

For Public Release


 Canadian Security Intelligence Service / Service canadien du renseignement de sécurité

**Analytical Brief**  
**Précis analytique**




TOP SECRET//

CAB 2021-22/102  
January 13, 2022

[Redacted]

[Redacted]

**Background:**

[Redacted]

**Case Study - [Redacted] use of spyware in Canada**

[Redacted]

2. [Redacted] open-source reporting indicates that, after he moved to Canada, [Redacted] On September 18, 2018, the University of Toronto's Citizen Lab<sup>3</sup> published a research paper on Pegasus, a spyware that infected devices of activists worldwide. [Redacted] In October 2018, open

[Redacted]

[Redacted]

<sup>3</sup> Citizen Lab is a think tank that conducts research related to online censorship and identifying threats to an individual's privacy online.

For Public Release



CAB 2021-22/102  
 January 13, 2022  
 TOP SECRET/ [ ]

sources confirmed that [ ] was using Pegasus spyware [ ]

[ ]

[ ]

[ ]

[ ] builds its cyber arsenal with commercially available tools

[ ]

6. [ ] that the NSO Group sells cyber tools to foreign government agencies and has sold the Pegasus tool to state actors—including the [ ]—who are known to use surveillance tools to target dissidents, human rights activists and advocates worldwide. Pegasus is a highly advanced tool with both 'zero click' and 'one click' attacks. The 'zero click' attack infects a target's phone through a short phone call that automatically infects a compatible phone. A 'one click' attack relies on spear phishing techniques as an initial infection vector. (U)

[ ]

For Public Release



CAB 2021-22/102  
 January 13, 2022  
 TOP SECRET/

### NSO Group – PEGASUS

The NSO Group – also known as Q Cyber Technologies, OSY Technologies and Westbridge depending on jurisdiction – is an Israeli company that was founded in 2010 by former members of the Israeli Intelligence Corps responsible for signals intelligence, Unit 8200. The NSO Group contracts with multiple governments to provide advanced cyber capacities. While the NSO Group does not disclose their clients, investigation by The Guardian and The Citizen Lab has collected a significant amount of data that has identified a number of probable NSO clients, including Mexico, Morocco, Togo, Rwanda, Hungary, Saudi Arabia, the UAE, Bahrain, Azerbaijan, Kazakhstan and India. (U)

The NSO Group's renowned product, Pegasus, has been the subject of considerable controversy. Several media outlets reported that the malware has been used by governments, such as the KSA, India and UAE, to spy on activists, journalists, lawyers and politicians. While infections through Pegasus can be discovered in iOS devices through examining the device, detecting Pegasus infection on Android devices is more difficult. The use of Pegasus by Saudi Arabia prior to and following the murder of Jamal Khashoggi prompted the NSO Group to freeze its ties to Saudi Arabia, pending review. Attempts were made to compromise the devices of Khashoggi's wife in the months prior to his death; his fiancée's phone was also compromised in the days following his murder. Pegasus was also used to target a number of Khashoggi's close associates and individuals who were involved in the investigation into his death, including Canadian resident and prominent Saudi regime critic, Omar Abdulaziz. (U)

### DARKMATTER

Various media reports have highlighted concerns surrounding the activities, powers, and potential targets of DarkMatter – most of this under the name Project Raven – where operatives utilized an arsenal of cyber tools, including a cutting-edge espionage platform known as Karma to spy on human rights activists, journalists and political rivals. In late 2020, DarkMatter formally changed its company name to Digital 14. [redacted] the name change was a mere attempt to distance the company from negative attention in the media. (U)

For Public Release



CAB 2021-22/102  
January 13, 2022  
TOP SECRET//

[Empty rectangular box]

[Empty rectangular box]

**Conclusion**

[Empty rectangular box]

For Public Release




Analytical Brief  
Précis analytique

CAB 2021-22/102  
January 13, 2022

TOP SECRET//

CSIS\_PUBLICATIONS / SCRS\_PUBLICATIONS

THIS INFORMATION IS SHARED WITH YOUR ORGANIZATION FOR INTELLIGENCE PURPOSES ONLY AND MAY NOT BE USED IN LEGAL PROCEEDINGS. THIS DOCUMENT MAY NOT BE RECLASSIFIED, DISSEMINATED OR DISCLOSED IN WHOLE OR IN PART WITHOUT THE WRITTEN PERMISSION OF CSIS. THIS DOCUMENT CONSTITUTES A RECORD WHICH MAY BE SUBJECT TO EXEMPTIONS UNDER THE FEDERAL ACCESS TO INFORMATION ACT OR PRIVACY ACT OR UNDER APPLICABLE PROVINCIAL OR TERRITORIAL LEGISLATION. IF A REQUEST FOR ACCESS UNDER THESE ACTS IS MADE, THE RECEIVING AGENCY MUST CONSULT CSIS IN RELATION TO APPLYING THE AVAILABLE EXEMPTIONS. FURTHER, CSIS MAY TAKE ALL NECESSARY STEPS UNDER SECTION 38 OF THE CANADA EVIDENCE ACT OR OTHER LEGISLATION TO PROTECT THIS INFORMATION. IF YOU LEARN THAT THIS INFORMATION HAS OR MAY BE DISCLOSED, THAT THESE CAVEATS HAVE NOT BEEN RESPECTED OR IF YOU ARE UNABLE TO ABIDE BY THESE CAVEATS, INFORM CSIS IMMEDIATELY.



Intelligence Assessments Branch  
Direction de l'Évaluation du renseignement

5 / 5