Digital Dictatorship: The Psychological Impact of State-Sponsored Cyberattacks on Gulf Corporation Council Dissidents

Ali Abdulemam

Master of Science by research

University of York

Computer Science

December 2023

Abstract

This dissertation presents a critical examination of the psychological repercussions of state-sponsored cyberattacks on dissidents within the Gulf Cooperation Council (GCC)1 states with a specific focus on the deployment of advanced spyware such as Pegasus. This study addresses several critical research questions: What are the specific psychological consequences of such attacks on dissidents, and how do they manifest in their daily lives? How does the persistent threat of surveillance contribute to anxiety, paranoia, or other psychological distress? Furthermore, how do these cyberattacks affect victims' trust in digital infrastructure, leading to self-censorship? The research also investigates how technical mechanisms, such as zero-click exploits, amplify feelings of vulnerability and powerlessness. Finally, it critically examines the legal landscape surrounding these attacks, assessing the efficacy of current policies and avenues for victim recourse.

A mixed-methods research design was employed to address these questions, integrating quantitative, qualitative, technical, and legal analyses. Quantitative data were derived from structured questionnaires administered to 16 participants, utilizing the Harvard Trauma Questionnaire (HTQ) to assess trauma symptomatology. These data were supplemented by in-depth qualitative interviews exploring the lived experiences of targeted individuals. The empirical investigation was supported by a technical deconstruction of Pegasus spyware and a critical review of relevant legal frameworks.

The findings reveal pervasive psychological distress among dissidents, including chronic stress and social isolation. The technical analysis confirms that the covert nature of zero-click exploits is a primary contributor to victims' sense of powerlessness. The legal analysis identifies a significant accountability void, with existing policies proving inadequate for protecting individuals or providing effective recourse. This research underscores the urgent imperative for comprehensive policy reforms, including stricter regulation of surveillance technologies and the establishment of robust international legal norms to ensure state accountability and safeguard human rights in the digital era.

[1] Gulf Cooperation Council is a regional union comprising six countries, Bahrain, Kuwait, Oman, Saudi Arabia and United Arab Emirates

Declaration :

I declare that this thesis is a presentation of original work, and I am the sole author. This work has not previously been presented for an award at this, or any other, University. All sources are acknowledged as References.

Table of Contents

1 Introduction

The Internet has undergone a profound transformation over the past three decades, evolving into a fundamental pillar of contemporary society [1, 2]. Its pervasive influence permeates diverse sectors, encompassing commerce, finance, healthcare, and critical infrastructure [3]. Characterized by an unprecedented rate of adoption, the Internet has revolutionized communication paradigms, facilitated ubiquitous information access, and fundamentally reshaped economic activities [3, 4]. Moreover, it has emerged as a vital platform for civil society engagement and political discourse [5].

While the internet offers numerous advantages, its inherent architecture and widespread adoption introduce significant security and privacy challenges. The reliance on the Border Gateway Protocol (BGP) for routing traffic across a global network creates vulnerabilities, including data interception and compromise of integrity, confidentiality, and availability [6]. Although these vulnerabilities are critical at the infrastructure level, they are amplified at the user level due to limited security awareness among many individuals. This widespread vulnerability necessitates a comprehensive approach to cybersecurity that encompasses both technological solutions and user education. [7].

Journalists, human rights defenders (HRDs), legal professionals, activists, and civil society members increasingly rely on the internet to conduct their professional and advocacy activities [8]. However, this reliance exposes them to a unique and heightened set of security challenges. While engaged in critical activities such as promoting freedom of expression, advocating for political and social reform, and exposing corruption, these individuals are subjected to intense scrutiny by state authorities seeking to monitor their activities, networks, and information [9]. Consequently, surveillance and spyware technologies have become essential tools for governments to gain surreptitious access to electronic devices and extract sensitive data. This intrusive surveillance poses a significant threat to the privacy, safety, and freedom of expression of targeted individuals.

The deliberate targeting of dissidents through sophisticated cyberattacks has become an increasingly prevalent and alarming phenomenon, attracting significant international attention. High-profile data leaks exposing the extensive scope of state-sponsored surveillance operations have revealed a disturbing global pattern, with individuals perceived as threats, including dissidents, journalists, human rights defenders, public figures, politicians, and government officials, being systematically targeted [9-12]. These revelations underscore the pervasive nature of this threat to fundamental human rights, particularly the right to privacy and freedom of expression, highlighting the urgent need for robust legal frameworks and technological safeguards to protect vulnerable individuals. This study argues that the infliction of psychological harm is not merely a consequence of such surveillance but a primary strategic objective, a form of weaponized abuse designed to neutralize dissent and control public discourse.

1.1 Why This Study is Important

The deployment of spyware to target dissidents has become a critical tool for certain governments. The substantial financial investment required to acquire and operate these sophisticated surveillance technologies underscores their strategic importance. For example, the acquisition and operation of Pegasus, a leading spyware product, entail significant expenditures, with costs ranging from hundreds of thousands to millions of dollars [13, 14]. Notably, these figures exclude ongoing maintenance fees and do not account for the development and operational costs incurred by spyware producers. Such substantial investments highlight the prioritization of surveillance capabilities within the strategic objectives of these governments. .

The acquisition of spyware technology, despite the substantial financial investment it necessitates, has become a strategic imperative for certain governments aiming to monitor and control dissidents. The global spyware market has experienced significant growth, with sophisticated products like Pegasus attaining the status of a national asset, subject to strict export controls [15]. Conversely, the black market provides alternative acquisition channels, often operating with fewer legal and ethical constraints [16-18]. While governments frequently cite national security imperatives to justify spyware deployment, evidence suggests that in non-democratic states [19], in particular, innocent civilians, including human rights defenders, journalists, and political opponents, are disproportionately targeted and adversely affected by these intrusive surveillance practices. This raises serious concerns regarding the potential for abuse, the erosion of fundamental rights, and the chilling effect such surveillance has on freedom of expression and political dissent.

The ramifications of such attacks extend beyond the immediate extraction of data. Victims may experience significant psychological distress, including anxiety, depression, and post-traumatic stress disorder, in addition to potential legal repercussions and reputational damage resulting from the exposure of private information. Moreover, the long-term psychological consequences of these attacks are often complex and challenging to identify, particularly among individuals accustomed to high-stress environments, such as human rights defenders and journalists, who may exhibit resilience or employ coping mechanisms that mask underlying trauma. This research posits that the harm extends beyond generalized distress, manifesting as a unique trauma profile characterized by persistent hypervigilance, a profound erosion of interpersonal trust, and a distinct form of moral injury, all directly shaped by the invisible and continuous nature of the threat. This necessitates a comprehensive approach to victim support, encompassing both immediate crisis intervention and long-term psychological care. To comprehensively examine the utilization of surveillance technology and its impact on targeted individuals, this research will conduct an in-depth analysis of the psychological consequences of state-sponsored cyberattacks against dissidents. While the correlation

between cyberattacks and mental health has been explored in previous researches, existing studies primarily focus on the impact of cybercrime on broader populations, such as children and adolescents [2]. There is a notable lack of scholarly investigation specifically examining the psychological effects of state-sponsored cyberattacks on dissidents, particularly within the context of authoritarian regimes and the unique challenges faced by those who actively oppose or challenge governmental authority. This research aims to address this gap by providing a nuanced understanding of the psychological impact of such attacks on dissidents, contributing to a more comprehensive understanding of the human rights implications of surveillance technologies.

