PSUEDOSCIENCE

The Spyware Case of Omar Radi

Jonathan Boyd Scott

Pseudoscience: The Spyware Case of Omar Radi

Jonathan Boyd Scott

May 23rd, 2023

Abstract

Mobile spyware research represents a highly specialized and daring pursuit undertaken by a select few individuals worldwide. Within this realm of inquiry, there exists no middle ground; it is an unequivocal affirmation of infection or a complete absence of evidence to substantiate any such occurrence. Those who dare to question the claims put forth by those asserting definitive proof of a spyware infection find themselves automatically categorized as the primary adversaries of non-governmental organizations or special interest groups. Among these special interest groups are The Citizen Lab and Amnesty International, which release reports on spyware infections while leveling accusations of cyber espionage against governments across the globe. In the year 2021, Amnesty International and The Citizen Lab collaborated in the development of a forensics methodology aimed at detecting the widely known Pegasus spyware developed by the NSO Group. However, the methodology in question lacked the rigor and scientific foundations expected of such an endeavor. Instead, it relied upon mere conjecture, failing to provide the essential supporting evidence required in this line of research.

The initial segment of their methodology placed particular emphasis on the spyware case centered around Omar Radi, an individual presently incarcerated in The Kingdom of Morocco for the offenses of rape and treason. Amnesty International and The Citizen Lab expounded upon what they perceived as evidence of a spyware infection on Radi's phone, including indicators discovered on his device. These indicators were subsequently treated as concrete proof of Pegasus infiltration and were considered indicative of a Pegasus infection on other phones around the world. However, this methodology suffered from a significant flaw. Not only did it produce numerous false positive results, but these inaccuracies were never rectified within the report detailing the forensic methodology.

In a similar vein, no public acknowledgement or explicit addressing of these false positives occurred beyond a comment and code commit in a GitHub code repository. No efforts were made to alert the media, issue press releases, or provide public statements regarding the matter. Both Amnesty International and The Citizen Lab maintained a conspicuous silence on the subject. Despite being aware of these false positive results, Amnesty International and The Citizen Lab proceeded to present the flawed methodology report. This report delves extensively into the history surrounding the case of Omar Radi, the technical indicators of compromise, and the purported methods of infection.

History of Self-Referencing

For over a decade, special interest groups such as The Citizen Lab[1] and Privacy International, have consistently published reports making allegations of human rights abuses through the utilization of digital surveillance tools. Additionally, they have actively pursued the filing of complaints and composed letters, claiming to possess evidence of surveillance technologies being used unlawfully against members of civil society.

On February 3rd, 2013, a document titled "**Briefing note on OECD Complaints against Gamma International and Trovicor in the UK and Germany**[2]" was authored. This document involved known organizations such as The Citizen Lab and Privacy International. Its primary concern revolved around the export of surveillance technology, with specific focus on Gamma International and its FinSpy software. The mentioned special interest groups accused Gamma of violating export regulations and lodged a complaint under the OECD Guidelines for Multinational Enterprises. The complaint alleged that the use of surveillance products in Bahrain led to human rights abuses. Given the seriousness of these allegations, the special interest groups are endorsing the complaint's findings. However, undisclosed is the true identity of the individuals or entities behind these aforementioned organizations.

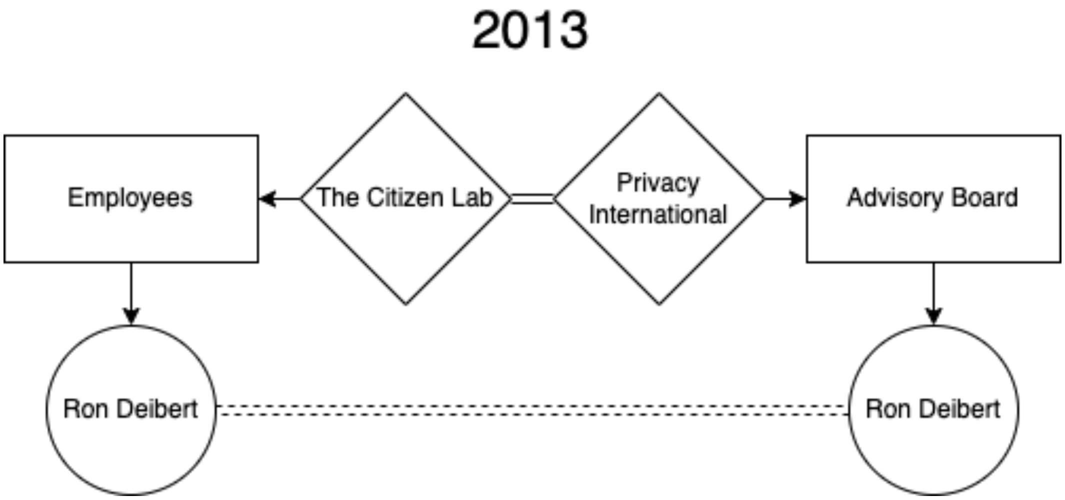


Figure 1 Circular Validation Between The Citizen Lab & Privacy International

[1] https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/

[2] https://web.archive.org/web/20130308002112/https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/2013_02_01_oecd_briefing_note.pdf

Figure 1 illustrates a long-standing pattern of self-referencing and circular validation, which has been observed in the practices of The Citizen Lab and their affiliates. This pattern can be traced back to 2013 when this complaint was written. Ron Deibert, who served on the Privacy International Advisory Board[3], also held a position as the director of The Citizen Lab. Concerns about the fairness and trustworthiness of the complaint and its findings can arise from the interconnections and overlapping roles depicted in Figure 1. If a thorough investigation of these organizations had taken place in 2013, it would have likely revealed clear signs of scientific and biased prejudice.

Now, a clear pattern of circular validation becomes evident as the EU Parliament criticizes and signs a resolution against The Kingdom of Morocco for purportedly engaging in unlawful cyber espionage targeting journalist Omar Radi[4]. In this case, The Citizen Lab and Amnesty International are the organizations that mutually support and strengthen each other's accusations. Additionally, The Citizen Lab has asserted that it independently conducted an independent peer review of Amnesty International's methodology to detect Pegasus[5] in Omar Radi's phone. Upon further investigation, it has been found that this assertion is incorrect. Amnesty International and The Citizen Lab had personnel in common who were under the supervision of a shared authority figure during the investigation. The statement made by The Citizen Lab suggests that they offered an impartial evaluation of Amnesty International's approach. However, the presence of shared personnel presents a clear conflict of interest or bias leading up to the formulation of the methodology and through the entirety of the investigation into Omar Radi's spyware incident.

According to the principles and guidelines of the University of Toronto on Human Ethics, it is essential to avoid conflicts of interest when conducting research within their institution. They emphasize the importance of maintaining impartiality during evaluations or reviews. This implies that reviewers must be independent and devoid of any conflicts of interest that might undermine the objectivity and fairness of the review process[6].

