FMDB *Transactions on Sustainable Computing Systems*

Critical Analysis and Countermeasures Tactics, Techniques, and Procedures (TTPs) that Targeting Civilians: A Case Study on Pegasus

Osama Hussien[1,*], Usman Butt[2], Rejwan Bin Sulaiman[3]

[1,2,3]Department of Computer Science and Engineering, Northumbria University, Middlesex Street, London, United Kingdom.
ossama.akram@northumbria.ac.uk[1], usman.butt@northumbria.ac.uk[2], rejwan.sulaiman@northumbria.ac.uk[3]

Abstract: Individuals, businesses, and governments all face additional difficulties because of the rise of sophisticated cyberattacks. This paper examines the targeting of journalists and activists by the Pegasus malware. To gain a deeper understanding of the tactics utilised by cybercriminals and the vulnerabilities that facilitate their scope, this research examines numerous occurrences. It identifies recurring patterns in the strategies, methods, and practices employed. In this paper, a comprehensive analysis is conducted of the far-reaching consequences of these attacks for cybersecurity policy, encompassing the pressing need for enhanced threat intelligence-sharing mechanisms, the implementation of more resilient incident response protocols, and the allocation of greater financial resources to advance cybersecurity research and development initiatives. The research also discusses how Pegasus will impact SCADA systems and critical infrastructure. It outlines some of the most crucial tactics businesses can employ to mitigate the risk of cyberattacks and protect themselves against the evolving threats of the 21st century. The extent of Pegasus spyware, which can access various data and communications on mobile devices running iOS and Android, potentially jeopardises the civil rights and privacy of journalists, activists, and political leaders worldwide. It was found to be worrying.

Keywords: Pegasus Spyware; Cyberattack Tools; Cybersecurity Policy; SCADA Systems; Critical Infrastructure; Privacy and Civil Liberties; Threat Intelligence Sharing; Incident Response Plans; Natural Language Processing.

Received on: 02/10/2024, **Revised on:** 17/12/2024, **Accepted on:** 21/01/2025, **Published on:** 05/06/2025

Journal Homepage: https://www.fmdbpub.com/user/journals/details/FTSCS

DOI: https://doi.org/10.69888/FTSCS.2025.000435

Cite as: O. Hussien, U. Butt, and R. B. Sulaiman, "Critical Analysis and Countermeasures Tactics, Techniques and Procedures (TTPs) that Targeting Civilians: A Case Study on Pegasus," *FMDB Transactions on Sustainable Computing Systems*, vol. 3, no. 2, pp. 114-121, 2025.

1. Introduction

Cyberattacks targeting major businesses, human rights advocates, and journalists have increased in the past decade [1]; [2]. The assaults damaged essential infrastructure, damaged finances, and damaged reputations. Attacks are becoming more frequent and sophisticated due to a range of factors, including the use of linked devices, cloud computing, and hackers' utilisation of AI and machine learning. The Pegasus malware, used to covertly access and examine mobile devices in the modern era, stands out as one of the most notable threats. State-sponsored actors and other groups use this tool to target human rights

[*]Corresponding author.

defenders, journalists, and activists, causing widespread disruption. This underscores the need for individuals and organisations to understand the latest hacking techniques and how to defend against them as the threat landscape evolves. The author will analyse the Pegasus spyware attack, including cybercriminal tactics and vulnerabilities, and briefly mention other common attacks in this research paper.

Comprehensively, the author will provide an overview of crucial tactics and techniques that both individuals and organisations can effectively utilise to safeguard themselves against the constantly evolving threat of cyber-attacks. The selection of Pegasus attacks and techniques was intended to provide a broad overview of different types of attacks and TTPs in phishing, while still focusing on the most significant and recent incidents, such as Pegasus. The investigation aims to strengthen cyber safety by analysing incidents, deliberating on preventive measures, and understanding how to safeguard against emerging threats. This paper aims to provide an in-depth and comprehensive account of the Pegasus spyware, detailing its extensive and harmful impact on the fundamental rights of privacy and civil liberties, which are severely compromised by governments' covert and surreptitious monitoring of journalists and activists. Additionally, it seeks to emphasise the dangers and risks posed by Pegasus spyware, coupled with a thorough examination of the TACTICS, TECHNIQUES, AND PROCEDURES (TTPs) utilised by cyber offenders to carry out comparable attacks. The central focus of this manuscript is the scrutiny and assessment of the methodologies used in the execution of contemporary and renowned cyberattacks, accompanied by an in-depth discussion on the most effective tactics and precautionary measures that can be implemented to minimize the risk of future attacks.