1.2 Research Questions

This research investigates the methods employed in state-sponsored cyberattacks targeting dissidents' iPhones, with a particular focus on the Pegasus spyware. The study aims to examine the psychological consequences of these attacks. To guide this investigation, the following research questions have been formulated:

- **Psychological Consequences**: What are the specific psychological consequences for dissidents in the GCC states targeted by state-sponsored cyberattacks, and how do these consequences manifest in their daily lives?
- **Mental Health and Well-being**: How do advanced surveillance and covert data extraction affect the mental health of targeted individuals, particularly concerning the development of anxiety, paranoia, and other forms of psychological distress?
- **Trust and Technology**: In what ways do these cyberattacks impact victims' trust in digital infrastructure and alter their relationship with technology, specifically in terms of online behaviour and self-censorship?
- **Technical Impact**: How do the specific technical mechanisms of the attacks, such as zero-click exploits and persistent surveillance, contribute to and amplify the psychological impact, including feelings of vulnerability and powerlessness?
- **Legal Framework and Recourse**: What is the legal landscape surrounding state-sponsored cyberattacks, what legal grounds, if any, exist for these actions, and how effective are current policies in enabling victims to pursue their rights?

By addressing these questions, this research seeks to contribute to a deeper understanding of the psychological impact of state-sponsored surveillance on dissidents. To achieve this, the study employs a mixed-methods approach, integrating in-depth qualitative interviews with targeted individuals and quantitative trauma assessment to provide a holistic analysis of the phenomenon.

1.3 Scope of Study

Cyberattacks targeting dissidents have become a global phenomenon[20], with the proliferation of sophisticated spyware products readily available to state actors. Pegasus, developed by the NSO Group, represents a particularly potent example due to its advanced capabilities, enabling complete control over a targeted device. This includes the ability to activate camera and microphone functions, exfiltrate data, and circumvent security measures through zero-click exploits—a method that enables the surreptitious installation of spyware without any user interaction 2. Given its prominence and demonstrated use against dissidents, journalists, and human rights defenders, Pegasus has been selected as the primary focus of this research, serving as a case study to analyse the technical mechanisms and psychological consequences of state-sponsored cyberattacks. .

While the risk of hacking extends across various platforms and devices, this research focuses specifically on iOS devices for two primary reasons. Firstly, the majority of confirmed cases that have undergone forensic examination by experts involve iOS devices. Secondly, iOS devices are among the most widely used in the GCC region [21]. This focus is not intended to diminish the risks associated with Android or other platforms but rather reflects the availability of robust technical evidence and documented cases related to iOS devices. It is important to acknowledge that the NSO Group, the developer of Pegasus spyware, claims the capability to infiltrate Android devices as well [22]. However, to date, no confirmed investigations by independent researchers have been published to corroborate this assertion. Therefore, this study concentrates on iOS as the primary platform for analysis, recognizing the need for further research to explore the vulnerabilities of other operating systems in the context of state-sponsored cyberattacks.

Though acknowledging the global prevalence of state-sponsored cyberattacks against dissidents, this study deliberately focuses on the Gulf Cooperation Council (GCC) region due to resource constraints and the region's unique sociopolitical context. The GCC has experienced a documented surge in cyberattacks targeting dissidents[9] and its conservative societal norms, which place a strong emphasis on privacy and personal reputation, amplify the potential psychological impact of such breaches. By examining the experiences of individuals within this specific context, the research aims to provide valuable insights into the nuanced psychological consequences of spyware attacks, contributing to a broader understanding of the human rights implications of these intrusive surveillance practices. This focused approach allows for a deeper exploration of the interplay between cultural factors, individual vulnerabilities, and the psychological impact of state-sponsored cyberattacks.

[2] More details about zero-click vulnerability will be discussed later.

2.0 Literature Review

2.1 Psychological Impact on Dissidents

Dissidents within the GCC region who challenge authoritarian practices, expose corruption, or advocate for human rights frequently face state-sanctioned harassment, arbitrary detention, and imprisonment under false charges. Annual reports by international non-governmental organizations consistently document these human rights violations, contributing to a climate of fear and self-censorship among citizens [23]. The mistreatment endured by dissidents often results in significant mental health challenges due to two primary factors. Firstly, the stark contrast between their pursuit of social justice and the unjust punishment they experience can engender profound cognitive dissonance, leading to internal conflict and disillusionment [24]. Secondly, the repressive tactics employed by authorities often deliberately target the individual's core values and sense of self. These tactics, which include torture, blackmail, economic sanctions, and disinformation campaigns, can inflict severe psychological trauma and contribute to the development of mental health disorders [23-25]. This underscores the urgent need for greater protection of dissidents and accountability for state actors who engage in such repressive practices. Furthermore, it is essential to consider the role of social and cultural factors in shaping the psychological experiences of dissidents. The stigma surrounding mental health issues in some societies may prevent individuals from seeking help or disclosing their struggles, further exacerbating their distress or even the lack of knowledge about mental health issues. Future research should investigate how cultural norms and social support systems influence the coping mechanisms and resilience of dissidents facing state-sponsored persecution.

Conversely, the internet has become an indispensable tool for dissidents to communicate, disseminate information, mobilize support, and expose human rights violations [26]. However, this reliance on digital technologies exposes them to the risk of state-sponsored hacking and data breaches, which can have profound psychological consequences, including trauma, anxiety, and depression [27]. While the perpetrators of cybercrime are often difficult to identify and prosecute [28], the fear of being targeted by state actors with sophisticated surveillance tools represents a far greater concern for dissidents than the risks posed by ordinary hackers. This highlights the inherent tension between the internet's empowering potential for dissidents and the heightened vulnerability it creates in the face of state surveillance and repression. This duality necessitates a critical evaluation of digital security practices and the development of strategies to mitigate the risks associated with online activism. Furthermore, it raises important questions about the role of technology companies and international organizations in protecting the digital rights and security of dissidents. Should tech

companies be held accountable for facilitating state surveillance? How can international legal frameworks be strengthened to address the transnational nature of cyberattacks against dissidents?
Recent years have witnessed a surge in documented cases of human rights defenders, journalists, legal professionals, and politicians being targeted by state-sponsored spyware, resulting in the exposure of their networks, confidential communications, and private lives [29]. The consequences of such attacks extend beyond immediate privacy violations, generating both emotional and psychological repercussions for victims. While emotional impacts, such as distress and anxiety, are often immediate and readily observable, psychological impacts are typically more profound, enduring, and can manifest as serious mental health disorders[30]. These psychological consequences can include, but are not limited to, post-traumatic stress disorder, depression, anxiety disorders, and complex trauma, potentially leading to long-term impairments in social, occupational, and personal functioning. This highlights the need for a comprehensive approach to victim support that addresses both the immediate emotional distress and the potential for long-term psychological harm.