[3] Archive.org shows Ron Deibert as an advisor as early as June, 2012 and well beyond the publication of the Feb, 2013 complaint. [link 1 – June, 2012 https://web.archive.org/web/20120706172455/https://privacyinternational.org/people] [Link 2 March, 2013 - https://web.archive.org/web/20130307220652/https://privacyinternational.org/people]

[4] https://www.europarl.europa.eu/doceo/document/RC-9-2023-0057_EN.html

[5] https://citizenlab.ca/2021/07/amnesty-peer-review/

[6] https://research.utoronto.ca/ethics-human-research/human-ethics-principles-guidelines

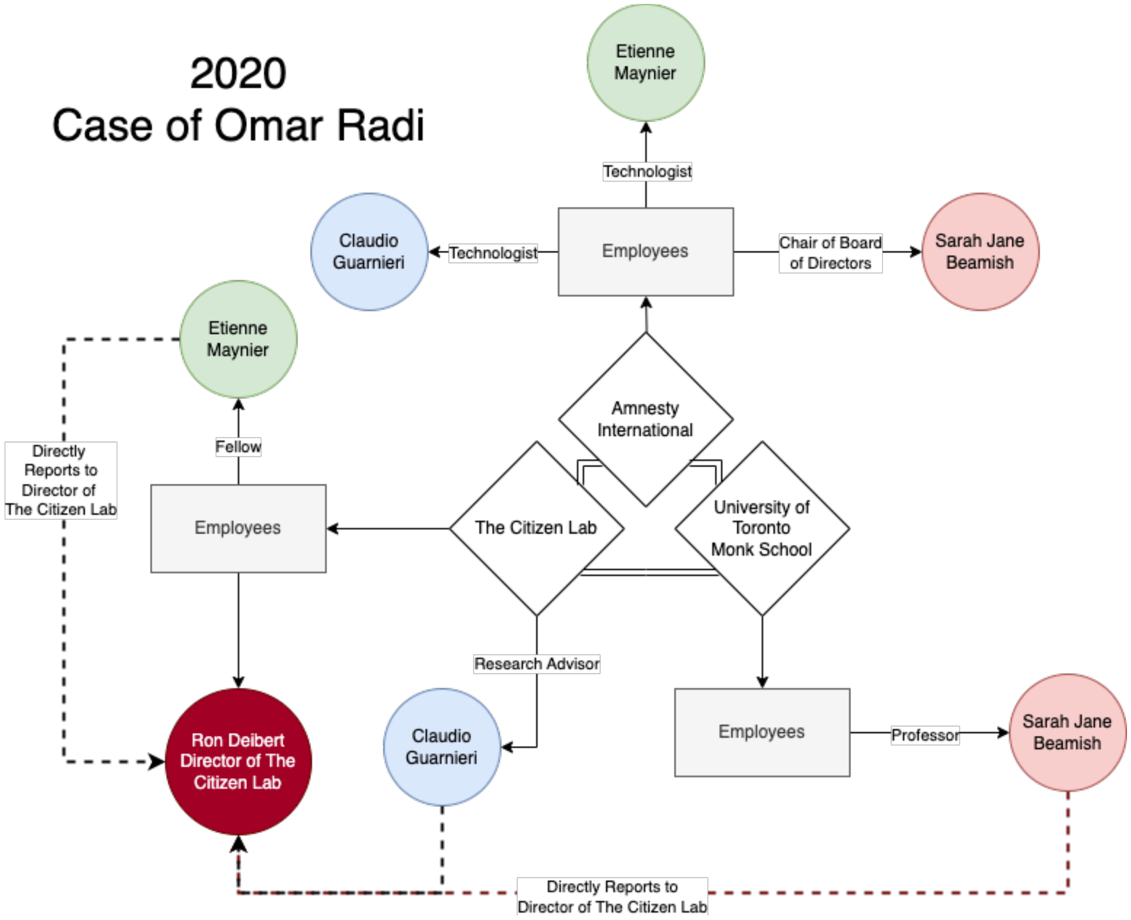


Figure 2 Citizen Lab & Amnesty International Employ Same People During Omar Radi's investigation. The Infection was confirmed by Amnesty Feb, 2020

The connections highlighted in Figure 2 reveal significant relationships between Amnesty International and The Citizen Lab, which cast doubt on claims of independent peer review and objectivity. One notable figure in this context is Claudio Guarnieri, who served as a research advisor at The Citizen Lab[7] while simultaneously being employed by Amnesty International. In September 2020, Guarnieri held the position of senior research fellow at The Citizen Lab[8] and also technologist at Amnesty International's Technology group.

Another key individual in this web of connections is Etienne Maynier, a researcher and forensics investigator. Maynier held concurrent positions at both The Citizen Lab and Amnesty International when the Omar Radi spyware case became public in 2020[9]. It is worth mentioning

[7] https://web.archive.org/web/20200618113556/https://citizenlab.ca/people/
[8] Link 1. Claudio self asserts that he is a senior research fellow at the citizen lab September 27th, 2020 https://web.archive.org/web/20200927032322/https://www.allamericanspeakers.com/speakers/398576/Claudio-Guarnieri
[9] https://randhome.io/about/

that Maynier's affiliation with The Citizen Lab ended in April 2021, after which he joined Amnesty International on a full-time basis. During his time at Amnesty International, Maynier played a significant role in developing the MVT-Tool, a software claimed to detect Pegasus spyware.

Adding to the intertwined relationships, Sarah Jane Beamish, who served as the Chair of Amnesty International's board of directors[10], also held a professorship[11] at The University of Toronto's Monk School, the institution that houses The Citizen Lab. Maynier, Beamish and Guarnieri all directly reported to Ron Deibert, the director of The Citizen Lab. Taken together, these connections between Claudio Guarnieri, Etienne Maynier, Sarah Jane Beamish, and Ron Deibert expose the intricate interplay between Amnesty International and The Citizen Lab. These relationships challenge the notion of independent scrutiny and objectivity in their respective roles and activities related to the Omar Radi spyware case and the development of spyware detection tools

Requests Denied

Amnesty International had confirmed Omar Radi's infection February of 2020[12] and formally released a report June 2020 in which they accused the Moroccan government of engaging in surveillance of journalist Omar Radi through the utilization of the NSO Group's Pegasus. The Moroccan government promptly demanded that Amnesty provide substantiating evidence for these allegations. Saaïd Amzazi, the Minister of National Education, Vocational Training, Higher Education, and Scientific Research, expressed that the Kingdom of Morocco was being unjustly targeted by an international campaign tarnishing its reputation, and insisted on receiving an official response from this organization purporting to advocate for human rights. This response should have included comprehensive evidence substantiating the organization's claims against Morocco. Despite a waiting period of five days, Amnesty International neither provided a response nor presented any evidentiary materials to the Moroccan officials[13].

It was not until July 18th, 2021 that the global community gained any insight into the confirmation of Pegasus spyware infections worldwide through the joint efforts of Amnesty International and The Citizen Lab. The publication of the **Forensic Methodology Report: How**

[10] https://www.amnesty.org/en/documents/fin40/4743/2021/en/ (Financials, Pg 50, payments to directors 2019 & 2020)

[11] https://munkschool.utoronto.ca/mga/news/meet-mga-alumna-turned-faculty-sarah-beamish (Current professor as of Nov, 2022)

[12] https://www.amnesty.org/en/latest/news/2020/06/omar-radi-moroccan-journalist-refuses-to-be-silenced/

[13] https://fr.le360.ma/politique/video-affaire-omar-radi-le-gouvernement-exige-de-nouveau-une-reponse-officielle-damnesty-218462/

to catch NSO Group's Pegasus[14] received significant acclaim within the information security community. However, upon closer examination, it became apparent that the report, despite its title implying a systematic and replicable scientific approach, primarily relied on speculative accusations rather than rigorous scientific methodology.