2. Literature Review

2.1. Section Remarks

This section examines recent attacks/techniques using Pegasus. Additionally, it provides a critical evaluation of the nature of these attacks, the methods employed, and the potential effects on both enterprises and individuals. The study also examines potential defences against such attacks, as well as the analysis and reflections that might be made in response to them.

2.2. Introduction and History

Pegasus is spyware developed by the Israeli cyber-arms company NSO Group, which can be covertly installed on mobile phones (and other devices) running most versions of iOS and Android. Pegasus can exploit iOS versions up to 14.7 through a zero-click exploit, allowing it to infect a device without requiring any user interaction [3]. Pegasus can access various data and functions on the infected device, including contacts, messages, photos, the microphone, camera, and location (Figure 1).

Figure 1: Documentation reveals Pegasus can access various data from infected devices

One of the most notorious Pegasus spyware deployments involved hacking the smartphone of Amazon and Washington Post owner Jeff Bezos. The Saudi Arabian government reportedly organised the event as punishment for the Washington Post's critical coverage of the country, according to sources [5]. This incident demonstrated Pegasus's potential to target influential figures and compromise their personal and professional data. However, Bezos was not the only victim of Pegasus. In 2019, WhatsApp discovered that Pegasus had been used to hack into the phones of multiple activists and journalists in India [6]. These attacks raised questions about the role of Pegasus in suppressing dissent and undermining democracy in India. Moreover, Pegasus has been implicated in violating the rights of human rights defenders in Palestine. In July 2021, an investigation by Front Line Defenders (FLD), a Dublin-based human rights group, found that the mobile phones of Palestinian rights defender

and lawyer Salah Hammouri and five others were hacked using Pegasus [7]. This attack was particularly alarming given that Hammouri's Jerusalem residency status had already been revoked, raising concerns that the spyware was being used to further curtail his human rights work [7].

2.3. Methodology

The first Pegasus version, dating back to 2016, was CVE-2016-4657 in Apple's WebKit. This open-source browsing engine allowed third-party developers and even rivals to incorporate it into their own products. For instance, the Nintendo Switch was vulnerable to this vulnerability because it used WebKit in its native internet browser, which was intended only for connecting to networks with captive portals [9]. Due to a flaw in WebKit's JavaScript engine, it can be vulnerable to this attack. The threat actor exploits the CVE-2016-4657 flaw to gain access to Safari's memory in WebKit [8]. After that, malware is installed on the target device that exploits the kernel memory-addressing leak caused by CVE-2016-4655 [10]. Apple's deserialization approach lacks a size-checking function for one of the user-provided parameters that represents a 64-bit integer, allowing this malware to proceed. The iOS kernel's address space configuration randomisation option, which randomly generates the kernel image base through the boot loader before each boot, can thus be determined by the threat actor using this vulnerability [11]. To mitigate the Pegasus vulnerability, which allows the installation of a surveillance tool on the target's device, the malware initially deactivates code signing. Code signing ensures that code is secure and authentic. Disabling code signing is analogous to a doctor permitting a patient to ingest any substance, regardless of its safety. Another flaw, CVE-2016-4656 [12], enables the malware to reallocate previously freed memory from a string and insert a stack pivot into the NULL page, allowing it to execute code in a privileged environment. The vulnerability enables root access by granting an attacker a shell [11].

