parts of memory giving attackers a foothold to gain control of the system
- No social engineering


PEGASUS SPYWARE DISGUISED AS VOIP DATA PACKET
VOIP CALL
VOIP CALL
Internet
NSO COMMAND CENTER
POINT OF ATTACK
DATA PACKET SENT TO OVERWHELM BUFFER OVERFLOW AND INITIATE AN OVERWRITE TO DOWNLOAD PEGASUS
START
VOIP WHATSAPP CALL
MISSED CALL
INFECTED PHONE
VICTIM
CLIENT

WHATSAPP
END-END
ENCRPTION



MESSAGES DECRYPTED WHEN RECEIVED

MESSAGES ENCRYPTED BEFORE BEING SENT

Internet

ENCRYPTED MESSAGE/DATA VIA WHATSAPP

END-END ENCRYPTION PROVIDED BY WHATSAPP

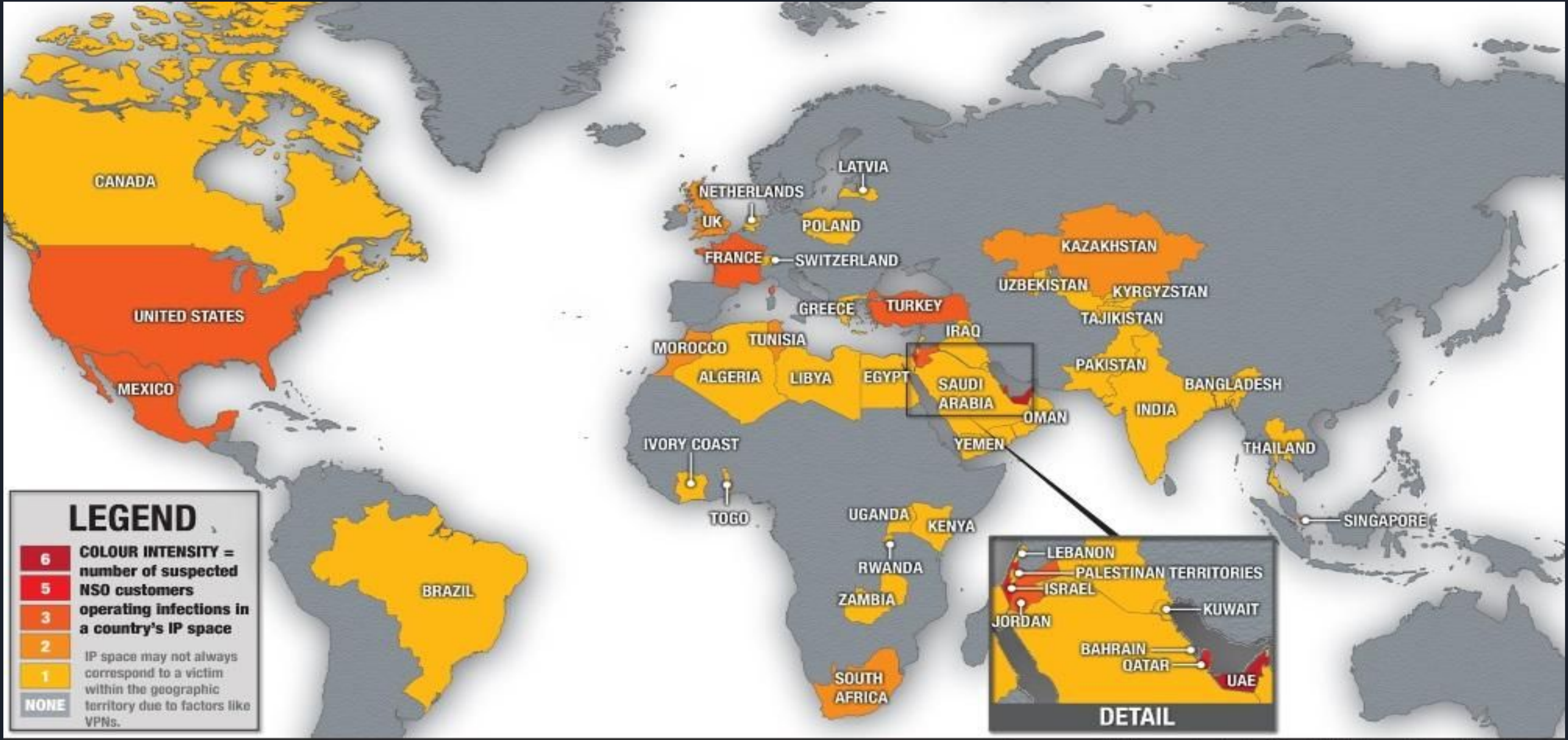
HACKED PHONE ABLE TO READ DECRYPTED MESSAGES