Although the report contained numerous phrases such as "*Amnesty International believes*," "*we discovered suspected*," "*might stand for*," and "*suspicious processes*," it was universally accepted as an authoritative source of truth, without facing critical scrutiny from the information security community. Individuals who had the courage to question or critically assess the report faced unwarranted denigration from certain members associated with The Citizen Lab and Amnesty International. These individuals were unjustly labeled as frauds, charlatans, or conspiracy theorists[15], and, colloquially speaking, were subjected to cancellation[16]. The cancelation attempts by Amnesty and The Citizen Lab created a Streisand effect and more researchers[17] around the world began to question the validity of this methodology to detect Pegasus.

The Methodology Overview

According to the Forensic Methodology Report, which was written by Amnesty International and verified by The Citizen Lab, it clearly states that upon discovering cases of Pegasus infection among Moroccan human rights defenders, they undertook efforts to improve their forensic methodologies. However, the report fails to provide any detailed explanation of the actual process they followed.

[14] https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/
[15] https://twitter.com/jonathandata1/status/1580236372593344518?s=20
[16] https://theobjective.com/espana/2022-11-23/comision-veta-experto-catalangate/
[17] https://twitter.com/_Raghave/status/1639264188576190464?s=20

Table 1 Amnesty Forensics Methodology Process List

Forensics Methodology Sections			
1	Discovering Pegasus network injection attacks	9	Unravelling the Pegasus attack infrastructure over the years
2	Pegasus' BridgeHead and other malicious processes appear	9.1	Further attempts by NSO Group to hide their infrastructure
2.1	Additional suspicious processes following BridgeHead	9.2	Identifying other NSO attack domains
3	Pegasus processes following potential Apple Photos exploitation	9.3	What can be learned from NSO Group's infrastructure
4	An iMessage zero-click 0day used widely in 2019	9.4	Attack infrastructure hosted primarily in Europe and North America
5	Apple Music leveraged to deliver Pegasus in 2020	9.5	Infection domain resolutions observed in Passive DNS database
6	Megalodon: iMessage zero-click 0-days return in 2021	10	Mobile devices, security and auditability
7	Incomplete attempts to hide evidence of compromise	11	With our Methodology, we release our tools and indicators
8	Pegasus processes disguised as iOS system services		

The methodology report is broken into 17 sections and after a thorough review spanning over a year, several aspects of the self-asserted forensics methodology became remarkably evident.

1. The presented content was not a methodology as initially expected; instead, it focused on targeting a specific country, namely The Kingdom of Morocco.
2. Out of the 17 sections within the forensics methodology report, approximately 52.9%[18] of them directly pertain to or reference a Moroccan spyware case, forming a significant portion of the report that revolves around allegations of espionage by Morocco.
3. Within the forensics methodology report, 4 out of the 17 sections were dedicated to the spyware case of Omar Radi, making it the most prominent individual focus in the report, accounting for approximately 23.5%[19] of its content.

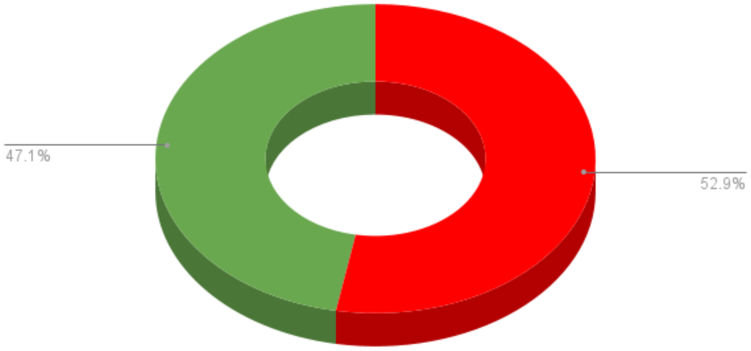


Figure 3 – 52.9% of Methodology Focusing on Morocco 9 of 17 sections

[18] Out of 17 sections 9 sections referenced or specifically focused on Morocco, Omar Radi and or Maati Monjib, these sections are: 1,2,2.1,4,5,6,9.1,9.2,9.5

[19] Out of 17 sections 4 sections referenced or specifically focused on Omar Radi, these sections are: 1,2,2.1,6

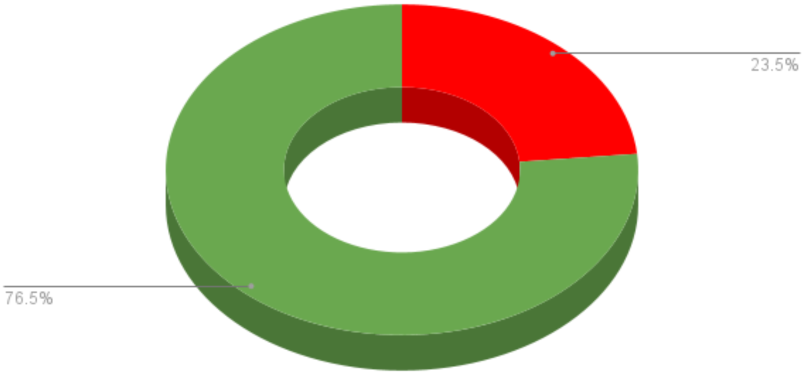


Figure 4 - 23% of Methodology Focusing on Omar Radi 4 of 17 sections

4. Upon the initial release of The Methodology Report, 100% of the "forensics traces" presented in Appendix B and Appendix C were exclusively from Moroccan members of civil society[20], despite the report explicitly mentioning confirmed infections in France, India, Rwanda, UAE, Hungary, and Azerbaijan.

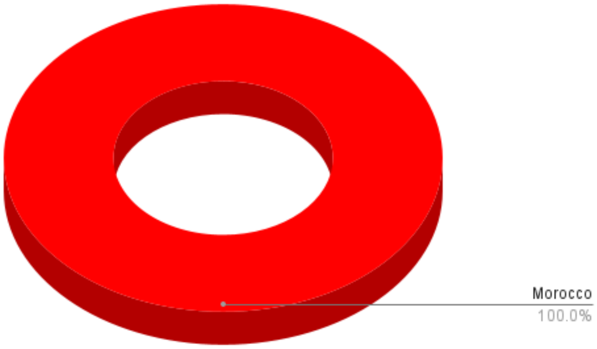


Figure 5 - 100% of Appendix B & C Detailed Forensics Traces were from Morocco even though members of civil society from 6 other countries were alleged to be infected with Pegasus. Only Maati Monjib and Omar Radi were listed.

[20] https://web.archive.org/web/20210718160124/https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/ (The other 6 countries would later be added to Appendix D and E, but those did not exist at the time of the release of the report)

Summary of Methodology Observations

When comparing Amnesty International's forensics methodology report to a proper mobile forensics response like the one developed by ENISA[21], the shortcomings of the former become even more apparent. ENISA's methodology stands out from Amnesty International's report by adhering to recognized industry standards and best practices, while also providing in-depth technical insights into the process of identifying malicious threats.

