Student Occasional Paper Series No. 1 | May 2023

Examining Pegasus Spyware

By Brooke Spens

Abstract

Pegasus spyware is a novel exploit capable of allowing a diverse array of actors to undermine the mobile security of targeted devices. Research indicates that more than 50,000 phone numbers were "selected for surveillance."[1] Forbidden stories labeled Pegasus as "The New Global Weapon for Silencing Journalists."[2] Although the scale and scope of the most recent revelations are astounding, previous research has provided insight into the technical functionality of Pegasus and its users. This analysis builds on the work of the University of Toronto's Citizen Lab, Amnesty International's Security Lab, and The Pegasus Project to analyze the use of this malware as well as methods to counter the threat posed to journalists and other civil society actors as a result of its existence. Finally, this paper examines the use of malware by authoritarian states to target individuals both within their sovereign boundaries and beyond. Pegasus spyware, a piece of technology created by the NSO Group to "collect data from the mobile devices of specific suspected major criminals" has been critically misused. The irresponsible utilization of Pegasus threatens journalists and risks irreversibly changing the landscape of free press (NSO Group, 2021).[3]

Introduction

Pegasus spyware is impressive and elegant exploit; it has the ability to circumvent encryption and security protocols to gain access to audio, visual, and location data and constitutes the prelude to the next generation of spyware technology.[4] Although the code and exploit is itself elegant in its execution, the implications of its use are deleterious and dangerous. General sentiment associated towards Pegasus constitutes a feeling of paranoia rooted in years of well-founded abuse allegations and security concerns raised against the spyware's creator, the NSO Group. Healthy apprehension of Pegasus is warranted particularly as many of its targets

have experienced some of the worst consequences of the use of this malware by state and non-state actors.

In particular, journalists have long been targets of government surveillance within oppressive regimes and authoritarian governments.[5] Good journalism challenges the status quo power structures of repressive states. Technologies such as Pegasus are partially created as tools to suppress the voices of dissidents, political, opposition, and particularly members of the 4th estate who hold non-democratic regimes accountable. This research differentiates itself from previous studies by emphasizing how malware targets journalists acting as agents of change and as the keepers of democratic institutions. This analysis dissects the technical details of Pegasus and contextualizes its use in the targeting of journalists beginning in 2016 and continuing to the present. The modifications to infection delivery and operating techniques post-infection are examined in the context of the forensic analyses leading to the discovery of the spyware on targets mobile devices. This analysis provides a timeline for the implementation of novel features of the malware and its increasing sophistication and effect. Finally, this analysis presents the best practices for how to both measure and minimize the potential impact of spyware deployed by NSO's clients that target human rights activists, dissidents, and journalists.

The Beginning

In 2011, the NSO Group produced the first version of Pegasus spyware. Based in Israel, the NSO Group was formed by Niv Karmi, Shalev Hulio, and Omri Lavie — all programmers with backgrounds in the Israeli military.[6] It was the company's first notable product resulting from several of its founder's past projects coming to fruition. Past ventures had been a video marketing company and the company CommuniTake which allowed for remote control of a device with the user's permission.[7] According to Hulio, the ability to skirt encryption protocols and infiltrate devices attracted the attention of an unnamed European intelligence agency, facilitating the NSO Group's role as a cyber-intelligence company.[8] The work of the NSO Group bridges the private industry and the military, creating military-equivalent cyber weapons within a privatized company.

The first version of Pegasus spyware was documented in 2016. A forensic analysis of Omar Radi's phone provides insight into the fundamentals of Pegasus; the complete report is accessible through Amnesty International 's Security Lab.[9] The spyware was delivered through SMS and WhatsApp messages. The spyware sent data back to NSO group-controlled domains; following the access of that domain, suspicious redirects to URLs, the result of a network injection attack from either a rogue cell-phone tower or specific equipment at the wireless carrier, would be accessed.[10] The redirects are classified as suspicious due to non-standard high port numbers, random URIs, and 4th level subdomains.[11] Once the infection delivery is complete, necessary processes are executed on the device such as the "_kBridgeHeadConfigurationFilePath" file export. This export led to the identification of the "bh" process as bridgehead. This process "completes the browser exploitation, roots the device and prepares for its infection with the full Pegasus suite" (Amnesty International).[12] Various other processes are vital to the infection and ultimately the surveillance of Pegasus's clients chosen targets. The processes and methods of infection delivery listed are associated with the beginning

stages of Pegasus spyware implementation, the variations resulting from the changing stages of Pegasus will be detailed in subsequent sections.