2.2 Emotional Impact

Dissidents targeted by state-sponsored cyberattacks often endure significant emotional distress and psychological trauma, with potentially enduring consequences for their mental health and well-being. The emotional impact can manifest in a range of intense and debilitating experiences, including anger, frustration, vulnerability, fear, anxiety, erosion of trust, feelings of betrayal and social isolation, shame, self-blame, and even depression [31-35]. These emotional responses, often overlooked or underestimated, can have profound and long-lasting effects on individuals' psychological well-being. The psychological impact is amplified by the unique characteristics of the threat itself. Unlike a discrete traumatic event, the continuous and invisible nature of digital surveillance creates a state of chronic, unresolved stress, which academic literature suggests is more akin to the trauma experienced by victims of persistent stalking [36]. than to that of a single cybercrime incident. If left unaddressed, such emotional distress can contribute to the development or exacerbation of mental health conditions, including anxiety disorders, depression, and complex trauma, potentially leading to significant impairments in social, occupational, and personal functioning. This underscores the critical need for timely and comprehensive psychological support for victims of state-sponsored cyberattacks, recognizing the profound and enduring impact of these intrusive violations on their emotional and psychological well-being. It is crucial to recognize that diverse societies and cultures can elicit varying emotional responses. Some individuals may be open about their emotions, while others may be sensitive or reluctant to acknowledge the impact, particularly among those who perceive themselves as courageous in challenging authority [37, 38].

2.3 Psychological Impact

Dissidents targeted by state-sponsored cyberattacks often experience a range of psychological consequences that extend beyond immediate emotional distress. Victims may exhibit symptoms indicative of various mental health disorders, including Post-Traumatic Stress Disorder (PTSD), anxiety disorders, sleep disturbances, difficulty concentrating, and social withdrawal [39-42]. While these symptoms have been extensively studied in the context of cyberbullying and general cybercrime, it is crucial to recognize that dissidents facing state-sponsored attacks are equally susceptible, if not more so, due to the politically motivated nature of these attacks and the potential for severe repercussions. The unwavering commitment of dissidents to their cause, often characterized by a willingness to endure hardships and confront powerful adversaries, can paradoxically increase their vulnerability to the psychological effects of cyberattacks. These attacks can undermine their sense of agency, instil fear of future reprisals, and disrupt their ability to continue their activism. The pervasive threat of surveillance and the potential exposure of sensitive information can lead to self-censorship, withdrawal from online spaces, and a chilling effect on freedom of expression, ultimately hindering their efforts to challenge authoritarianism and advocate for human rights. While victims of cyberattacks may experience a range of psychological effects, including anxiety, depression, and PTSD, which share common symptoms such as sleep disturbances, emotional dysregulation, loss of interest, difficulty concentrating, and fatigue [43]. each disorder also presents unique clinical manifestations. PTSD is characterized by intrusive flashbacks, nightmares, hypervigilance, and avoidance of trauma-related stimuli; anxiety manifests as excessive worry, restlessness, muscle tension, and panic attacks; while depression is characterized by persistent sadness, feelings of worthlessness or guilt, and changes in appetite or sleep patterns[44].

Within the PTSD framework, research on victims of persistent threats suggests that the hyperarousal symptom cluster—including hypervigilance, an exaggerated startle response, and chronic anxiety—is often the most dominant and debilitating dimension of distress. This is a logical response to a threat that is perceived as ongoing and inescapable, a key feature of state-sponsored surveillance [45, 46].

Recognizing the potential for severe and long-lasting psychological harm, this research will focus specifically on the symptoms of PTSD among victims of state-sponsored cyberattacks, while acknowledging that other mental health disorders may also arise. This focus is further justified by research suggesting that the psychological harm caused by cyberattacks, particularly those perpetrated by state actors, can be comparable in severity to that inflicted by political violence. By examining the prevalence and severity of PTSD symptoms among dissidents targeted by cyberattacks, this study aims to contribute to a deeper understanding of the psychological consequences of these

intrusive practices and inform the development of effective interventions to support victims and mitigate the long-term impact on their mental health and well-being [47].

Furthermore, the psychological impact may transcend the fear-based framework of PTSD to include what the literature defines as moral injury. This refers to the profound distress that results from events that transgress deeply held moral beliefs, such as failing to prevent harm to others. For journalists and activists, whose work is often guided by an ethical duty to protect sources and networks, the compromise of their devices can be experienced as a deep personal and professional failing, leading to intense feelings of guilt, shame, and betrayal, even when they were technologically powerless to stop the attack [48-51].

Finally, the psychological toll of these attacks can also lead to counterintuitive behavioural outcomes. The literature on **security fatigue** describes a state of mental and emotional exhaustion from constant security demands, which can lead to risk-minimization and decision avoidance. This is often compounded by [52, 53] **learned helplessness**, a psychological state where individuals, feeling powerless against an overwhelming and unstoppable adversary, cease protective efforts altogether, believing them to be futile [54].

Although the focus here is on individual victims, the psychological harm inflicted on dissidents through cyberattacks can have ripple effects throughout society. When vocal critics are silenced or driven to self-censorship due to fear and trauma, it undermines the open exchange of ideas and weakens democratic discourse. However, the psychological distress experienced by victims is often exacerbated by the lack of accountability for perpetrators of state-sponsored cyberattacks. When governments operate with impunity, it creates a sense of powerlessness and injustice that can hinder healing and recovery. Addressing this requires strengthening international legal frameworks and mechanisms for holding states accountable for human rights violations committed through digital means.

2.4 Geopolitical context on the region

The Gulf Cooperation Council (GCC) is a political and economic alliance comprising six Arab states situated in the Persian Gulf region: Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates. These nations share a common history, geographic proximity, and religious affiliation [55], as well as linguistic [56], cultural [57, 58] and heritage-based commonalities [59].

Beyond these sociocultural affinities, GCC countries exhibit similar political structures, predominantly characterized by monarchical rule, where power is concentrated within ruling families [60] Kuwait presents a partial exception, with a political system that incorporates limited power-sharing between the monarchy and elected representatives. Furthermore, GCC members typically align their foreign policies on regional and international issues, particularly in matters of security and defence[61]. The GCC is characterized by extensive cooperation on security matters, with member states routinely

exchanging intelligence information pertaining to citizens, security threats, and cybercrimes [62]. Cybersecurity represents a key area of collaboration, with member states actively sharing knowledge and expertise to enhance their collective defence against digital threats[63].

This regional context of shared values, political structures, and security cooperation is crucial for understanding the implications of state-sponsored cyberattacks against dissidents within the GCC. The close collaboration between member states on security matters raises concerns about the potential for transnational surveillance and the sharing of information that could be used to target and suppress dissent across borders. Furthermore, the sociocultural emphasis on privacy and reputation within the GCC amplifies the potential psychological impact of cyberattacks, which can expose dissidents to social ostracization, reputational damage, and further persecution.