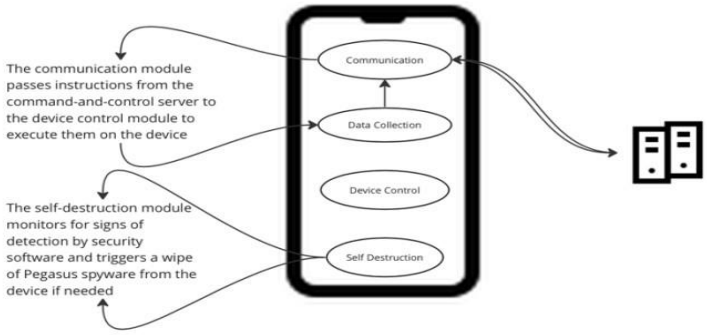

Figure 2: Inner working and methodology of Pegasus

According to Ibarra et al. [18], this section concludes that Pegasus contains several key components, as described in Figure 2, starting with the Communication module, which is responsible for sending and receiving data between the device and the command-and-control server controlled by the attacker.

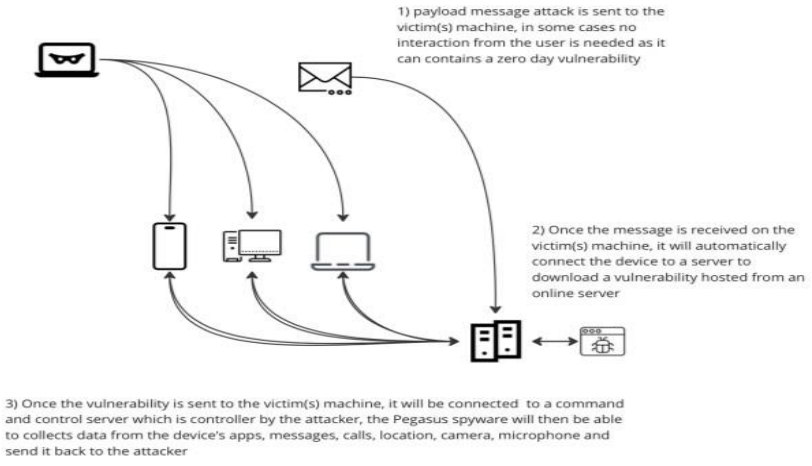

Figure 3: Pegasus exploitation process

The Data Collection Module is responsible for collecting data from various sources on the device, including messages, calls, photos, videos, location, passwords, and apps. At the same time, the Device Control module is responsible for controlling the device's functions, such as turning the microphone or camera on or off, recording audio or video, or deleting files or apps. Finally, the Self Destruction module is responsible for removing traces of Pegasus spyware from the device when instructed by the attacker or when detected by security software. Figure 3 summarises how the Pegasus exploits zero-day vulnerabilities to attack any vulnerable device [18].

2.4. General Impact

The Pegasus vulnerability poses a grave risk to privacy and civil liberties, as it enables governments and other hostile actors to infiltrate individuals and organisations without their awareness or consent [13]. The ability to remotely access confidential data and communications on a mobile device constitutes a severe breach of privacy and a potential instrument of surveillance and censorship. A major concern about Pegasus is that it can be used to target journalists, activists, and other individuals who oppose government policies or are involved in human rights work [13]. By tracking their communication and activities, governments can monitor and intimidate these individuals, potentially silencing free speech and limiting civil liberties (Figure 4).