ENISA's mobile methodology emphasizes a clear definition of scope and objectives, ensuring a focused and systematic approach to investigations. It provides guidelines for identifying the types of devices, operating systems, and evidence to be examined. In contrast, Amnesty International's report lacks a comprehensive scope, focusing disproportionately on specific incidents in Morocco and failing to establish clear boundaries for its investigation. This lack of a defined scope limits the applicability and generalizability of the report as a methodology.

Moreover, ENISA's methodology places great importance on preparation, including establishing a secure forensic environment and following rigorous evidence handling procedures. It emphasizes the need to maintain the integrity and admissibility of evidence in legal proceedings. Conversely, Amnesty International's report does not provide explicit details on the protocols and procedures used for evidence preservation and handling, which raises concerns about the reliability and credibility of the findings.

Additionally, ENISA's methodology promotes a systematic approach to data acquisition, analysis, and interpretation. It outlines specific steps and techniques for extracting and examining evidence, employing a range of forensic tools. In contrast, Amnesty International's report lacks a structured methodology for data acquisition and analysis. It relies heavily on specific cases and anecdotal evidence, such as the case of Omar Radi, rather than providing a systematic and reproducible approach applicable to different scenarios. This lack of a rigorous methodology undermines the reliability and objectivity of the report's findings.

[21] https://www.enisa.europa.eu/topics/training-and-exercises/trainings-for-cybersecurity-specialists/online-training-material/documents/Mobileincidenthandlinghandbook.pdf

Omar Radi's Findings: Section 1

Given the substantial influence of Omar Radi's forensic findings on the claimed methodology's development, a thorough evaluation of Amnesty's assertions and evidence, validated by The Citizen Lab, becomes imperative. This assessment will specifically concentrate on Sections 1, 2, 2.1, and 6 of the methodology report, followed by an analysis of the "forensics traces."

Table 2 Section 1 Assertions and Factual Conclusions

Section 1 Discovering Pegasus Network Injection Attacks	
Assertions	**Factual Conclusions**
In our October 2019 report, we detail how we determined these redirections to be the result of network injection attacks performed either through tactical devices, such as rogue cell towers, or through dedicated equipment placed at the mobile operator. When months later we analysed the iPhone of Moroccan independent journalist Omar Radi, who as documented in our 2020 report was targeted, we found similar records involving the free247downloads.com domain as well.	To begin, a "network injection attack" is non-existent, and Amnesty is engaging in unsubstantiated speculation regarding the method of infection of Omar Radi's phone. They put forward possibilities such as the use of tactical devices like rogue cell towers or dedicated equipment positioned at the mobile operator. Additionally, they claim that a domain called free247download.com played a role in the infection, but they fail to provide any supporting evidence to substantiate this assertion.
Although Safari history records are typically short lived and are lost after a few months (as well as potentially intentionally purged by malware), we have been able to nevertheless find NSO Group's infection domains in other databases of Omar Radi's phone that did not appear in Safari's History. For example, we	The main purpose of the favicon.db database is to store information about website icons (favicons). It is not intended to keep a detailed record of browsing history or visited websites. It only includes a limited set of websites that have associated favicons. Since the favicon.db database is independent of Safari's browsing

could identify visits through Safari’s Favicon.db database, which was left intact by Pegasus:	history, it is possible to modify or change the data stored in this database. Consequently, the accuracy and dependability of the information obtained from favicon.db can be compromised. Additionally, if a link was accessed in private browsing mode, there will be no record in either the favicon.db or Safari's browsing history.
Similarly, on a different occasion Omar Radi visited the website of French newspaper Le Parisien, and a network injection redirected him through the staging domain tahmilmilafate[.]com and then eventually to free247downloads[.]com as well. We also saw tahmilmilafate[.]info used in the same way:	Amnesty uses the term "network injection attack" to refer to a man-in-the-middle (MITM) attack. Specifically, this MITM attack occurs when the victim accesses an insecure website using HTTP instead of HTTPS. Amnesty claims that Radi visited leparisien.fr, and historical data indicates that the website was secured during the period of 2019-2020 when Radi allegedly visited it. Additionally, Amnesty implies that Radi accessed an unsecured version of leparisien.fr, but it does not specify whether he clicked on a link or manually entered the HTTP address.

Section 1 Summary

First, while Amnesty International states that their technical investigation into NSO Group's Pegasus intensified following the discovery of targeting their staff and a Saudi activist, Yahya Assiri, in 2018, no concrete evidence or verifiable data is presented to support this claim. Furthermore, their reliance on "suspicious redirects" recorded in Safari's browsing history as evidence of network injection attacks is questionable. The presence of odd-looking URLs and non-standard port numbers alone cannot conclusively prove the involvement of NSO Group or the existence of malicious activities.

Additionally, the inclusion of domains like free247downloads.com and urlpush.net does not automatically implicate NSO Group or establish a direct link to Pegasus. The mere appearance of these domains in Safari's browsing history or other databases does not provide sufficient evidence to support the allegations made by Amnesty International. Moreover, the lack of clear documentation regarding the methodology used in their analysis raises concerns about the reliability and accuracy of their findings.

The reliance on Safari history and app-specific data as indicators of compromise has limitations. Amnesty International assumes these records are conclusive evidence of network injection attacks, overlooking other influencing factors. Attribution to NSO Group based solely on these records is speculative and lacks substantiation. The absence of concrete proof of NSO Group's involvement is evident. Amnesty International's reports from 2019 and 2020 are self-referential and lack independent corroboration, undermining the credibility of their findings.

Omar Radi's Findings: Section 2

Section 2 presents 8 assertions attempting to establish a correlation between a 2016 report by Lookout[22] and the presence of a process named "bh" in an iPhone backup. Each assertion, taken verbatim from Amnesty's methodology report, is documented with reference numbers. The utmost significance of this section within Omar Radi's findings cannot be overstated, as these results often form the bedrock for attributing Pegasus infections to individuals across the globe. The validity and accuracy of these assertions play a critical role in shaping the narrative and potential consequences surrounding Pegasus-related incidents.

Table 3 Section 2 Assertions Pegasus' BridgeHead and other malicious processes appear

#	Section 2 Assertions Pegasus' BridgeHead and other malicious processes appear
1	iOS maintains records of process executions and their respective network usage in two SQLite database files called "DataUsage.sqlite" and "netusage.sqlite" which are stored on the device. It is worth noting that while the former is available in iTunes backup, the latter is not.