Given the prevalence of absolute monarchies in the GCC, instances of social unrest often arise in response to political restrictions and socioeconomic inequalities, manifesting in demonstrations and protests [64]. Bahrain, for example, has experienced numerous uprisings over the past century, with the most recent occurring during the 2011 Arab Spring This situation prompted other GCC countries to deploy their military forces in support of the local government, aiming to quell the unrest [65, 66]. Oman faced a protracted civil war in the 1970s [67]. while Kuwait, despite its relatively more reformed political system, has witnessed the dissolution of its parliament multiple times in the past four decades [3] [68]. These instances of social unrest underscore the underlying tensions between the desire for greater political participation and socioeconomic justice and the constraints imposed by the existing political structures within the GCC. The use of state-sponsored cyberattacks to monitor and suppress dissent adds another layer of complexity to this dynamic, raising concerns about the erosion of fundamental freedoms and the potential for increased social instability.

While monarchies maintain a firm grip on power, successive generations continue to challenge the status quo, demanding a more equitable distribution of wealth and resources [66], This underlying tension is further fuelled by limited political participation and restrictions on freedom of expression, leaving many citizens feeling marginalized and unrepresented within the political system. This, in turn, can lead to discrimination against those perceived as disloyal to the ruling authorities [58]. To maintain their grip on power and prevent any challenges to their authority, ruling elites within the GCC often resort to repressive tactics to quell dissent and discourage social unrest [58]. These tactics can include arbitrary arrests, detention without trial, torture, restrictions on freedom of expression and assembly, and the deployment of surveillance technologies to monitor and intimidate perceived opponents. By employing such measures, authorities aim to instil fear within the population, creating a chilling effect that discourages public displays of dissent and reinforces the existing power structure.

[3] In May 2024 while working on this study, the Emir dissolved the parliament for two years and freeze some articles from the constitution .

Geopolitical tensions between the western and eastern shores of the Persian Gulf, particularly following the Iranian Revolution of 1979, have significantly impacted the sociopolitical landscape of the GCC. The establishment of an Islamic republic in Iran was perceived as a threat by the GCC monarchies, particularly given the presence of Shia minorities within their own populations, who have historically experienced marginalization and discrimination[66]. This has fuelled a narrative within the GCC that portrays Iran as a destabilizing force seeking to exploit sectarian divisions and foment unrest within their borders.

This climate of suspicion and hostility towards Iran has contributed to restrictions on freedom of expression and increased surveillance of individuals and groups perceived as sympathetic to the Iranian regime or critical of the GCC governments. Reporters Without Borders has consistently ranked GCC countries as challenging or dangerous for journalists, with Qatar, Kuwait, and Oman categorized as "challenging" and Saudi Arabia, Bahrain, and the UAE labelled as "dangerous" [69]. Similarly, Freedom House, in its annual Freedom in the World report, categorizes Saudi Arabia, Bahrain, and the UAE as "not free" [25][4]. , although it should be noted that Kuwait, Qatar, and Oman were not included in that particular report.

More than that, GCC countries signed different memorandum and agreement aim to counter cybersecurity which include data sharing and experience exchange [70, 71].

These assessments highlight the restrictive media environment and limited civic freedoms within the GCC, which are further exacerbated by the use of sophisticated surveillance technologies to monitor and suppress dissent. The perceived threat from Iran has been used to justify these repressive measures, creating a chilling effect on freedom of expression and contributing to a climate of fear and self-censorship. However, it is crucial to critically examine the extent to which this narrative of external threat is used to deflect attention from internal challenges and justify the suppression of legitimate dissent and calls for political reform.

3.0 Methodology

This thesis employs a mixed-methods approach to conduct a comprehensive and nuanced investigation into the psychological impact of state-sponsored cyberattacks on dissidents. This design is uniquely suited to exploring the intricate nature of digital repression and its human consequences, as it allows for the synergistic integration of both quantitative and qualitative data. The quantitative data will provide insights into the prevalence and severity of psychological distress, while the qualitative data will illuminate the lived experiences, coping mechanisms, and individual narratives of those affected. This integrated approach will generate a more holistic and multifaceted understanding

[4] Kuwait, Qatar and Oman wasn’t cover in that report

of the psychological consequences of these attacks, ultimately informing the development of effective support mechanisms and interventions for this vulnerable population.

Specifically, the culturally sensitive Harvard Trauma Questionnaire (HTQ) will be employed to quantify psychological distress, while qualitative narratives will offer essential human context, illuminating lived experiences and coping strategies. Access to dissidents, a hard-to-reach group, will be facilitated by established researcher rapport within their communities. To uphold rigor and ethical soundness, the methodology will explicitly detail strategies for mixed-methods integration, trauma-informed interview question refinement, nuanced interpretation of HTQ results, transparent acknowledgment of sampling limitations, detailed technical analysis specifications, and robust data security protocols to ensure anonymity and confidentiality. This integrated methodology aims to generate profound knowledge to significantly support individuals affected by state-sponsored cyberattacks.

3.1 Qualitative Research Design and Implementation

he qualitative component of this study was systematically designed to explore the central research questions through in-depth participant narratives. To ensure a clear and logical connection between the study's overarching objectives, the data collection instruments, and the analytical outcomes, a thematic map was developed. This map, presented in Table 1, illustrates the alignment between each research question, the corresponding interview questions and emergent themes, and the key qualitative codes that were generated through NVivo analysis.

Table 1：Research Question and Thematic Alignment Matrix

Research Question	Relevant Interview Question(s)	Associated Thematic Codes
1. What are the specific psychological consequences and how do they manifest in daily life?	Q2, Q5, Q6, Q7, Q8, Q9, Q11	Emotional: (Vulnerability, Shock, Paranoia, Guilt, Fear, Anger)Intrusive: (Unwanted Thoughts, Triggers, Flashbacks)
2. How do these attacks affect mental health, well-being, and contribute to anxiety or paranoia?	Q5, Q6, Q9	Emotional: (Paranoia, Fear)Intrusive: (Unwanted Thoughts)
3. How do these attacks affect victims' trust in technology and alter their online behaviour?	Q10, Q12, Q13, Q19	Perception of Technology and Ongoing Surveillance Behavioural & Professional Impact: (Work Modification, Social Withdrawal)
4. How do the technical mechanisms (e.g., zero-click) contribute to the psychological impact?	Q1, Q2, Q16	Attribution of Causality/Responsibility: (No Self-Blame)Emotional: (Vulnerability)
5. What is the legal landscape and what are the avenues for victims to pursue their rights?	Q16, Q17, Q18	Attribution of Causality/Responsibility(Seeking Support - a potential emergent theme from Q17)

3.1.1 Participant Recruitment and Sampling Strategies

Accessing participants for this highly sensitive study was primarily achieved through the researcher's established network and reputation within dissident communities and non-governmental organisations (NGOs), fostering essential trust. This foundation was critical for conducting research with a hard-to-reach population facing significant risks. The study employed non-probability sampling techniques, specifically a combination of purposive sampling and snowball sampling. Purposive sampling involved intentionally selecting participants who possessed direct experience with state-sponsored cyberattacks, ensuring the collection of information-rich cases crucial for an in-depth understanding. Snowball sampling complemented this by leveraging initial participants to identify and refer other eligible individuals within their trusted networks, proving invaluable for reaching a population where no comprehensive sampling frame exists [72, 73].

3.1.2 Recruitment Procedures:

Recruitment was systematically conducted through two primary approaches, prioritizing participant safety, informed consent, and security at every stage.