Clients and Capabilities of Pegasus

Pegasus spyware marked an emergence in "pay-to-play government customers."[13] This meant countries lacking in cyber capabilities were able to write a check and gain near instantaneous access to spyware of the highest sophistication. NSO Group sells Pegasus through licenses. These licenses authorize the client to several "simultaneous infections" during a certain window of time for one specific device; the number of licenses is the number of devices able to be infected at one time.[14] The purpose guiding these transactions, according to the NSO Group, was "work[ing] to save lives and create a better, safer world," but the business model promoting this spyware focused on the abilities of the spyware, not the characteristics of its chosen targets.[15]

Pegasus spyware capabilities are extensive. As detailed in leaked marketing material from the NSO Group and confirmed through forensic analysis, this spyware has the ability to access photos, videos, text messages, emails, voice memos, call history, and browsing history; it can remotely enable camera and video features as well as track a device's location through GPS movements. [16]

Figure 1: Leaked graphic from an NSO marketing brochure detailing the collecting capabilities of the spyware, used in Kim Zetter's article "Pegasus Spyware How It Works and What It Collects"

The countries believed to have been sold Pegasus, enabling unregulated access to surveil individuals, include democratic states, including Mexico and India as well as authoritarian regimes in Morocco and Bahrain.[17] The best estimates are that NSO has in excess of forty-five clients, including ten operators suspected to be involved in surveillance outside of their sovereign boundaries and six operators with past allegations of human rights abuses using spyware against civil society. [18] In rare circumstances, individual nation states are identified as the likely candidates that specific operators are acting on behalf of. In 2020, utilizing patterns of reoccurring IP addresses and server communications found in network logs, the Citizen Lab was able to name four operators: SNEAKY KESTREL, MONARCHY, CENTER-1, and CENTER-2.[19] It was concluded with "medium confidence" that SNEAKY KESTREL is linked to the United Arab Emirates (UAE) government and MONARCHY to Saudi Arabia; CENTER-1 and CENTER-2 have unknown affiliations but their targets are in the Middle East.[20] This identification follows that of PEARL, linked to Bahrain, and a previous Saudi Arabia actor KINGDOM in 2017. These clusters were created through an analysis of the nature of the targets connected to each operator, as well as device logs from the phones of targets, the most notable being journalists from the Middle Eastern media outlet *Al Jazeera*.[21] The importance of these actors' recognition relates to the accountability that is necessary following the discovery of the abuse of this spyware; the particulars of the abuses reported will be described in the next segments.

The Validity of the 50,000 Surveillance List

In July of 2021, a consortium of seventeen media outlets published stories about a list of 50,000 phone numbers. The origin of the list was unknown, but the basis of the news was the claim that it constituted the phone numbers of those targeted by the NSO Group's surveillance software.[22] Apprehension around the validity of the list ensued, fueled by NSO Group's remarks that 50,000 targets is unfeasible and that the servers in Cyprus, which the leaking of the list was reportedly traced back to, were nonexistent.[23] However, a thorough analysis of the data available demonstrates a high likelihood of the 50,000-surveillance list representing targets of Pegasus spyware and confirms at minimum a connection of some degree between the list and potential targets.