[22] https://info.lookout.com/rs/051-ESQ-475/images/pegasus-exploits-technical-details.pdf

	Additionally, it should be noted that only processes that performed network activity will appear in these databases.
2	Both Maati Monjib's and Omar Radi's network usage databases contained records of a suspicious process called "bh". This "bh" process was observed on multiple occasions immediately following visits to Pegasus Installation domains.
3	Crucially, we find references to "bh" in the Pegasus iOS sample recovered from the 2016 attacks against UAE human rights defender Ahmed Mansoor, discovered by Citizen Lab and analyzed in depth by cybersecurity firm Lookout.
4	As described in Lookout's analysis, in 2016 NSO Group leveraged a vulnerability in the iOS JavaScriptCore Binary (jsc) to achieve code execution on the device. This same vulnerability was also used to maintain persistence on the device after reboot. We find references to "bh" throughout the exploit code:
5	bh.c – Loads API functions that relate to the decompression of next stage payloads and their proper placement on the victim's iPhone by using functions such as BZ2_bzDecompress, chmod, and malloc"
6	Lookout further explains that a configuration file located at /var/tmp/jb_cfg is dropped alongside the binary. Interestingly, we find the path to this file exported as _kBridgeHeadConfigurationFilePath in the libaudio.dylib file part of the Pegasus bundle:
7	Therefore, we suspect that "bh" might stand for "BridgeHead", which is likely the internal name assigned by NSO Group to this component of their toolkit.
8	The appearance of the "bh" process right after the successful network injection of Omar Radi's phone is consistent with the evident purpose of the BridgeHead module. It completes the browser exploitation, roots the device and prepares for its infection with the full Pegasus suite.

Section 2: Assertion Review

1. The statement highlights the availability of the "DataUsage.sqlite" file in iTunes backup, indicating that process execution records can be retrieved from backups. However, it also notes that the "netusage.sqlite" file is not included in iTunes backup, which implies that network usage records may not be accessible through this backup

method. Additionally, Amnesty underscores that the databases exclusively contain records of processes that have engaged in network activity. Consequently, processes that have not performed network-related operations would not be captured in these databases.

2. The observation of a process named "bh" immediately following visits to alleged Pegasus Installation domains does not indicate a direct causal relationship or involvement of the Pegasus spyware. There could be other factors or explanations for the appearance of this process, such as coincidental naming or unrelated activities.

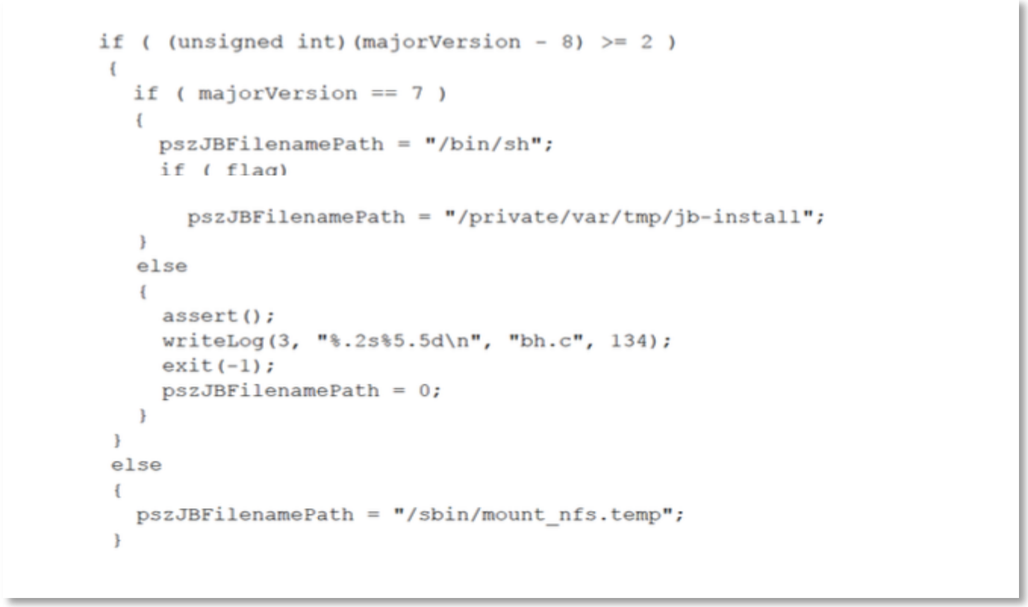
3. Amnesty International is seeking to establish a link between CVE-2016-4657 and an alleged attack on Omar Radi that took place between 2019 and 2020. Their discovery of the presence of "bh" in an iPhone backup has led them to speculate that "bh" could be part of another exploit chain. However, it is worth noting that CVE-2016-4657, which pertains to WebKit in Apple iOS prior to 9.3.5, would require Omar Radi's phone to have not been updated for three years in order for this vulnerability to be exploited on his device. This raises questions regarding the timeline and the potential execution of this particular vulnerability on his mobile device.

4. Once again, it becomes apparent that Amnesty is attempting to utilize the Lookout report titled "Technical Analysis of the Pegasus Exploits on iOS" from 2016. However, what is particularly intriguing is their assertion that they discovered references to "bh" within the exploit code. This implies that they possess a copy of the iOS malware, yet they have not made this malware sample available to the public. Furthermore, while Amnesty provides a code snippet, they fail to disclose its origin.

```
var compressed_bh_addr =  shellcode_addr_aligned +
shellcode32.byteLength;
replacePEMagics(shellcode32, dlsym_addr, compressed_bh_addr,
bundle.bhCompressedByteLength);
storeU32Array(shellcode32, shellcode_addr);
storeU32Array(bundle.bhCompressed32, compressed_bh_addr);
```

Code Block 1- Amnesty presents this JS code without any reference to where it came from

5. Amnesty again makes use of Lookout's 2016 report and mentioning "bh.c" as an effort to establish a connection between the bh process discovered in the iPhone backup and the previously detected malware from 2016. However, a closer examination of the context within the Lookout report[23] reveals that Lookout suspects bh.c to be a component of a larger modular exploit system that then generates a stage 2 binary. Furthermore, when Amnesty quotes the Lookout reference stating, "bh.c - Loads API functions that pertain to decompressing subsequent stage payloads and correctly positioning them on the victim's iPhone using functions such as BZ2 _ bzDecompress, chmod, and malloc," it invalidates assertion #2 because "BZ2 _ bzDecompress, chmod, and malloc" have no relevance to network usage.



```
if ( (unsigned int)(majorVersion - 8) >= 2 )
{
  if ( majorVersion == 7 )
  {
    pszJBFilenamePath = "/bin/sh";
    if ( flag)

      pszJBFilenamePath = "/private/var/tmp/jb-install";
  }
  else
  {
    assert();
    writeLog(3, "%.2s%5.5d\n", "bh.c", 134);
    exit(-1);
    pszJBFilenamePath = 0;
  }
}
else
{
  pszJBFilenamePath = "/sbin/mount_nfs.temp";
}
```

Code Block 2 - Image of a code block from 2016 Lookout report (pg. 37)

Looking further into the 2016 Lookout discovery we find a usage of “bh.c”

Breakdown of Code Block 2

The code begins with an if statement that checks a condition (unsigned int) (majorVersion - 8) ≥ 2. Here, majorVersion is likely an integer variable representing a

[23] https://info.lookout.com/rs/051-ESQ-475/images/pegasus-exploits-technical-details.pdf [pg. 14]

software version number. The condition is checking if the difference between majorVersion and 8 is greater than or equal to 2.

If the condition in the first if statement is true, the code enters the block enclosed by curly braces {}. Inside this block, there is another if statement that checks if majorVersion is equal to 7.