Security & Privacy Challenges

- Difficult to find infected devices
- Difficult to trace Pegasus servers (can self destroy)
- Monitoring is silent (stealth capabilities)
- Government abuse

NSO & Pegasus Updates

- Where is Pegasus today?
- Other targets?
- Journalism, Governments, Defectors, and Advocates



SUSPECTED PEGASUS INFECTIONS

A GLOBAL MAP MADE WITH DNS CACHE PROBING

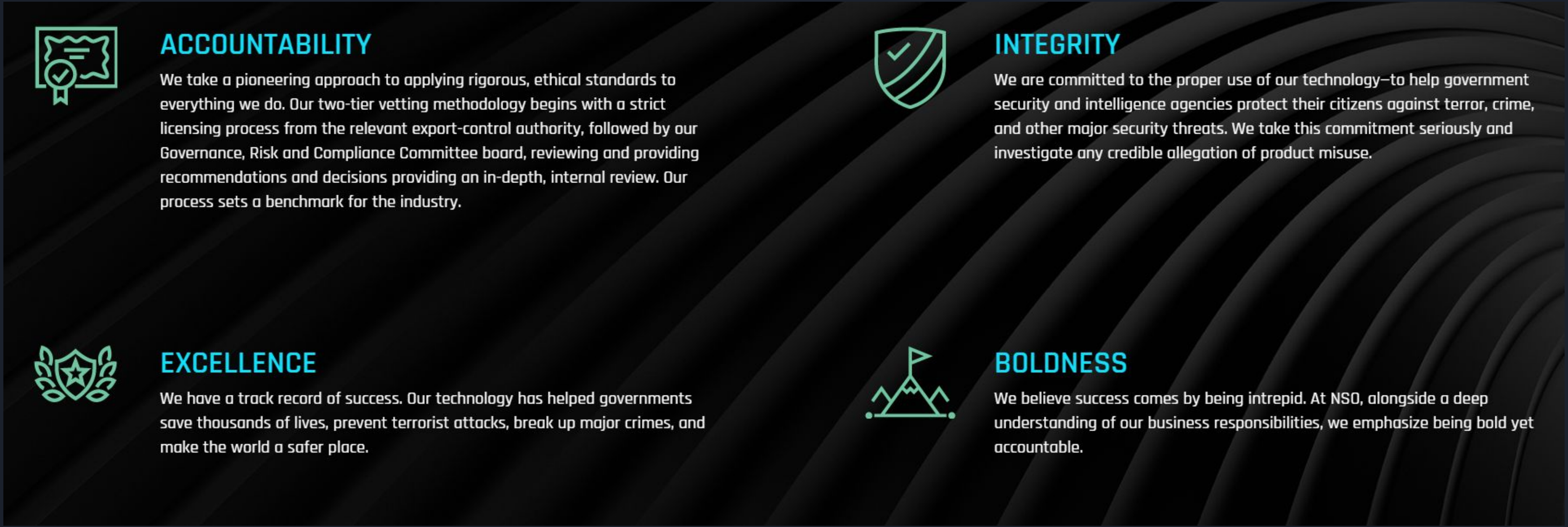
Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak & Ron Deibert