The list of 50,000 phone numbers developed from the story of an information broker who approached the NSO Group with the information that someone had hacked servers in Cyprus and had a list comprising the targets of Pegasus spyware; Shalev Hulio, cofounder of the NSO Group, responded by saying there was no reasoning behind it as no servers were located in Cyprus.[24] Although Hulio is correct that at the time of his response NSO Group had no servers in Cyprus, there is key information absent. NSO Group did at one time operate out of servers in Cyprus that they acquired from the company Circles, with whom they had partnered with in the hopes of obtaining the necessary technology to add location tracking abilities to their spyware.[25] In conjunction with the knowledge of server operations, evidence obtained through forensic analysis further proves the link existing between the list and the mobile devices with visible infection attempts.[26]

Forensic analysis was conducted by the Amnesty International Security Lab and the Citizen Lab on 67 phones. 37 devices showed residual evidence that an infection had either occurred or an attempt had been made; 15 Android phones did not show evidence, it can be inferred that this is due to Android phones not storing the logs comparable to the expansive logs found on iOS systems that are necessary in the recognition of Pegasus infection.[27] From the list, The Pegasus Project was able to identify the owners of more than a thousand numbers. According to their analysis, while criminals and suspected terrorists were on the list, 188 were journalists.[28] The journalists were accompanied by dissidents and human rights activists targeted by oppressive regimes.

Circumstantial evidence pertaining to the timing of attacks corroborates the data presented on the volume of hacked devices. Similar to bridgehead processes appearing seconds after successful network injection of a target, quick execution was again visible when seconds after a new phone number was added to the database targeting attempts followed.[29] This process was traced on the 37 phones analyzed by Amnesty International. Journalist Kim Zetter also illustrates the nuances surrounding NSO Group's responses, in this instance including their questioning the plausibility of the list being a Home Location Register (HLR) lookup service, and the conclusions by The Pegasus Project by stating "it could, however, be a database maintained by a third-party HLR lookup service whose customers include regimes that use Pegasus. Or it could also be an HLR lookup database that is completely benign and not used in conjunction with spying at all, as NSO suggests, and it just happens to include numerous people who have been spied on or would be coveted targets for spying by NSO customers."

Client's Alleged Abuse of Pegasus Spyware

In early October 2018, Washington Post columnist and dissident journalist Jamal Khashoggi arrived at the Saudi consulate in Istanbul, Turkey; once inside the building, Khashoggi was brutally killed by the Saudi government.[30] Details following the murder draw connections between the journalist's death and Pegasus spyware and call into question the NSO Group's mission of "help[ing] governments protect innocents from terror and crime..."[31]

French media outlet Forbidden Stories, a member of The Pegasus Project, revealed the infections of Khashoggi's personal network including: his fiancée, son, close friends, and colleagues.[32] The operator responsible is believed to have been working on behalf of Saudi Arabia and the UAE, both authoritarian regimes with past human rights violations.[33] This occurrence contextualizes the irresponsible use of mercenary spyware and the ethical consequences stemming from the accessibility of Pegasus spyware for nation states. As indicated by John Scott-Railton, "abuses are a persistent feature of any hacking technology when sold widely."[34] The proliferation of digital surveillance tools has led to rampant allegations of misuse. Known victims are "several Arab royal family members, at least 65 business executives, 85 human rights activists, 189 journalists, and more than 600 politicians and government officials — including cabinet ministers, diplomats, and military and security officers."[35] Through reports from The Pegasus Project and the Citizen Lab, there is evidence of the extensive targeting of journalists; Mexico is "the deadliest non-conflict zone in the world to be a journalist," and an epicenter of abuse against journalists.[36] The targeting of this population with intrusive digital

surveillance technology is one of various subversive techniques utilized. The domain *notisms[.]net* used in Pegasus operations with the operator RECKLESS-1 was linked to the Mexican government and is traced to the attacks against Ricardo Raphael, a journalist reporting on official corruption, Mexican cartels, and investigations like the Iguala Mass Disappearances.[37] Mexico is suspected of the surveillance of Carmen Aristegui, a second journalist investigating corruption within Mexico; her family and colleagues were recipients of infection attempts and she herself received twenty text messages containing Pegasus exploit links.[38] Numerous journalists have similar experiences being victims of censorship through invasive means.