If majorVersion is indeed 7, the code assigns the string "/bin/sh" to the variable pszJBFilenamePath. Then, there is a nested if statement checking the value of a variable flag. If flag is true, pszJBFilenamePath is reassigned the string "/private/var/tmp/jb-install". Otherwise, the value of pszJBFilenamePath remains "/bin/sh".

If majorVersion is not equal to 7, the code proceeds to an else block. Inside this block, there is an assert() function call, which is typically used for debugging purposes to verify assumptions or conditions.

Following the assert() function call, there is a call to the writeLog() function. This function appears to write a log message with three parameters: a log level of 3, the string "8.285.5d\n", the file name "bh.c", and the line number 134.

After logging the message, the code calls the exit() function with the argument -1, which typically terminates the program execution. The value of -1 is commonly used to indicate an abnormal termination or an error condition.

Finally, the code assigns the value 0 to the variable ps2JBFilenamePath and exits the current scope.

If the condition in the initial if statement evaluates to false, the code proceeds to an else block. Inside this block, the variable pszJBFilenamePath is assigned the string "/sbin/mount nfs.temp."

Code Block 2 Conclusion

“bh.c” would not be a binary process that executes a network function as asserted in Amnesty’s claim #2. In fact, Lookout explicitly states the following about code block 2.

“The code snippet shows that for iOS version 7, the install path for the next stage’s binary is either /bin/sh or /private/var/tmp/jb-install (if flag is non-zero). For iOS versions older than 7, the assert callback is called and the program terminates. For iOS 8 and greater, the install path is specified as /sbin/mount _ nfs.temp.

*The size of the data blob containing the next stage binary is verified to be non-zero. If the size is zero, the assert callback occurs and Stage 2 is terminated. The BZ2 _ * API functions are then used by Stage 2 to decompress the data into two files: the first file is the next stage binary, which, for iOS 9, is stored at /sbin/mount _ nfs.temp. The second file is the configuration file, which is stored at /private/var/tmp/jb _ cfg.*

The permissions of the two files are changed to 0755 (making the files executable) before control returns to the main thread.

The final function that Stage 2 calls before terminating is responsible for moving the binary dropped by the previous step. For iOS versions 8 and 9, the file /sbin/mount _ nfs.temp is renamed to /sbin/mount _ nfs. If the iOS on the victim’s phone is iOS 9, an attempt is made to delete /sbin/mount _ nfs prior to the renaming operation. After renaming the file, the assert callback function is called followed by the exit function, terminating Stage 2. Once execution returns to the main thread, Stage 2 terminates silently[24].”

6. Amnesty summarizes Code Block 2 and states that the presence of the configuration file *"/var/tmp/jb_cfg"* is observed alongside the Stage 2 binary. Subsequently, Amnesty

[24] https://info.lookout.com/rs/051-ESQ-475/images/pegasus-exploits-technical-details.pdf [pg. 37]

tries to establish a link between an unidentified configuration file and a dylib file, namely the libaudio.dylib file, which they allege is part of the Pegasus bundle. Amnesty does not provide any source for this connection, no samples were shared, and they now assert having access to a "Pegasus bundle."

7. Amnesty claims that based on assertions 1-6, which are dependent on a 2016 exploit unrelated to network usage, they conclude that the two-letter process discovered in a network usage data table within an iPhone backup is actually referred to as "Bridgehead," and it is believed to be a component of the NSO Group exploit chain.

8. In section 2, the last assertion once again draws conclusions about the presence of "bh" and labels it as Bridgehead. However, similar to previous claims, there is no supporting evidence provided to validate any of these statements.

Omar Radi's Findings: Section 2.1

Table 4 Section 2.1 Assertions Additional suspicious processes following BridgeHead

#	Section 2.1 Assertions Additional suspicious processes following BridgeHead
1	The bh process first appeared on Omar Radi's phone on 11 February 2019. This occurred 10 seconds after an IndexedDB file was created by the Pegasus Installation Server and a favicon entry was recorded by Safari. At around the same time the file com.apple.CrashReporter.plist file was written in /private/var/root/Library/Preferences/, likely to disable reporting of crash logs back to Apple. The exploit chain had obtained root permission at this stage. Less than a minute later a "roleaboutd" process first appears.
2	Omar Radi's device was exploited again on the 13 September 2019. Again a "bh" process started shortly afterwards. Around this time the com.apple.softwareupdateservicesd.plist file was modified. A "msgacntd" process was also launched.
3	Based on the timing and context of exploitation, Amnesty International believes the roleaboutd and msgacntd processes are a later stage of the Pegasus spyware which was loaded after a successful exploitation and privilege escalation with the BridgeHead payload.

4	Amnesty International verified that no legitimate binaries of the same names were distributed in recent versions of iOS. The discovery of these processes on Omar Radi’s and Maati Monjib’s phones later became instrumental for Amnesty International’s continued investigations, as we found processes with the same names on devices of targeted individuals from around the world.

Section 2.1: Assertion Review

1. Amnesty and The Citizen Lab frequently create scenarios where they believe something malicious is happening. According to Amnesty, when Omar Radi visited a suspicious website, a file called "*com.apple.CrashReporter.plist*" was written in the "*/private/var/root/Library/Preferences/"* directory, possibly to prevent crash logs from being reported to Apple.

   There are several factors to consider here. We don't know which apps were running on Radi's device, the specific iOS version, or the device model. These variables could explain why the CrashReporter.plist file appeared in the root of the iPhone backup. When Amnesty suggests that the file was placed there to disable reporting, it implies that they were uncertain if any changes were made to the property list at all.

   Amnesty stated that finding com.apple.CrashReporter.plist in either the root or home domain of an iPhone backup indicates infection with Pegasus, this was stated by Amnesty adding the .plist to their STIX2 file. The STIX2 file is their list of indicators of compromise (IOCs). In essence, if any of these keywords are found in an iPhone backup, it is considered evidence of Pegasus infection.

   The presence of CrashReporter.plist in the root or home domain raised concerns on Amnesty's GitHub account. An iOS developer opened an issue titled "*False Indication of Pegasus*," explaining that the mere presence of "*Library/Preferences/com.apple.CrashReporter.plist*" is considered an infection indicator for Pegasus. This leads to false alarms for any iPhone used for normal iOS development.

The developer suggested that Amnesty should check the content of the file and look for specific code modifications to determine if CrashReporter.plist was actually altered[25].

Amnesty responded to the iOS developer, acknowledging the accuracy of their statement. However, they explained that their MVT-Tool only relies on the manifest file and does not examine the file's content. Despite the potential for false positives, Amnesty decided to retain this indicator as it can provide valuable information.

The significance of com.apple.CrashReporter.plist as an indicator of compromise cannot be overstated, and I have extensively researched this particular indicator due to its widespread impact on individuals worldwide.

Amnesty ultimately acknowledged com.apple.CrashReporter.plist as a false positive results and announced their decision to eliminate com.apple.CrashReporter.plist[26] from their list of indicators of compromise in the STIX2 file. However, as I have previously discussed in detail [27] , this removal effectively renders any detection of com.apple.CrashReporter.plist in the root domain and home domain NULL. Consequently, if Omar Radi's device were to be scanned again using Amnesty's MVT-Tool at the time they had removed the IOC from the STIX2 file, com.apple.CrashReporter.plist would no longer be detected, thereby undermining the entire theory proposed in Amnesty's 2.1 section.