The first approach, accounting for the majority of participants, leveraged the researcher's established professional network from previous documented and published work in state-actor spyware detection. Instead of direct communication with potential participants, an initial approach was made through trusted third parties, such as family members or close friends. These intermediaries were provided with clear information regarding the study's objectives, assurances of participant safety and security, and official university documentation and contact details for verification. If a potential participant expressed willingness to consider participation, secure communication was initiated via an encrypted platform (primarily Signal messaging application). This initial direct contact focused explicitly on participant safety, a detailed explanation of their rights to participate and withdraw at any stage, and ensuring their comfort and full understanding before proceeding. Interviews were only scheduled once participants were fully confident in their safety and rights.

The second approach utilized the researcher's professional connections within research institutes and NGOs working closely on related issues. These institutes, recognizing the researcher's established work in the field, facilitated initial contact with potential participants. The institutes managed the first phase of communication, providing potential participants with comprehensive information about the study, researcher credentials, university affiliation, and crucial safety and assurance details. Once individuals indicated satisfaction with this preliminary information, the institutes assisted in establishing secure communication channels with the researcher on an agreed encrypted platform. This direct communication mirrored the first approach, focusing on participant safety, rights, and ensuring full comfort prior to any interview scheduling.

In one specific instance, where a participant's name had been publicly disclosed in the media, the same third-party contact procedure via a family member was meticulously followed to ensure their safety and informed decision-making. It is noteworthy that no individuals approached for participation declined the invitation to join the study.

While the researcher's established network provided a pragmatic and effective means of accessing this highly sensitive and hard-to-reach population, ensuring methodological transparency necessitates explicitly acknowledging and justifying this non-probability sampling strategy. It is imperative to acknowledge that, by design, non-probability methods inherently influence the generalizability of findings, particularly concerning quantitative data such as Harvard Trauma Questionnaire (HTQ) scores. As the selection process is not random, the statistical representativeness of the sample to the broader dissident population cannot be definitively determined. Consequently, the study's strength

lies not in statistical generalizability, but in the rich, contextual, and in-depth understanding derived from this specialized sample, focusing on the transferability of qualitative insights [74, 75].

Sixteen participants provided informed consent and completed the HTQ. For the qualitative component, this sample size of 16 participants is considered appropriate for achieving data saturation [76]. In qualitative research, the primary objective is to uncover recurring themes and patterns rather than statistical significance. Data saturation is anticipated when new information ceases to emerge from additional interviews, typically occurring within a range often cited as 10-20 participants, indicating sufficient thematic depth has been explored. Further comprehensive details regarding the recruitment process, comprehensive ethical practices, and specific measures taken to safeguard the well-being of these vulnerable participants are elaborated in the dedicated Ethical Considerations chapter, which follows this methodology chapter.

3.1.3 Semi-Structured Interview Protocol

The interview questions for this study were developed through a rigorous process that involved:

- **Comprehensive Literature Review**: An in-depth examination of scholarly literature on mental health disorder symptoms, diagnostic criteria, and existing research on the psychological impact of cyberattacks and cyberbullying.
- **Consultation with Experts**: Collaboration with the research supervisor and other relevant experts to ensure the questions' alignment with the study's objectives, ethical considerations, and methodological rigor.

This meticulous approach to question development aimed to ensure the validity and reliability of the qualitative data collected, enabling a nuanced and comprehensive understanding of the psychological impact of state-sponsored cyberattacks on dissidents.

Following this development, the qualitative data collection will utilize the resultant semi-structured interview protocol. This protocol is systematically structured around three core thematic areas: "The Incident," "Psychological Impact," and "Aftermath of the Incident," providing a coherent yet flexible framework for eliciting narratives from participants.

The interview protocol was structured to gather comprehensive data on the participants' experiences and psychological responses to state-sponsored cyberattacks. Demographic information was collected separately to maintain anonymity and confidentiality. The interview questions were organized into three core areas:

- **The Incident**: This section focused on the specifics of the cyberattack, including its nature, the perceived perpetrator, confirmation of the attack, and any technical details the participant could recall (Questions 1, 2, 3, 4, 5, and 12).

- **Psychological Impact**: This section explored the psychological and emotional consequences experienced by the participants following the cyberattack. Questions 6, 7, 9, 10, 15, 16, and 18 focused on any mental health issues, emotional distress, or changes in psychological well-being that the participants perceived as being linked to the attack.
- **Aftermath of the Incident**: This section investigated the long-term impact of the cyberattack and the participants' coping mechanisms. Questions 8, 11, 13, 14, 17, 19, and 20 examined how the participants coped with the incident, any significant life changes that occurred as a result, and any new behaviours or strategies they adopted to protect themselves.

This structured approach to the interview process ensured a systematic exploration of the participants' experiences, enabling a comprehensive analysis of the psychological impact of state-sponsored cyberattacks on dissidents.

3.2 Trauma-Informed Interviewing and Rapport Building

Given the sensitive nature of researching the psychological impact of state-sponsored cyberattacks on dissidents, trauma-informed interviewing and rapport building are paramount. While the researcher's established network and reputation facilitate initial trust and comfort, general rapport-building must be augmented with specific, systematic trauma-informed communication techniques throughout the interview process. This deliberate application of principles is essential for individuals who have experienced trauma, moving beyond a mere commitment to comfort.

To facilitate the capture of rich, detailed narratives and encourage a dynamic exchange during interviews, the protocol explicitly details strategies for flexible probing and follow-up questions. While a core set of questions provides a robust starting point, the semi-structured format will be fully leveraged to explore emergent themes and unanticipated insights. Interviewers will be trained to use non-directive prompts to encourage participants to elaborate, ensuring the collection of comprehensive, in-depth information beyond the pre-defined inquiries and thus enabling a more profound understanding of their experiences.

Specific strategies explicitly integrated into the interview protocol to minimize the risk of re-traumatization and ensure participant well-being include:

- **Acknowledging the Nature of Questioning**: Participants will be informed that some questions, while potentially unusual, are designed to help the interviewer fully understand their experiences.
- **Empowering Participants**: Participants will be actively encouraged to ask questions at any point for clarification or if they feel uncomfortable.

- **Offering Control over the Narrative**: Interviews will commence with open-ended invitations (e.g., "Where would you like to start?" or "Would you tell me what you are able to about your experience?"). This reduces pressure, allowing participants to share at their own pace.
- **Acknowledging Memory Impacts of Trauma**: The interview process will accommodate for the potential effects of trauma on memory retrieval, avoiding demands for strict chronological accounts.
- **Minimizing Re-traumatization**: Proactive strategies will be employed to mitigate re-traumatization, such as scheduling shorter conversations over several days rather than extensive single interviews. A routine for recurring conversations will be established to enhance safety, and potential triggers will be identified by inviting participants to share what makes them feel safe or unsafe. Consent will be continuously prioritized, with explicit reminders that participants are not obligated to answer uncomfortable questions. Interviewers will maintain an open mind, create space for relaxation (e.g., suggesting breathing exercises if appropriate), and ensure mental health resources are readily available.

These measures collectively demonstrate a proactive and robust ethical framework, vital for sensitive research and ensuring that the interview process itself does not inflict further harm, thereby upholding participant well-being and data integrity.