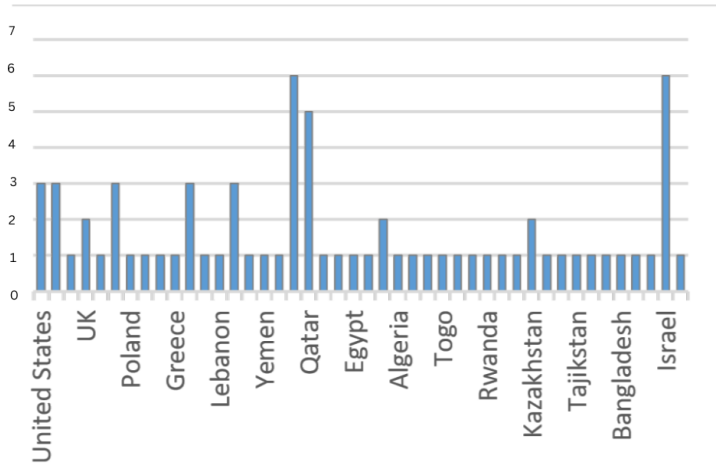

Figure 4: Suspected Pegasus usage intensity in different companies

The global reach and impact of Pegasus spyware on human rights were revealed by a report based on DNS cache probing of domain names extracted from command-and-control (CandC) servers. The report Albergotti et al. [4] found that at least 45 countries were suspected of having Pegasus infections, operated by at least 33 likely NSO customers, including governments, intelligence agencies, and law enforcement agencies. The report also noted that Pegasus had been used to target journalists, activists, and opposition politicians in various countries, raising concerns about privacy violations and civil liberties. The report called for greater transparency from companies like NSO Group, the Israeli company that developed Pegasus, and for greater regulation of the surveillance industry to prevent abuses. However, the Pegasus vulnerability also poses challenges for governments in regulating and monitoring the development and use of cyberweapons. While some believe it is the duty of governments to safeguard their populations from cyber threats, others argue that the widespread use of technologies like Pegasus can weaken democracy and may ultimately be ineffective in the battle against terrorism and other criminal behaviour [14]. Therefore, when dealing with cyberweapons like Pegasus, an approach that balances security and human rights concerns must be adopted.

Tight rules for the creation and use of these tools are required in light of the major concerns highlighted by the use of Pegasus spyware, as well as the increasingly sophisticated nature of cyberattacks. The NSO Group has been under scrutiny for providing its spyware to nations with a history of human rights violations. Requests for stricter export controls have increased in recent years, leading to its inclusion on the US Blacklist as of [15]. The widespread use of Pegasus and other advanced spyware highlights the need for greater regulation and oversight of the cybersecurity industry to prevent the abuse of these tools by authoritarian regimes and other malicious actors. More openness and accountability in the creation and use of cyberweapons are required to address these issues. Authorities must be held accountable for any misuse of their authority or invasion of privacy that occurs as a result of using these technologies and spyware [38]. They should be forced to report how they use them. There should be increased efforts to support and safeguard human rights and privacy, particularly by enhancing encryption and developing additional privacy-enhancing technologies [16].

2.5. SCADA Impact

Another serious threat posed by Pegasus is the compromise of the operational integrity and reliability of SCADA systems and critical infrastructure. By exploiting various vulnerabilities in SCADA systems, Pegasus spyware can access and manipulate data, commands, sensors, actuators, and other components of these systems [37]. This could result in loss of control, malfunctioning, damage, or shutdown of critical processes and equipment. For example, Pegasus spyware could alter the pressure or temperature readings of a gas pipeline or a nuclear reactor, causing leaks or explosions Alternatively, it could disrupt the power supply or communication networks of a transportation system or a hospital, affecting the safety and efficiency of these services and with the power of being able to infiltrate devices with zero clicks, it can be catastrophic. It can also have significant financial implications. A cyberattack on these systems could result in direct costs, such as repair expenses, fines, lawsuits, compensation claims, or ransom payments [17].

Moreover, it could result in indirect costs, such as loss of revenue, damage to reputation, customer dissatisfaction, or a competitive disadvantage. For instance, Pegasus spyware could steal confidential information or trade secrets from an industrial company or a utility provider, thereby giving its competitors or adversaries a significant advantage. Additionally, Pegasus spyware could expose sensitive data, such as personal, financial, or health records, of customers or employees of these systems, leading to identity theft or fraud [18]. Researchers at NIST NVD [19] highlight the challenge posed by zero-day vulnerabilities in SCADA Systems that malicious actors can exploit before they are patched. A recent example of such a vulnerability is CVE-2021-30860, which was exploited by the Pegasus spyware to infect iOS devices without user interaction [20]. The paper's analysis and suggestions are also relevant and timely for cybersecurity and human rights, given the Pegasus vulnerability and its misuse by authoritarian governments. The same researcher proposed a simulation and detection framework to protect SCADA systems against ransomware attacks that exploit zero-day vulnerabilities such as Pegasus [21].