In the subsequent claim, the mention of the "roleaboutd" process being identified as malicious lacks any attribution from Amnesty regarding the basis for deeming it as such. Furthermore, upon examining the "forensic traces," it becomes evident that the timelines of Radi's infections do not align, and the sequence of events surround “roleaboutd” described by Amnesty does not correspond to how the infection supposedly occurred.

[25] https://github.com/AmnestyTech/investigations/issues/19

[26] https://github.com/AmnestyTech/investigations/commit/928ea5a820df6596762241da147b5afa1458b5ee

[27] https://www.researchgate.net/publication/365743925_Review_of_Catalangate_Amnesty_International_Validation, starting on PDF page 20, I discuss in much detail the impact of Amnesty removing the false positive result com.apple.CrashReporter.plist

2. Amnesty's assertion that com.apple.softwareupdateservicesd.plist was altered is presented without any attribution, and they hastily identify it as an indicator of compromise. However, Amnesty later retracts this claim and removes the alleged malicious property list, acknowledging it as a false positive result[28]. It is revealed that this property list is, in fact, a standard property list on iOS devices and poses no threat. In The Citizen Lab's assessment of Amnesty's methodology, they explicitly state, *"We have not observed Amnesty's list of 45 process names associated with any benign or legitimate apps[29]."* This raises the question of how The Citizen Lab can confidently affirm the soundness of Amnesty's methodology when numerous false positive results have been discovered both internally by Amnesty and by other developers.

3. Once again, Amnesty is asserting that both "roleaboutd" and another identified process, "msgacntd," represent a subsequent phase of the Pegasus spyware that is installed after a successful exploitation. However, their statements lack concrete evidence, and they persist in using phrases like "we believe" without substantiating their claims. This pattern indicates that they are essentially making speculative assumptions rather than providing solid proof.

4. Amnesty asserts that they have confirmed the absence of legitimate binaries with identical names in recent versions of iOS, a claim also made by Citizen Lab in their alleged independent peer review of Amnesty's methodology. However, there is a flaw in this statement. The binary property lists, present in either .bplist or XML format, which form part of the iOS binaries structure, were not thoroughly examined. These property lists were incorrectly identified as malicious, even though they were not. Therefore, Amnesty's assertion that no legitimate binaries with the same names were distributed in recent iOS versions is erroneous.

[28] https://github.com/AmnestyTech/investigations/commit/1c694217c3efb4e40f34822b6ef99a7b5bd8a064
[29] https://citizenlab.ca/2021/07/amnesty-peer-review/

Omar Radi's Findings: Section 6

#	Section 6 Assertions Megalodon: iMessage zero-click 0-days return in 2021
1	Amnesty International subsequently analyzed the iPhone of a journalist (CODE MOJRN1), which contained very similar records. This device was exploited repeatedly on numerous times between February and April 2021 and across iOS releases. The most recent attempt showed the following indicators of compromise:
2	It is worth noting that among the many other malicious process names observed executed on this phone we see msgacntd, which we also found running on Omar Radi's phone in 2019, as documented earlier.

Section 6: Assertion Review

1. Amnesty's latest analysis focuses on the iPhone of another Moroccan journalist identified as CODE MOJRN1, named Hicham Mansouri. This marks the third Moroccan journalist to be extensively discussed in their "forensics methodology report."
2. Amnesty refers to the case of Omar Radi to associate the supposed 2021 attacks on Hicham Mansouri with the Pegasus software.
3.

Omar Radi's Forensic Traces

Characterizing this collection of forensics traces presented by Amnesty as undermining the entire field of mobile forensics, as it lacks traceability and lacks attributions for the listed "events." Furthermore, upon closer examination, it becomes apparent that these traces, supposedly representing detailed information for each target, as stated in the section titled "Appendix C: Detailed Traces per Target," do not align with the claims made throughout the methodology report. Specifically, the absence of com.apple.softwareupdateservicesd.plist, com.apple.CrashReporter.plist, and tahmilmilafate.com raises concerns. Additionally, section C.2 and section 2.1 present the same alleged malicious URLs but attribute different infection times down to the second. Likewise, the mentioned "bh" and "roleaboutd" display differing infection times down to the second in section C.2 and section 2.1. The sheer inconsistency within this data is sufficient grounds to dismiss all arguments put forth.

Table 5 Same Indicators of compromise different times show in different sections of the methodology report

Section C.2		Section 2.1	
2019-02-11 13:45:53	Safari favicon from URL hxxps://d9z3sz93x5ueidq3.get1tn0w.free247downloads[.]com:30897/rdEN5YP	2019-02-11 14:45:53	Safari Favicon record for URL hxxps//d9z3sz93x5ueidq3.get1tn0w.free247downloads[.]com:30897/rdEN5YP
2019-09-13 15:01:38	Safari favicon for URL hxxps://2far1v4lv8.get1tn0w.free247downloads[.]com:31052/meunsnyse#011356570257117296834845704022338973133022433397236	2019-09-13 17:01:38	https://2far1v4lv8.get1tn0w.free247downloads[.]com:31052/meunsnyse#011356570257117296834845704022338973133022433397236
2019-09-13 15:01:56	Safari favicon for URL hxxps://2far1v4lv8.get1tn0w.free247downloads[.]com:31052/meunsnyse#0680995616146262785199253586387891615724278336 45389	2019-09-13 17:01:56	https://2far1v4lv8.get1tn0w.free247downloads[.]com:31052/meunsnyse#0680995616146262785199253586387891615724278336 45389
2020-01-27 10:06:24	Safari favicon for URL hxxps://gnyjv1xltx.info8fvhgl3.urlpush[.]net:30875/zrnv5revj#074196419827987919274001548622738919835556748325946	2020-01-27 11:06:24	https://gnyjv1xltx.info8fvhgl3.urlpush[.]net:30875/zrnv5revj#074196419827987919274001548622738919835556748325946

Table 6 Same Indicators of compromise different times show in different sections of the methodology report

Section C.2		Section 2.1	
2019-02-11 13:45:56	Process: bh	2019-02-11 14:45:56	Process: bh
2019-02-11 13:46:23	Process: roleaboutd	2019-02-11 14:46:23	Process: roleaboutd first
2019-02-11 16:05:24	Process: roleaboutd	2019-02-11 17:05:24	Process: roleaboutd last

Conclusion

The practices of The Citizen Lab and Amnesty International have a troubling history of self-referencing and circular validation, which raises concerns about their credibility and objectivity. Key individuals such as Claudio Guarnieri, Etienne Maynier, Sarah Jane Beamish, and Ron Deibert have overlapping roles and connections, creating a network of relationships that challenge the idea of independent scrutiny and impartiality. Moreover, the undisclosed identities of the individuals or entities behind these organizations give rise to doubts about their motives and potential biases. A thorough investigation conducted earlier could have potentially uncovered signs of scientific and biased prejudice.