3.3 Qualitative Data Analysis:

All interviews will be video-recorded and transcribed verbatim. The transcribed data will then be systematically analysed using NVivo 14 (QSR International, Version 14), a leading Computer-Assisted Qualitative Data Analysis Software (CAQDAS) package. NVivo was selected for its robust capabilities in managing large volumes of textual data, facilitating transparent and systematic coding, and supporting the rigorous development of themes and patterns [77]. Its features enable efficient data organization, coding, query execution, and the visualization of relationships between themes, thereby enhancing the auditability and credibility of the analysis process [78].

To ensure both methodological transparency and rigor, this study will employ Braun and Clarke's (2006, 2012) thematic analysis as its primary qualitative analysis framework. This particular approach is highly flexible and well-suited for identifying, analysing, and interpreting patterns of meaning ("themes") across rich textual data. It is considered particularly advantageous for this study's aims due to several key characteristics:

- **Theoretical Flexibility**: Unlike some other qualitative methodologies (e.g., Grounded Theory or IPA), Braun and Clarke's thematic analysis is not tied to a specific theoretical or epistemological position. This flexibility allows for an approach that can be inductive (themes emerging directly from the data) and/or deductive (themes guided by existing theory or the

research questions), which is crucial for exploring a complex, under-researched phenomenon like the psychological impact of cyberattacks on dissidents [79].

- **Accessibility and Transparency**: The six-phase guide proposed by Braun and Clarke provides a clear, systematic, and accessible roadmap for conducting the analysis, making the process transparent and enhancing the study's replicability and trustworthiness. This structured yet iterative approach is valuable for demonstrating thoroughness, especially in sensitive research [79, 80].
- **Focus on Meaning and Experience**: Thematic analysis is adept at capturing rich, nuanced detail regarding participants' experiences, meanings, and realities. This directly aligns with the study's objective to gain a deeper understanding of the psychological and emotional consequences, coping mechanisms, and individual narratives related to state-sponsored cyberattacks [79].
- **Suitability for Complex Data**: The method's ability to handle diverse and complex datasets allows for a thorough exploration of the multifaceted psychological impacts, which might involve various emotional responses, cognitive appraisals, and behavioural changes following digital repression.

The analysis process will involve several iterative phases, adhering to Braun and Clarke's (2006) guidelines:

1. **Familiarization with the data**: Repeated reading of transcripts to achieve immersion [81].
2. **Generating initial codes**: Systematically coding interesting features of the data relevant to the research question.
3. **Searching for themes**: Grouping codes into potential themes.
4. **Reviewing themes**: Refining and clarifying themes, ensuring they are distinct and coherent.
5. **Defining and naming themes**: Developing clear definitions and names for each theme.
6. **Producing the report**: Selecting compelling extracts to illustrate themes and linking them back to the research question.

This analytical process resulted in the development of a structured codebook, which organizes the findings into several key thematic areas. The final themes and codes that guide the analysis, along with their definitions, are presented in Table 2 below. This codebook serves as a reference for the thematic discussion in the Results chapter.

Table 2 : Theme and Code Definition Table

Theme	Code	Short Description
Emotional	Vulnerability	Feelings of being exposed, unprotected, or susceptible to future harm.
	Shock	Sudden and intense feelings of disbelief, surprise, or distress upon discovering the attack.
	Paranoia	Irrational or heightened suspicion and distrust, often related to surveillance or monitoring.
	Guilt	Feelings of self-blame or regret concerning the attack.
	Fear	Apprehension or dread related to personal safety, privacy, or future attacks.
	Anger	Feelings of strong displeasure or hostility directed at perpetrators, systems, or circumstances.
	Anticipation/Expectation	A sense of expecting or anticipating future attacks or surveillance.
Avoidance	Social Withdrawal	Reduced engagement in social interactions or activities.
	Procrastination	Delaying or postponing tasks, possibly due to emotional distress or disengagement.
	Denial	Refusal to acknowledge or accept the reality or impact of the attack.
Intrusive	Unwanted Thoughts	Repetitive, distressing mental content concerning the incident.
	Triggers	Specific cues or situations that evoke memories or strong reactions associated with the attack.
	Flashbacks	Vivid, re-experiencing of parts of the traumatic event as if it were happening in the present.
Perceived Attack Drivers	Professional/Activist Motivation	Belief that the attack was due to their work as human rights defenders, journalists, or activists.
	Network/Affiliation-Based Motivation	Belief that the attack was aimed at their associates, colleagues, or groups they are part of.
	Personal Motivation	Belief that the attack stemmed from personal reasons or characteristics not directly related to public activities.
Behavioural & Professional Impact	Impact Present	Acknowledgment or evidence of changes in behaviour or professional activities.
	No Impact	Acknowledgment or evidence of no significant changes in behaviour or professional activities.
	Work Continuity	Continuation of professional activities despite the attack.
	Work Discontinuation	Cessation of professional activities after the attack.
	Workload Adjustment	Changes in the volume or intensity of professional tasks.
	No Workload Adjustment	Absence of changes in the volume or intensity of professional tasks.
	Work Modification	Changes in the methods or approach to carrying out professional duties.
	No Work Modification	Absence of changes in the methods or approach to carrying out professional duties.
Attribution of Causality/Responsibility	No Self-Blame	Participants explicitly stating they do not hold themselves responsible.
	Self-Blame	Participants expressing personal responsibility or regret for the attack's success.
	External Factors	Attributing the attack to external circumstances beyond personal control.

To operationalize these phases, a comprehensive coding frame was developed to ensure a systematic and transparent analytical process. This frame linked specific words and phrases from the participant interviews to initial codes and broader, interpretive themes, documenting the rationale for each analytical step. For instance, participant statements such as 'felt exposed' and 'not secured any more' were systematically grouped under the theme of 'Vulnerability,' which itself falls under the parent

code 'Emotional.' This structured approach ensured consistency and rigor throughout the analysis. The complete thematic analysis coding frame is provided in Appendix 14 for Full Methodological Transparency.

This detailed and systematic approach moves beyond a general statement of "in-depth analysis," demonstrating a rigorous qualitative methodology that upholds the scientific integrity of this complex and sensitive study.

3.4 Rationale and Application of the Harvard Trauma Questionnaire (HTQ)

While semi-structured interviews serve as the primary instrument for in-depth exploration of participants' experiences, the Harvard Trauma Questionnaire (HTQ) was selected as a complementary instrument for quantitative data collection. The HTQ's inclusion provides valuable additional context into self-reported distress symptoms, thereby enriching the comprehensive qualitative narratives, a common practice in mixed-methods designs where different data types offer unique insights [74].

To assess the psychological impact of state-sponsored cyberattacks on dissidents with greater precision, this study utilized a standardized self-assessment tool developed by researchers at Harvard University for measuring symptoms of Post-Traumatic Stress Disorder (PTSD). While various self-assessment tools exist for measuring different mental health disorders—such as the Positive Mental Health Questionnaire (PMHQ) [82, 83] for positive mental health, and the Mental Health Self-Management Questionnaire (MHSQ) [84, 85] for self-management strategies—the HTQ was deemed most appropriate. This decision was based on its specific focus on trauma-related symptoms and its user-friendly format [86].