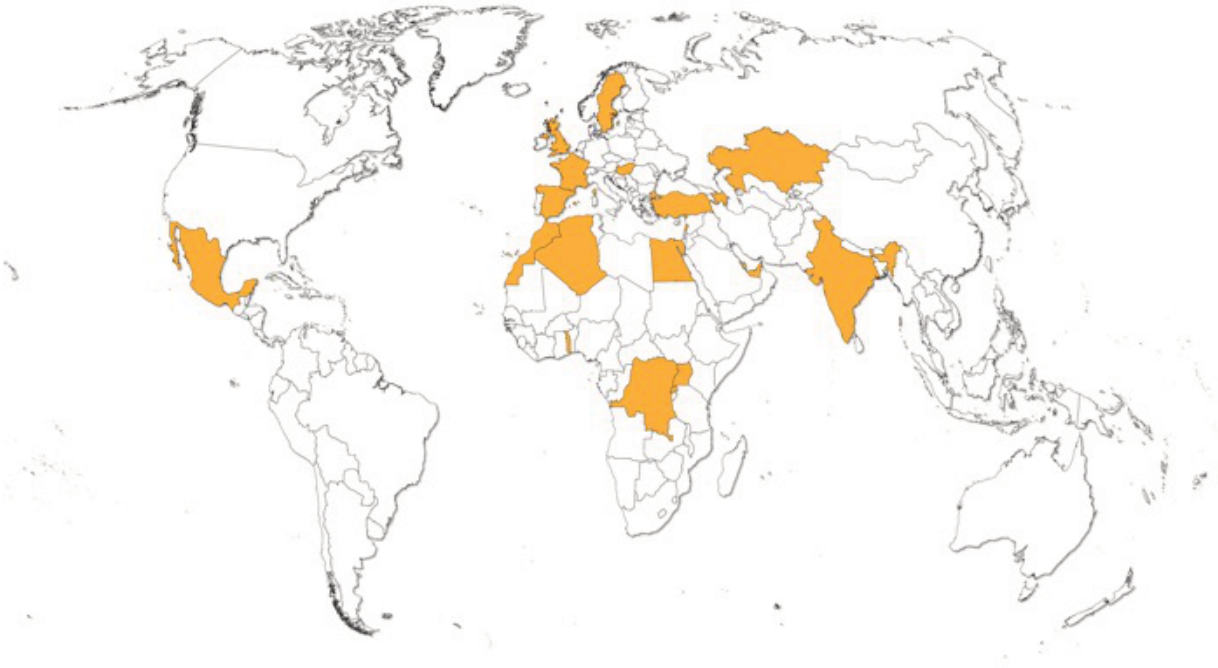

Figure 2: Countries where journalists were targeted included: Mexico, United Kingdom, France, Spain, Morocco, Algeria, Togo, Hungary, Turkey, Lebanon, Egypt, Uganda, Rwanda, Democratic Republic of the Congo, Kazakhstan, Azerbaijan, Bahrain, Qatar, United Arab Emirates, and India. *This map does not represent the citizenship and/or country of residence of the targeted journalist, it indicates the location at the time of Pegasus infection attempts; Jamal Khashoggi was a permanent U.S. resident. The impact of the targeting stretches beyond the sovereign boundaries dictated on this map.

The involvement of Pegasus spyware has been found at numerous levels of government, from accessing a device at 10 Downing Street, the symbolic home of the British Prime Minister, to 11 staff members at the U.S. Embassy in Uganda.[39] The electoral processes in democratic countries have not been left untouched by the "spyware revolution." The presence of Pegasus spyware in opposition groups has been discovered in India, Poland, and Spain.[40] Additionally, indications of spyware use in Spain surrounding the independence of the Catalonia region have been documented by the Citizen Lab, which noted the infection of 63 devices with Pegasus Spyware. Targeted individuals were supporters of Catalan independence, the European Union (EU), and members of the opposition movement.[41] Preliminary indications link the attacks to Spanish authorities.[42]