In the case of the Omar Radi spyware incident, The Citizen Lab and Amnesty International both support and reinforce each other's accusations, establishing a clear pattern of circular validation. The claim made by The Citizen Lab regarding an independent peer review of Amnesty International's methodology loses credibility due to the shared personnel and conflicting interests involved. Consequently, this compromises the objectivity and fairness of the investigation.

Amnesty International's response to the Moroccan government's demand for substantiating evidence further raises concerns about their credibility. The failure to provide comprehensive evidence and the delay in responding to official requests undermine the organization's claims of advocating for human rights.

The Forensic Methodology Report, co-authored by Amnesty International and verified by The Citizen Lab, lacks a systematic and replicable scientific approach. It primarily relies on speculative accusations rather than rigorous scientific methodology. The report's disproportionate focus on specific incidents in Morocco, particularly the case of Omar Radi, undermines its generalizability and applicability to different scenarios.

A comparison with recognized industry standards, such as ENISA's mobile forensics response methodology, highlights the shortcomings of Amnesty International's approach. ENISA's methodology adheres to industry standards and best practices, providing clear guidelines, rigorous evidence handling procedures, and a systematic approach to data acquisition and analysis. In contrast, Amnesty International's report lacks a defined scope, explicit protocols for evidence preservation, and a structured methodology for data analysis.

A critical examination of Omar Radi's findings within Amnesty International's methodology report reveals questionable claims and lack of concrete evidence. The reliance on speculative interpretations of Safari browsing history and the presence of a process named "bh" raises doubts about the validity of their attributions to NSO Group and the existence of malicious activities. Amnesty and The Citizen Lab's questionable "methodologies" call for a more critical and thorough evaluation of their practices to ensure transparency and accountability in the field of digital surveillance and human rights.

References

Adam BIELAN, A. F. (2023, January 18). *Joint motion for a resolution on the situation of journalists in Morocco, notably the case of Omar Radi: RC-B9-0057/2023: European Parliament*. JOINT MOTION FOR A RESOLUTION on the situation of journalists in Morocco, notably the case of Omar Radi | RC-B9-0057/2023 | European Parliament. https://www.europarl.europa.eu/doceo/document/RC-9-2023-0057_EN.html

Amnesty International. (2020a, June 22). *Moroccan journalist Omar Radi refuses to be silenced*. Amnesty International. https://www.amnesty.org/en/latest/news/2020/06/omar-radi-moroccan-journalist-refuses-to-be-silenced/

Amnesty International. (2020b, June 22). *Moroccan journalist targeted with network injection attacks using NSO group's tools*. Amnesty International. https://www.amnesty.org/en/latest/research/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools/

Amnesty International. (2021a, July 18). *Forensic methodology report: How to catch nso group's pegasus*. Amnesty International. https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

Amnesty International. (2021b, September 20). *Amnesty International Limited: Report and financial statements for the year ended 31 December 2020*. Amnesty International. https://www.amnesty.org/en/documents/fin40/4743/2021/en/

AmnestyTech. (2021a, July 19). Removing false positive · AmnestyTech/investigations@1c69421. https://github.com/AmnestyTech/investigations/commit/1c694217c3efb4e40f34822b6ef99a7b5bd8a064

AmnestyTech. (2021b, July 27). *False indication of pegasus · issue #19 · AmnestyTech/investigations*. GitHub. https://github.com/AmnestyTech/investigations/issues/19

Apple.com. (2012). *WebKitFaviconDatabase.cpp [plain text]*. WebKitFaviconDatabase.cpp. https://opensource.apple.com/source/WebKit2/WebKit2-7537.73.11/UIProcess/API/gtk/WebKitFaviconDatabase.cpp.auto.html

bahrainwatch.org. (2013, January 21). Bahrain Watch: About Us. https://web.archive.org/web/20130121160634/http://bahrainwatch.org/about.php

Bechtold, L. (2021, April 21). *Meet MGA alumna-turned-faculty, Sarah Beamish*. The Munk School. https://munkschool.utoronto.ca/mga/news/meet-mga-alumna-turned-faculty-sarah-beamish

The Citizen Lab. (2020, February 21). *People*. The Citizen Lab. https://web.archive.org/web/20200618113556/https://citizenlab.ca/people/

Gyewu, D., Zand, R., & Sharpe, D. (2019). *University of Toronto Human ethics principles & guidelines*. Human Ethics Principles & Guidelines | Ethics in Human Research. https://research.utoronto.ca/ethics-human-research/human-ethics-principles-guidelines

Le 360 Français. (2020, July 2). *Vidéo. Affaire Omar Radi: Le gouvernement exige de Nouveau une réponse officielle d'amnesty*. Le 360 Français. https://fr.le360.ma/politique/video-affaire-omar-radi-le-gouvernement-exige-de-nouveau-une-reponse-officielle-damnesty-218462/

Lookout. (2016, December 13). Whitepaper technical analysis of the pegasus exploits on IOS. https://info.lookout.com/rs/051-ESQ-475/images/pegasus-exploits-technical-details.pdf?ref=wonderfall

Marczak, B., Scott-Railton, J., Anstis, S., & Deibert, R. (2021, July 19). *Independent peer review of Amnesty International's forensic methods for identifying pegasus spyware*. The Citizen Lab. https://citizenlab.ca/2021/07/amnesty-peer-review/

Marquis-Boire, M., Marczak, B., Guarnieri, C., & Scott-Railton, J. (2013, March 13). *You only click twice: Finfisher's Global Proliferation - Citizen Lab*. The Citizen Lab. https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/

Palkmets, L. (2015, April 16). ENISA Mobile threats incident handling. https://www.enisa.europa.eu/topics/training-and-exercises/trainings-for-cybersecurity-specialists/online-training-material

Privacy International. (2012, June 3). *Our people*. Privacy International - Advisors. https://web.archive.org/web/20120603060951/https://privacyinternational.org/people

Privacy International. (2013, March 7). *Our people*. Privacy International - Advisors. https://web.archive.org/web/20130307220652/https://privacyinternational.org/people privacyinternational.org. (2013, February 3). Briefing note on OECD Complaints against Gamma International and Trovicor in the UK and Germany. https://web.archive.org/web/20130308002112/https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/2013_02_01_oecd_briefing_note.pdf

Raghave. (2023, March 24). *Would this imply, in the specific case of @svaradarajan/@mkvenu1, that @thewire_in/@amnestytech's conclusion that their phones were infected (and hence they were targets of surveillance) based on Plist Indicator is erroneous? CC: @runasand can you also confirm/deny? pic.twitter.com/roc4hlofhm*. Twitter. https://twitter.com/_Raghave/status/1639264188576190464?s=20

Scott, J. (2022a, October 12). *There is a blog post going around calling me Alex Jones of cybersecurity....i'm not surprised to see who stands behind it. @tenacioustek @runasand @jsrailton, @citizenlab, @AmnestyTech and of course all part of https://t.co/suqhc32yo4a "special interest group" pic.twitter.com/lgjdnetkv8*. Twitter. https://twitter.com/jonathandata1/status/1580236372593344518?s=20

Scott, J. (2022b, November). Review of Catalangate Amnesty International Validation. https://www.researchgate.net/publication/365743925_Review_of_Catalangate_Amnesty_International_Validation