The PMHQ and MHSQ, while valuable in their respective domains, primarily focus on depression and anxiety and may present greater complexity for participants to complete.

The HTQ was chosen due to several key advantages that make it particularly suitable for its complementary role within this mixed-methods design:

- **Targeted Focus**: The HTQ is specifically designed to assess trauma exposure and PTSD symptoms in survivors of torture, refugees, and individuals who have experienced violence [87]. This makes it profoundly relevant for assessing specific symptom patterns pertinent to the experiences of dissidents targeted by state-sponsored cyberattacks.
- **Cultural Sensitivity**: The HTQ has been translated and adapted for use in various cultural contexts, with multiple versions available for populations that have undergone diverse types of trauma and violence [87]. This sensitivity to cultural nuances ensures the instrument's validity and appropriateness for diverse populations, including those from the Middle East region.

- **Established Validity and Reliability**: The HTQ is a well-established and psychometrically sound instrument with demonstrated reliability and validity across multiple studies [87, 88]. Its structure is based on the Diagnostic and Statistical Manual of Mental Disorders (DSM) criteria for PTSD [87], providing a robust foundation for consistent symptom assessment even when serving a complementary function.

Among the various versions of the Harvard Trauma Questionnaire, this study specifically utilized the version published by Post-Traumatic Integration, an online institute co-funded by the Erasmus+ Programme of the European Union [89]. This specific version, known as Trauma Symptoms IV, comprises 40 items assessing potential PTSD symptoms. Each item is rated on a 4-point Likert scale, ranging from "not at all" (score of 1) to "extremely" (score of 4). Following the completion of the questionnaire, the sum of the scores is divided by the number of items answered. A resulting score of 2.5 or higher suggests the likely presence of PTSD symptoms, while a score below 2.5 indicates a lower likelihood of experiencing such symptoms. This adaptation of the HTQ was selected for its alignment with the study's objectives and participant population, as Post-Traumatic Integration's focus on providing accessible and culturally sensitive resources for trauma survivors aligns with the research's aim to understand the psychological impact of cyberattacks on dissidents within a specific socio-cultural context. Furthermore, the Trauma Symptoms IV subscale offers a concise and focused assessment of PTSD symptoms, making it suitable for the study's methodological framework [89].

Ultimately, the inclusion of the HTQ as a complementary quantitative tool is anticipated to provide an additional layer of evidence and verification, strengthening the overall findings and contributing to a more robust understanding of the psychological impact experienced by this vulnerable population.

3.5 Mixed-Methods Integration and Analysis Strategies

To analyse the findings from the interviews and the HTQ, we will employ a convergent parallel mixed-methods design. This approach is selected to achieve a comprehensive and synergistic understanding of the research phenomenon that transcends what each dataset could offer in isolation. The design involves the simultaneous collection and independent analysis of both quantitative and qualitative data. Specific[90]ally, quantitative data are derived from scores on the Harvard Trauma Questionnaire (HTQ), while qualitative data are generated from in-depth interview narratives[90, 91]. The core objective of this comprehensive strategy is to move beyond mere comparison of findings, generating novel understandings and a holistic perspective that is richer than what either quantitative or qualitative data could provide alone [92-94]. This active integration is considered the "centrepiece" of mixed methods, enabling researchers to draw out new understanding and provide depth and context

for explaining the "why" and "how" of findings [74, 75]. For instance, if quantitative data from the HTQ indicates a high prevalence of certain PTSD symptoms, the qualitative interview data will be used to explain why and how those symptoms manifest in the lived experiences of dissidents, adding crucial depth and context to the numerical findings. This exemplifies the "Complementarity" (elaboration) and "Expansion" functions of mixed methods [93, 94].

3.6 Joint Displays: Operationalizing Integration：

To achieve this robust integration and synthesis, the implementation of Joint Displays is central to this study's analytical strategy. Joint displays are powerful visual tools that systematically bring quantitative and qualitative data together, facilitating the discovery of unforeseen linkages and providing crucial context for explaining the "why" and "how" of findings[90, 92, 95]. They move beyond simple side-by-side presentation to active synthesis, allowing for the systematic merging, connecting, or building together of quantitative and qualitative results, thereby generating "**meta-inferences**" – interpretations derived from the integrated mixed data that transcend individual findings [90, 92, 96].

The development of joint displays is an iterative process, ensuring a thoughtful and systematic approach to data integration [90]. This process involves:

- **Identifying Data Sources and Variables**: Clearly delineating each distinct data source (e.g., HTQ, interviews) and the specific quantitative and qualitative variables within them.
- Aligning by Constructs: Organizing variables from both sources under relevant theoretical constructs or research questions.
- **Iterative Refinement and Integration**: Systematically merging, connecting, or building relationships between the quantitative and qualitative variables within each construct, compelling consideration of how data interact, complement, explain, or contradict each other.
- **Explanatory Questions and Integrated Understandings**: Applying example questions within each construct row to articulate the organizational rationale and the specific types of integrated understandings expected [90].

A joint Displays will primarily employ a "**Merging Integration**" strategy, characteristic of convergent parallel designs, utilizing "Side-by-Side Display" and "Statistics-by-Themes Display" formats. The analytical process will involve three key steps: (1) conducting thorough, independent analyses of both quantitative and qualitative data [92, 97], (2) systematically linking findings within the joint display framework [90, 92], and (3) interpreting the integrated data to develop meta-inferences, discussing convergence, divergence, and expansion [90-93]. The table presented in the original report serves as a methodological blueprint, illustrating these specific integration points.

3.7 Expected Contributions of Integrated Analysis:

This robust mixed-methods integration, systematically facilitated by Joint Displays, is expected to yield a more nuanced, comprehensive, and theoretically rich understanding of the psychological impact of cyberattacks on dissidents. By systematically integrating quantitative prevalence and severity data from the HTQ with rich qualitative narratives from interviews, the study will not only identify the extent and frequency of psychological distress but also illuminate the nature, context, and lived experience of this distress [95]. The integrated approach will enable the identification of patterns, relationships, and explanations that might not be evident in either dataset alone, moving beyond descriptive accounts to explanatory understandings [93, 95].

4 Technical analyses

State-sponsored cyberattacks, a pervasive form of digital transnational repression, increasingly target human rights defenders, journalists, and lawyers globally, leveraging sophisticated tools like Pegasus spyware[98]. These attacks, often employing zero-click methods, aim to silence dissent and control information, making digital technologies, once seen as empowering, a source of insecurity and fear [99]. Responding effectively requires a dual approach: robust technical analysis to uncover these covert operations and a deep understanding of the severe psychological and social harm inflicted upon victims. This report argues that technical evidence is crucial not only for unmasking attacks but also for validating victim experiences and personal reflection to the incident which is vital for advocacy and accountability.

Mobile forensic analysis is indispensable for investigating these compromises, particularly on iPhones. This specialized field involves extracting data in a forensically sound manner through file system analysis [98]. The global Pegasus spyware scandal exemplifies this, where forensic analysis by organizations like Citizen Lab and Amnesty International revealed widespread government use of the sophisticated spyware . Notably, iPhones, despite being frequent targets, retain "significantly more forensic traces" than Android devices, making them highly valuable for detecting and proving such infections [99]. This inherent logging capability paradoxically aids investigators in unmasking attacks like Pegasus, which Google's Project Zero considers "one of the most technically sophisticated exploits" [99].