CITIZEN LAB 2018

Pegasus Related Events in 2020

- **January 2020** - Israeli Judge refuses dismissal of NSO Group suit filed by Omar Abdulaziz, and for NSO Group to pay a portion of his legal expenses
- **March 2020** - NSO Group files motion for immunity to Facebook's lawsuit alleging breach of anti-hacking laws in the United States
- **May 2020** - News investigation claims NSO Group 'impersonated' Facebook to install Pegasus spyware using servers located in the U.S.
- **June 2020** - S.3905 Intelligence Authorization Act for Fiscal Year 2021
- **July 2020** - Israeli Court refuses to force NSO Group to stop selling software to 'rights abusers'
- **July 2020** - Citizen Lab confirms Speaker of Catalan Regional Parliament targeted by Pegasus
- **July 2020** - U.S. federal court judge rules that WhatsApp Facebook's lawsuit against NSO Group can go forward
- **July 2020** - Trial begins in Turkey of 20 Saudis accused of collaborating in the death of Khashoggi, now adjourned until November 24th

NSO Group - Values



ACCOUNTABILITY

We take a pioneering approach to applying rigorous, ethical standards to everything we do. Our two-tier vetting methodology begins with a strict licensing process from the relevant export-control authority, followed by our Governance, Risk and Compliance Committee board, reviewing and providing recommendations and decisions providing an in-depth, internal review. Our process sets a benchmark for the industry.

INTEGRITY

We are committed to the proper use of our technology–to help government security and intelligence agencies protect their citizens against terror, crime, and other major security threats. We take this commitment seriously and investigate any credible allegation of product misuse.

EXCELLENCE

We have a track record of success. Our technology has helped governments save thousands of lives, prevent terrorist attacks, break up major crimes, and make the world a safer place.

BOLDNESS

We believe success comes by being intrepid. At NSO, alongside a deep understanding of our business responsibilities, we emphasize being bold yet accountable.

NSO Group. (2020). About Us. Retrieved August 20, 2020, from https://www.nsogroup.com/about-us/

Conclusion

- Created as a helpful tool
- Potential for weaponization
- How vulnerable are devices today?
- What is the probability this tool is always being used for good?

?
Q
&
A
!

References

1. Alliance), C. (2020, January 01). NSO Pegasus. Retrieved August 03, 2020, from https://www.documentcloud.org/documents/4599753-NSO-Pegasus.html
2. Bazaliy, M., Flossman, M., Blaich, A., Hardy, S., Edwards, K., & Murray, M. (2017). *Technical Analysis of Pegasus Spyware* (Rep.). Retrieved August 3, 2020, from https://www.lookout.com/trident-pegasus-enterprise-discovery
3. Marczak, B., Scott-Railton, J., McKune, S., Razzak, B., & Deibert, R. (2020, May 08). HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries. Retrieved August 03, 2020, from https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/
4. Mazzetti, M., Goldman, A., Bergman, R., & Perlroth, N. (2019, March 21). A New Age of Warfare: How Internet Mercenaries Do Battle for Authoritarian Governments. Retrieved August 02, 2020, from https://www.nytimes.com/2019/03/21/us/politics/government-hackers-nso-darkmatter.html
5. NSO Group. (2020). About Us. Retrieved August 20, 2020, from https://www.nsogroup.com/about-us/
6. O'Neill, P. (2019, February 28). Israeli hacking company NSO Group is on sale for more than $1 billion. Retrieved August 26, 2020, from https://www.cyberscoop.com/nso-group-for-sale-1-billion-pegasus-malware/
7. Gardner, D. (2019, December 06). A meticulous account of the killing of journalist Jamal Khashoggi. Retrieved August 20, 2020, from https://www.ft.com/content/38ece616-16a9-11ea-8d73-6303645ac406