Zero-click, zero-day attacks appear to be the delivery method of choice after the initial phase of Pegasus spyware in mid-2018 transitioned to current methods; zero-click attacks are defined as requiring no interaction on the user-end of a device prior to a successful hack.[43] Zero-days are a form of cyber-attack where the vulnerabilities within the software are unknown prior to their exploitation. The discovery of infections in Morocco, found through the analysis of human rights defenders who were afflicted, first demonstrated changing methodology among spyware delivery.[44] The forensic analysis of Moroccan devices, such as the phone of activist Maati Monjib, helped to create a "fingerprint" of the Pegasus infrastructure to identify 201 Installation domains frequented during NSO Group operations.[45] The NSO Group excels at identifying vulnerabilities within a device to be used in execution, one instance is HOMAGE, a zero-click vulnerability identified during the Citizen Lab's investigation of the Catalan movement.[46] In late 2019, the exploit chain KISMET was identified as another zero-click, zero-day exploit used up until iOS 14, specifically labeled through a forensic analysis of victims in Mexico.[47] Despite new Internet scanning abilities and vulnerability patching efforts by those fighting to counter invasive technology, the infiltration methods continue to advance, both through the NSO Group and other mercenary spyware firms.[48] For as long as spyware tools like Pegasus are on the market, the abuses recounted in this section will persist.

The Threat of Mercenary Spyware: Implications on Journalists and Free Press

The fourth estate holds the powerful to account and amplifies the voices of those often silenced. Journalists and a free press play a critical role in democracies. Their role is often controversial and makes those in power uncomfortable. Yet it is precisely because they bring into the light issues of corruption, human rights abuses, political malfeasance and other problems in societies they the are often the targets of those in power. Pegasus and other forms of surveillance spyware are the modern tools of surveillance and intimidation.[49] They are used to foster fear, to undermine the flow of information, to hide bad behavior, and undermine transparency.

The implications of surveillance spyware affect the personal safety of its targets, both mentally and physically. Paranoia induced through the threat of surveillance technology can lead to the self-censorship. Journalists who are victims of spyware are right to fear publishing material critical of the state that might result in negative repercussions for themselves and their sources.[50] These concerns are warranted as journalists have witnessed firsthand their colleagues becoming the subjects of retaliation for challenging repressive regimes; including journalists from *The New York Times*, *Al Jazeera*, *Oromia Media Network*, Columbia's *Semana* magazine and Mexico's *Proceso.* Notable victims Jamal Khashoggi and Javier Valdez Cárdenas are the all too common worst case outcome of targeted surveillance facilitated by spyware. Both were murdered as a result of their reporting.[51]

Pegasus spyware is a tool that is being utilized to stifle dissent, and create what has become known as a "terrorizing" effect among independent media, synonymous with the paranoia described previously.[52] As Tasneem Khalil of Netra News put it, spyware is "scaring journalists into inaction."[53] This inhibits their crucial contribution to the information flow that shapes societies and leads to a less informed citizenry.

Figure 3: Journalists mentioned that were allegedly targeted with Pegasus spyware.

Going Forward: Regulation Suggestions and Journalist's Online Security

The ramifications of mercenary spyware are bleak. Its impact is disproportionally shouldered by the independent media. Presently governments are wholly dependent on the NSO group's own claims of corporate responsibility. To date the NSO Group claims they have only sold Pegasus to "thoroughly vetted and approved governmental agencies".[54] Yet it is important to consider that governments are both the guarantor and most common violator of human rights. Providing a powerful surveillance tool to well-funded and supported institutions that have the ability to self-regulate is akin to asking the wolves not to eat the sheep. If a state has a past record of abuses, it is doubtful they will use such a product solely for "anti-terrorist" or other declared legitimate purposes. This is born out by the data leaked from the NSO group. It is evident that the corporate self-regulatory model of surveillance is not functioning properly. Moreover, it is evident that governments have little incentive to regulate the use of tools that provide them surveillance capabilities. The result is a doubly dangerous condition in which not only is there no private or public (government) regulatory controls, but rather there is actually a disincentive to regulate.