2.6. Covid-19 and Hybrik/From Homework Environment Impact

According to Pliatsios et al. [17], the large number of Internet of Things (IoT) devices connected to home networks is one reason they are vulnerable to Pegasus. According to Pliatsios et al. [17], in the digital age, the average family has 10 IoT gadgets. The more Internet of Things devices there are, the easier it is for hackers to gain access to networks by exploiting vulnerabilities. Additionally, 59.7% of residents had routers susceptible to hacking and were not changing their passwords [18]. To prevent these threats, some governments and organisations have strict policies that forbid employees from using their own devices for work purposes [19]; [20]. Other security measures include updating cyber hygiene practices, providing security awareness training, and revising cyber hygiene rules. However, these precautions may not be sufficient to stop advanced attacks such as Pegasus [21]. Researchers at Pliatsios et al. [17] also highlight other challenges and threats faced by remote workers who are working from home due to the global pandemic. However, they proposed some robust protocols for organisations to protect their remote workers and corporate networks from cyberattacks. However, these protocols may not be enough to prevent the Pegasus spyware, which can exploit zero-day vulnerabilities. Remote workers who use their personal devices for work may be at risk of this spyware, which could compromise their sensitive data and networks [36].

2.7. Related and Similar Attack Vectors

These recent attacks have highlighted the importance of maintaining up-to-date security systems, replacing legacy systems, implementing regular backups, providing security awareness training, and enabling multi-factor authentication to guard against unauthorised access. This ransomware attack is one of many examples of the rise in global cyber threats [17]. Other notable examples include the 2017 Equifax data breach and the 2016 hack of the DNC, both high-profile cyberattacks that occurred in recent years [18]. State-sponsored cyberattacks are also becoming more frequent [19]; [20]. The governments of China and Russia were charged with funding cyber espionage against numerous U.S. agencies and commercial companies [21]; [22]. To guard against such attacks, organisations must adopt strict safety protocols, such as access controls, multi-factor authentication, and frequent security assessments.

3. Tactics, Techniques, Procedures, and Counter Measures

Cybersecurity is a critical concern in today's digital world, with cyberattacks becoming increasingly prevalent and sophisticated [35]. Attackers penetrate networks, steal data, and create disruption using a range of attack vectors and TTP. It may be difficult and slow down the process of identifying an attacker's TTPs when retrieving security data from unstructured material [23]. The problem was addressed by several researchers using a variety of approaches, including a thorough evaluation of various Natural Language Processing (NLP) and machine learning techniques, most notably a data processing pipeline that classifies unstructured content into attackers' tactics and techniques by using a knowledge base of adversary TTPs that makes it possible for textual data to be automatically and promptly extracted to extract crucial security information, supporting efficient threat detection and response [24]. One common TTP used by attackers is social engineering and phishing attacks [25]. It entails

coercing people into disclosing private information or allowing access to systems. Other TTPs used to obtain unauthorised access to systems and data include spear-phishing, malware, and brute-force assaults. Attackers also employ tactics such as ransomware to encrypt private information and demand payment from their targets [34]. To create effective defences and safeguard against cyberattacks, it is essential to understand the TTPs attackers use. To protect themselves against these risks, organisations must develop effective security measures and stay up to date with the latest TTPs (Table 1).