It is into this doubly dangerous condition that vulnerable actors fall. How then can journalists and human rights activists be protected? It is these scenarios where the outside interference of nongovernmental organizations (NGOs) should be employed. If the misuse of spyware is categorized as a human rights violation, humanitarian organizations can advocate and

enforce rights of free expression, personal security, and privacy. Amnesty International and the Citizen Lab have been impactful in reporting and urging accountability for the violations of human rights resulting from client's use of Pegasus. It is through these evidence-backed accusations in which reasoning for change is rooted. NGOs like Amnesty International intervene to garner the public support required to seek justice for the victims of government-endorsed surveillance. In the near future, these organizations will be increasingly indispensable as they are one of only a few limited means for countering more advanced threats emerging from the "pay-to-play" cyber industry.

The discourse surrounding the misuse of spyware as it relates to individual journalists and human rights activists cannot be discussed without acknowledging the role of the institutions supporting them. Following widespread awareness of the targeting of journalists, civil society and media organizations should implement best security practices to protect those engaged on their behalf in the collection of sensitive material. Tangible solutions should include the digital security training of journalists and activists on the many relevant digital privacy tools available. For freelance journalists, digital training can be acquired through guides released by organizations such as Reporter's Without Borders, the Electronic Frontier Foundation, Frontline Defenders, and others.[55] The benefits of digital security training extend beyond a journalist's online safety and ability to conduct their job, to their physical safety at all hours. The complexity of the problem presented necessitates a multi-vector approach including all relevant actors. Pegasus spyware is a prelude to the next level of digital espionage, as well as its probable misuses. As the coming generation of surveillance technology unfolds, unease is called for if the past abuses of Pegasus and other forms of spyware are left unchecked.

Bibliography:

Bergman, Ronen, and Mark Mazzetti. "The Battle for the World's Most Powerful Cyberweapon: A Times Investigation Reveals How Israel Reaped Diplomatic Gains around the World from NSO's Pegasus Spyware — a Tool America Itself Purchased but Is Now Trying to Ban." 28 Jan. 2022, https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html.

Deibert, Ron. "The Autocrat in Your iPhone: How Mercenary Spyware Threatens Democracy." *Foreign Affairs*, December 12, 2022. https://www.foreignaffairs.com/world/autocrat-in-your-iphone-mercenary-spyware-ronald-deibert?

"Forensic Methodology Report: How to Catch NSO Group's Pegasus." London, UK: Amnesty International, July 18, 2021. https://www.amnesty.org/en/wp-content/uploads/2021/08/DOC1044872021ENGLISH.pdf.

Hearing on "Combatting the Threats to U.S. National Security from the Proliferation of Foreign Commercial Spyware," § House Permanent Select Committee on Intelligence (2022). https://docs.house.gov/meetings/IG/IG00/20220727/115048/HHRG-117-IG00-TTF-Scott-RailtonJ-20220727.pdf.

Hulio, Shalev. "NSO Group Transparency and Responsibility Report 2021." 30 June 2021, https://www.nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf.

Kaster, Sean D., and Prescott C. Ensign. "Privatized Espionage: NSO Group Technologies and Its Pegasus Spyware." *Thunderbird International Business Review*, 2022, https://doi.org/10.1002/tie.22321.

Marczak, Bill, John Scott-Railton, Noura Al-Jizawi, Siena Anstis, and Ron Deibert. "The Great IPwn: Journalist Hacked with Suspected NSO Group IMessage 'Zero-Click' Exploit." Toronto, Canada: Citizen Lab, December 20, 2020. https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/.

Marczak, Bill, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert. "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries." Toronto, Canada: Citizen Lab. https://tspace.library.utoronto.ca/bitstream/1807/95391/1/Report%23113--hide%20and%20seek.pdf.