Table 1: Types of breaches or attacks in 2022, among the organisations

Attack Type/Organisation Type	Organization	Charities
Phishing	83	87
Impersonation	27	26
General Malware	12	11
Denial Of Service	10	2
Online Banking Attack	8	6
Organisation Account Takeover	8	6
Ransomware	4	4
Outsider unauthorised access	2	2
Unauthorised listening to video conference/ or Instant Messages	1	3
Insider unauthorised access	1	1

To defend against these attacks, individuals and organisations must also implement best cybersecurity practices, such as regularly updating software and hardware to address vulnerabilities, using strong passwords, and limiting access to sensitive information [26]. Security protocols such as firewalls, intrusion detection and prevention systems, endpoint protection software, encryption technologies, and Security Information and Event Management (SIEM) tools can be used to aggregate and analyse security events across the network, providing greater visibility into potential threats and help mitigate any unauthorised access to systems and data [27]. Regular security assessments and employee training on recognising and avoiding cyberattacks can also significantly reduce the risk of successful attacks. The Pegasus attacks are a prime example of how state-sponsored actors can utilise sophisticated spyware to compromise the security of mobile devices. Keeping mobile devices updated with the latest security patches, using strong passwords, and being cautious of unknown links and attachments are important countermeasures [28].

Common methods used in cyberattacks include phishing, malware, social engineering, and credential stuffing. These methods exploit flaws in software, hardware, or human factors to access systems and data, which can be executed with less technical knowledge, thanks to tools such as Metasploit and the Burp Suite [29]. Organisations must educate their employees about these techniques and regularly conduct vulnerability assessments and penetration testing to identify potential weaknesses [30]. The success of cyberattacks can be attributed to unremediated software, weak passwords, and unpatched hardware vulnerabilities [31]. To effectively shield their networks from looming threats and safeguard confidential data, it is of utmost importance for enterprises to take a pre-emptive approach to security by enforcing rigorous entry controls, conducting regular security inspections, and utilising state-of-the-art security mechanisms [32]. The malevolent acts of cybercriminals are a formidable menace; therefore, it is imperative to take measures to safeguard oneself against them. By adopting a proactive cybersecurity stance and staying informed about the latest threats, individuals and organisations can significantly reduce the likelihood of falling victim to digital attacks [33].

4. Conclusion

It is essential to create a comprehensive plan to defend against such threats as the complexity and severity of cyberattacks increase, to effectively reduce the associated risks. Undoubtedly, the appearance of Pegasus is a particularly unsettling example of such attacks because it exploits a variety of vulnerabilities in iOS devices to infect and track its victims without their knowledge or consent. This paper emphasises the importance of understanding the TTPs attackers use, discussing vulnerabilities and countermeasures to provide valuable insights for organisations and individuals. Implementing best practices such as strong passwords, regular security assessments, and advanced security technologies can help mitigate the risk of exploitation of known vulnerabilities. Users must nevertheless routinely update their devices and be vigilant for any unusual behaviour. It is crucial for governments and international organisations to regulate the use of cyberarms, such as Pegasus, and to hold those responsible for their misuse accountable.

Acknowledgment: The authors sincerely acknowledge Northumbria University for its support and resources that contributed to the successful completion of this research work.

Data Availability Statement: The data supporting the results of this study are available from the corresponding author upon reasonable request. All authors confirm that the data have been accurately collected and reported.

Funding Statement: This research work and manuscript were conducted independently by the authors without any external funding or financial assistance.

Conflicts of Interest Statement: The authors declare that there are no conflicts of interest associated with this research or its publication. This work represents their original contribution, and all relevant references have been properly cited.

Ethics and Consent Statement: The study was carried out in accordance with recognized ethical standards. Informed consent was obtained from all participants, and the authors collectively ensured compliance with the principles of ethical research throughout the study.

References

1. B. Marczak and J. Scott-Railton, "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender," *Citizen Lab*, 2016. Available: https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/ [Accessed by 04/08/2024].
2. Z. A. Sairafi, "Cybersecurity challenges for Human Rights Defenders in Gulf Cooperation Council (GCC) countries," *Diss. Central European University*, 2022. Available: https://www.etd.ceu.edu/2022/al-sairafi_zainab.pdf [Accessed by 08/08/2024].
3. B. Marczak, J. Scott-Railton, S. Mckun, and R. Deibert, "HIDE AND SEEK Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," 2018. Available: https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/ [Accessed by 01/08/2024].
4. R. Albergotti, C. Timberg, and J. Greene, "Jeff Bezos's IPhone Had Apple's State-ofthe-Art Security, and That May Have Helped Its Alleged Hackers," 2020. Available: https://www.washingtonpost.com/technology/2020/01/29/apple-iphone-bezos-hack/ [Accessed by 01/08/2024].
5. H. Pullanoor, "Explained: How Pegasus Is Used to Hack into Phones to Spy on Users," 2021. Available: https://www.ndtv.com/india-news/what-is-pegasusspyware-explained-2489195 [Accessed by 20/08/2024].
6. Front Line Defenders, "Press Release - Front Line Defenders Investigation Finds Pegasus Spyware on 6 Palestinian HRD Phones," 2021. Available: https://www.frontlinedefenders.org/en/press-release-front-line-defenders-investigation-finds-pegasus-spyware-6-palestinian-hrd-phones [Accessed by 18/08/2024].
7. NIST, "CVE-2016-4657," 2016. Available: https://nvd.nist.gov/vuln/detail/CVE-2016-4657 [Accessed by 16/08/2024].
8. A. Carman, "Nintendo Switch's Secret Browser Has a Flaw That Could Lead to a Jailbreak.," 2017. Available: https://www.theverge.com/circuitbreaker/2017/3/14/14921138/nintendo-switchexploit-jailbreak-webkit-vulnerability [Accessed by 28/08/2024].
9. NIST, "CVE-2016-4655," 2016. Available: https://nvd.nist.gov/vuln/detail/CVE-2016-4655 [Accessed by 18/08/2020].
10. Jndok, "Analysis and Exploitation of Pegasus Kernel Vulnerabilities (CVE-2016-4655 / CVE-2016-4656)," 2016. Available: http://jndok.github.io/2016/10/04/pegasus-writeup [Accessed by 02/06/2024].
11. NIST, "CVE-2016-4656," 2016. [Available: https://nvd.nist.gov/vuln/detail/CVE-2016-4656 [Accessed by 28/08/2024].
12. J. D. Rudie, Z. Katz, S. Kuhbander, and S. Bhunia, "Technical Analysis of the NSO Group's Pegasus Spyware," *in 2021 International Conference on Computational Science and Computational Intelligence (CSCI)*, Las Vegas, Nevada, United States of America, 2021.
13. A. Chawla, "Pegasus Spyware – 'A Privacy Killer'," 2021. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3890657 [Accessed by 30/08/2024].
14. C. J. Bennett, "The Privacy Advocates: Resisting the Spread of Surveillance," *The MIT Press*, Cambridge, Massachusetts, United States of America, 2008.
15. D. E. Sanger, N. Perlroth, A. Swanson, and R. Bergman, "U.S. Blacklists Israeli Firm NSO Group over Spyware.," 2021. Available: https://www.nytimes.com/2021/11/03/business/nso-group-spyware-blacklist.html [Accessed by 21/08/2024].
16. J. L. Koepke and D. G. Robinson, "Danger ahead: Risk assessment and the future of bail reform," *Wash. L. Rev*, vol. 93, no. 4, pp. 1725-1807, 2018.
17. D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, "A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 3, pp. 1942-1976, 2020.