OCCRP. "About the Pegasus Project - OCCRP." *About the Project*, July 18, 2021. https://www.occrp.org/en/the-pegasus-project/about-the-project

Priest, Dana, Craig Timberg, and Souad Mekhennet, "Private Israeli Spyware Used To Hack Cellphones of Journalists, Activists Worldwide," Washington Post, July 18, 2021, https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/?itid=lk_inline_manual_4.

"Reporters Without Borders: Digital Security Guides." Accessed April 7, 2023. https://helpdesk.rsf.org/digital-security-guide/.

Rueckert, Phineas. "The New Global Weapon for Silencing Journalists • Forbidden Stories," July 18, 2021. https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/.

Scott-Railton, John, Bill Marczak, Bahr Abdul Razzak, Siena Anstis, Paolo Nigro Herrero, and Ron Deibert. "New Pegasus Spyware Abuses Identified in Mexico," October 2, 2022. https://citizenlab.ca/2022/10/new-pegasus-spyware-abuses-identified-in-mexico/.

Scott-Railton, John, Elies Campo, Bill Marczak, Bahr Abdul Razzak, Siena Anstis, Gözde Böcü, Salvatore Solimano, and Ron Deibert. "CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru." Toronto, Canada, March 26, 2023. https://tspace.library.utoronto.ca/bitstream/1807/119418/1/Report_155--catalangate_012023_.pdf.

Woodhams, Samuel. "Spyware: An Unregulated and Escalating Threat to Independent Media." Accessed March 31, 2023. https://www.cima.ned.org/wp-content/uploads/2021/08/CIMA_Spyware-Report_web_150ppi.pdf.

Zetter, Kim. "Pegasus Spyware How It Works and What It Collects," August 4, 2021. https://zetter.substack.com/p/pegasus-spyware-how-it-works-and.

Zetter, Kim. "The NSO 'Surveillance List.'" *The NSO "Surveillance List": What It Is and Isn't*, July 22, 2021. https://zetter.substack.com/p/the-nso-surveillance-list-what-it.

Endnotes

[1] Rueckert, “The New Global Weapon for Silencing Journalists • Forbidden Stories.”

[2] Rueckert, “The New Global Weapon for Silencing Journalists • Forbidden Stories.”

[3] Hulio, ”NSO Group Transparency and Responsibility Report 2021”

[4] Marczak et al., “The Great IPwn: Journalist Hacked with Suspected NSO Group IMessage ‘Zero-Click’ Exploit.”

[5] Rueckert, “The New Global Weapon for Silencing Journalists • Forbidden Stories.”

[6] Bergman, Ronen, and Mark Mazzetti, ”The Battle for the World’s Most Powerful Cyberweapon: A Times Investigation Reveals How Israel Reaped Diplomatic Gains around the World from NSO’s Pegasus Spyware — a Tool America Itself Purchased but Is Now Trying to Ban”

[7] Bergman, Ronen, and Mark Mazzetti, ”The Battle for the World’s Most Powerful Cyberweapon: A Times Investigation Reveals How Israel Reaped Diplomatic Gains around the World from NSO’s Pegasus Spyware — a Tool America Itself Purchased but Is Now Trying to Ban”

[8] Kaster, Sean D., and Prescott C. Ensign. “Privatized Espionage: NSO Group Technologies and Its Pegasus Spyware.”

[9] “Forensic Methodology Report: How to Catch NSO Group’s Pegasus”

[10] “Forensic Methodology Report: How to Catch NSO Group’s Pegasus”

[11] “Forensic Methodology Report: How to Catch NSO Group’s Pegasus”

[12] “Forensic Methodology Report: How to Catch NSO Group’s Pegasus”

[13] Hearing on “Combatting the Threats to U.S. National Security from the Proliferation of Foreign Commercial Spyware,” § House Permanent Select Committee on Intelligence (2022)

[14] Hearing on “Combatting the Threats to U.S. National Security from the Proliferation of Foreign Commercial Spyware,” § House Permanent Select Committee on Intelligence (2022)

[15] Kaster, Sean D., and Prescott C. Ensign. “Privatized Espionage: NSO Group Technologies and Its Pegasus Spyware.”