18. J. Ibarra, U. J. Butt, A. Do, H. Jahankhani, and A. Jamal, "Ransomware Impact to SCADA Systems and its Scope to Critical Infrastructure," *in 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, London, United Kingdom, 2019.
19. NIST NVD, "CVE-2021-30860 Detail," 2021. Available: https://nvd.nist.gov/vuln/detail/CVE-2021-30860 [Accessed by 21/08/2024].
20. U. J. Butt, M. Abbod, A. Lors, H. Jahankhani, A. Jamal, and A. Kumar, "Ransomware Threat and its Impact on SCADA," *in 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, London, United Kingdom, 2019.
21. U. J. Butt, W. Richardson, A. Nouman, H. M. Agbo, C. Eghan, and F. Hashmi, "Cloud and its security impacts on managing a workforce remotely: A reflection to cover remote working challenges," *in Cybersecurity, Privacy and Freedom Protection in the Connected World: Proceedings of the 13th International Conference on Global Security, Safety and Sustainability*, London, United Kingdom, 2021.
22. F. Schmidt, "Tapping fiber optics," 2013. Available: https://www.dw.com/en/tapping-the-worlds-fiber-optic-cables/a-16916476 [Accessed by 11/08/2024].
23. Avast, "Avast Smart Home: Security Report 2019," 2019. Available: https://cdn2.hubspot.net/hubfs/486579/avast_smart_home_report_feb_2019.pdf [Accessed by 08/08/2024].
24. O. F. N. Statistics, "Coronavirus and homeworking in the UK," Office for National Statistics, 2020. Available: https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/bulletins/coronavirusandhomeworkingintheuk/april2020 [Accessed by 01/08/2024].
25. R. B. Sulaiman, "Future threats to Internet of Things (IoT) security and privacy: A survey," 2019. Available: https://www.researchgate.net/publication/338150171_Future_Threats_to_Internet_of_Things_IoT_Security_Privacy_A_Survey [Accessed by 08/08/2024].
26. N. Daswani and M. Elbayadi, "The Equifax Breach," in Big Breaches, *Apress*, New York, United States of America, 2021.
27. C. Lam, "A slap on the wrist: Combatting Russia's cyber-attack on the 2016 US presidential election," *BCL Rev.* vol. 59, no. 6, pp. 2167-2201, 2018.
28. K. -K. R. Choo and P. Grabosky, "CyberCrime", in Letizia Paoli (ed.), The Oxford Handbook of Organized Crime, *Oxford Handbooks, Oxford University Press*, Oxford, United Kingdom, 2014.
29. W. C. Banks, "Cyber espionage and electronic surveillance: Beyond the media coverage," *Emory LJ*, vol. 66, no. 3, pp. 513-525, 2017.
30. E. Iasiello, "China's three warfares strategy mitigates fallout from cyber espionage activities," *Journal of Strategic Security*, vol. 9, no. 2, pp. 45-69, 2016.
31. J. Wiggen, "The impact of COVID-19 on cyber-crime and state-sponsored cyber activities," *Konrad Adenauer Stiftung*, 2020. Available: http://www.jstor.org/stable/resrep25300 [Accessed by 08/08/2024].
32. C. Sauerwein, I. Pekaric, M. Felderer, and R. Breu, "An analysis and classification of public information security data sources used in research and practice," *Computers and security*, vol. 82, no. 5, pp. 140-155, 2019.
33. C. Sauerwein and A. Pfohl, "Towards Automated Classification of Attackers' TTPs by combining NLP with ML Techniques," *arXiv preprint arXiv:2207.08478*, 2022. Available: https://arxiv.org/abs/2207.08478 [Accessed by 29/08/2024].
34. GOV.UK, "Cyber Security Breaches Survey 2022," *GOV.UK*. 2022. Available: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022 [Accessed by 24/08/2024].
35. K. Arlitsch and A. Edelman, "Staying safe: Cyber security for people and organizations," *Journal of Library Administration*, vol. 54, no. 1, pp. 46-56, 2014.
36. G. González-Granadillo, S. González-Zarzosa, and R. Diaz, "Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures," *Sensors*, vol. 21, no. 14, pp. 1-28, 2021.
37. M. Agrawal, G. Varshney, K. P. Singh, S. Kakandwar, and M. Verma, "Pegasus: Zero-Click spyware attack – its and challenges," *ResearchGate*, 2022. Available: https://www.researchgate.net/publication/357956844_Pegasus_Zero-Click_spyware_attack_-its_countermeasures_and_challenges [Accessed by 16/08/2024].
38. H. Holm and T. Sommestad, "So long, and thanks for only using readily available scripts," *Information and Computer Security*, vol. 25, no. 1, pp. 47-61, 2017.