[16] Zetter, Kim. “Pegasus Spyware How It Works and What It Collects”

[17] Rueckert, “The New Global Weapon for Silencing Journalists • Forbidden Stories.”

[18] Marczak et al., “Hide and Seek: Tracking NSO Group’s Pegasus Spyware to Operations in 45 Countries.”

[19] Marczak et al., “The Great IPwn: Journalist Hacked with Suspected NSO Group IMessage ‘Zero-Click’ Exploit.”

[20] Marczak et al., “The Great IPwn: Journalist Hacked with Suspected NSO Group IMessage ‘Zero-Click’ Exploit.”

[21] Marczak et al., “The Great IPwn: Journalist Hacked with Suspected NSO Group IMessage ‘Zero-Click’ Exploit.”

[22] OCCRP. “About the Pegasus Project - OCCRP.”

[23] Zetter, Kim. "The NSO 'Surveillance List.'"

[24] Zetter, Kim. "The NSO 'Surveillance List.'"

[25] Zetter, Kim. "The NSO 'Surveillance List.'"

[26] Zetter, Kim. "The NSO 'Surveillance List.'"

[27] Zetter, Kim. "The NSO 'Surveillance List.'"

[28] OCCRP. "About the Pegasus Project - OCCRP."

[29] Zetter, Kim. "The NSO 'Surveillance List.'"

[30] Rueckert, "The New Global Weapon for Silencing Journalists • Forbidden Stories."

[31] Hulio, "NSO Group Transparency and Responsibility Report 2021"

[32] Rueckert, "The New Global Weapon for Silencing Journalists • Forbidden Stories."

[33] Rueckert, "The New Global Weapon for Silencing Journalists • Forbidden Stories."

[34] Hearing on "Combatting the Threats to U.S. National Security from the Proliferation of Foreign Commercial Spyware," § House Permanent Select Committee on Intelligence (2022)

[35] Priest et al., "Private Israeli Spyware Used To Hack Cellphones of Journalists, Activists Worldwide," Washington Post

[36] Rueckert, "The New Global Weapon for Silencing Journalists • Forbidden Stories."

[37] Scott-Railton, John et al.,"New Pegasus Spyware Abuses Identified in Mexico,"

[38] Rueckert, "The New Global Weapon for Silencing Journalists • Forbidden Stories."

[39] Deibert, Ron. "The Autocrat in Your iPhone: How Mercenary Spyware Threatens Democracy."

[40] Deibert, Ron. "The Autocrat in Your iPhone: How Mercenary Spyware Threatens Democracy."

[41] Scott-Railton et al., "CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru."

[42] Scott-Railton et al., "CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru."

[43] "Forensic Methodology Report: How to Catch NSO Group's Pegasus"

[44] "Forensic Methodology Report: How to Catch NSO Group's Pegasus"

[45] "Forensic Methodology Report: How to Catch NSO Group's Pegasus"
[46] Scott-Railton et al., "CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru."
[47] Scott-Railton., "New Pegasus Spyware Abuses Identified in Mexico."
[48] "Forensic Methodology Report: How to Catch NSO Group's Pegasus"
[49] Rueckert, "The New Global Weapon for Silencing Journalists • Forbidden Stories."
[50] Woodhams, Samuel. "Spyware: An Unregulated and Escalating Threat to Independent Media."
[51] Woodhams, Samuel. "Spyware: An Unregulated and Escalating Threat to Independent Media."
[52] Woodhams, Samuel. "Spyware: An Unregulated and Escalating Threat to Independent Media."
[53] Woodhams, Samuel. "Spyware: An Unregulated and Escalating Threat to Independent Media."

[54] Hulio, ”NSO Group Transparency and Responsibility Report 2021”
[55] “Reporters Without Borders: Digital Security Guides.”