Beyond technical compromise, these attacks inflict profound psychological and social harm. Cyber harm extends far beyond financial loss, encompassing severe emotional and psychological distress[98]. Victims consistently report intense fear, chronic anxiety, pervasive insecurity, paranoia, and a profound loss of trust . Hacking is experienced as a deep intrusion into a victim's "digital space," resembling a personal violation, leading to feelings of betrayal and vulnerability . The mere perception of surveillance, even without explicit technical confirmation, can induce significant self-censorship,

aligning with Bentham's panopticon theory, and fundamentally alter behaviour [99, 100]. This leads to behavioural consequences such as limiting online posts, meticulously controlling social media, and withdrawing from advocacy or social communities, directly achieving the state's goal of silencing dissent [101]. In severe cases, victims may exhibit symptoms similar to Post-Traumatic Stress Disorder (PTSD), including hyperactivity, hypervigilance, nightmares, and sleep deprivation, alongside depression symptoms and changes in habits .

The nexus between technical evidence and victim validation is critical. Digital evidence corroborates or refutes witness accounts, filling memory gaps and providing objective chronological order, which is especially significant for human rights defenders whose claims of surveillance might otherwise be dismissed as paranoia [98]. Forensic proof from iPhones provides undeniable validation, confirming the victim's experience as real and not imagined, which is a crucial step in their healing process and empowers them to pursue legal action and advocacy [99]. Technical findings offer irrefutable evidence for legal proceedings and accountability in national and international forums, revealing strategic implications like data exfiltration during sensitive meetings . Human rights organizations, like Human Rights Watch's Digital Investigations Lab, integrate digital forensic methodologies with human testimonies to expose abuses, demonstrating how technical evidence strengthens human narratives . However, challenges remain in translating complex technical findings into actionable legal outcomes due to a lack of understanding among legal professionals [101]. This highlights the urgent need for an interdisciplinary approach, merging digital forensics, forensic psychology, and human rights advocacy, to ensure comprehensive justice and support for victims .

To further contextualize this, the study will review notable zero-click attacks on iPhones, particularly those involving Pegasus spyware, which has been extensively documented for its sophisticated infiltration capabilities and widespread use by state actors. By examining these specific instances, this research aims to deepen the understanding of the unique relationship between the victim's complete absence of agency during such covert attacks and the subsequent psychological impact, specifically investigating whether feelings of self-blame are a justified or common outcome at a later stage, despite the technical nature of the compromise.

4.1 The Architecture of the Threat: State-Sponsored Spyware and the Nature of Digital Violation

To fully comprehend the profound psychological impact of state-sponsored cyberattacks, it is first necessary to understand the unique technical nature of the weapons employed. This chapter provides this essential context by analysing the security landscape of modern smartphones and the sophisticated mechanisms of spyware like Pegasus. It will demonstrate how specific technical features—particularly the covert and non-interactive nature of zero-click vulnerabilities—create the precise conditions for the distinct psychological trauma, loss of agency, and erosion of trust that this

thesis explores. The Internet, once heralded for its democratizing potential, has become a contested space where the exploitation of inherent vulnerabilities in protocols like BGP is a strategic objective for state actors seeking to maintain surveillance and control [102]. This chapter will deconstruct the architecture of that threat. A comprehensive explanation regarding device security, typologies of vulnerabilities, and the associated attack methodologies and detection strategies is detailed in Appendix 16.

4.2 The Smartphone as a Digital Repository and Battleground

In the current digital landscape, the ubiquitous nature of smartphones, serving as repositories of our most intimate personal data, has amplified the challenges associated with maintaining privacy and security. For individuals engaged in activism and dissent, these devices are both essential tools and primary vectors of vulnerability. Smartphones function as extensions of our lives, containing personal contacts, private communications, confidential documents, and location data. This deep integration has created an ongoing adversarial dynamic: manufacturers and developers continuously integrate robust security features to bolster user trust, while spyware developers and the state actors who employ them actively seek to exploit any remaining vulnerabilities to gain unauthorized access [103]. This continuous struggle imposes significant costs on manufacturers and highlights the ethical complexities inherent within the global spyware industry.

The development of secure smartphones necessitates a delicate balance between feature enhancement and robust security architecture. Operating systems employ hierarchical access control mechanisms, such as protection rings, to mitigate risks by isolating critical system components. However, as this chapter will demonstrate, even the most sophisticated security architectures are not impervious to attack by malicious actors with advanced capabilities [104, 105].

4.3 The Cyber Kill Chain: A Framework for Understanding Digital Violation

To facilitate a comprehensive understanding of the mechanics of a successful cyberattack, this study utilizes the Cyber Kill Chain framework. This analytical model, developed by Lockheed Martin, provides a structured approach to dissecting the lifecycle of an attack [106].

Crucially, for the purposes of this thesis, each stage of this technical process corresponds to a distinct phase of psychological violation for the victim.

- **Reconnaissance**: The attacker gathers information about the target, identifying vulnerabilities. For the target, this is the phase of being profiled and selected, the knowledge of which later fosters a deep sense of paranoia and the feeling of being perpetually watched.
- **Weaponization**: The attacker creates a payload, such as malware or an exploit, tailored to the identified vulnerabilities.
- **Delivery**: The payload is delivered to the target system.

- **Exploitation**: The attacker triggers the payload to gain unauthorized access. This is the moment of intrusion, the violation of digital boundaries that shatters the victim's fundamental assumptions about safety and security.
- **Installation**: The attacker installs malware to establish persistent access.

This stage transforms the victim's device from a personal tool into an instrument of the perpetrator, a constant and intimate presence that reinforces feelings of contamination and helplessness.

- **Command and Control**: The attacker establishes a channel to remotely control the compromised system.
- **Actions on Objectives**: The attacker achieves their goals, such as data theft or disruption. This final stage represents the ultimate realization of the victim's fears, where their private life, professional networks, and personal safety are placed entirely at the mercy of the attacker.

This systematic process highlights the sophisticated tactics employed by malicious actors and underscores the ongoing challenges in securing these ubiquitous devices against cyberattacks [107].

4.4 The Illusion of Security: Platform Vulnerabilities:

Smartphone manufacturers employ a multi-faceted security strategy encompassing hardware, software, and user-centric layers. However, the ability of state-sponsored spyware to bypass these defences is a key factor in the psychological trauma experienced by victims 5.

The iPhone's sophisticated security architecture includes sandboxing, secure enclaves, granular app permissions, and end-to-end encryption [108-110]. Yet, its monolithic kernel design and limited transparency have been sources of concern [111, 112]. Similarly, Android's open-source, layered architecture aims to safeguard data but introduces complexities where vulnerabilities can arise, particularly from third-party applications[113, 114].

The critical point for this research is that the compromise of these fortified systems shatters the user's perception of a "safe choice." When even the most secure and trusted platforms are proven vulnerable, it cultivates a pervasive sense of insecurity from which there is no escape, contributing directly to the hypervigilance and generalized anxiety documented in the findings.

4.5 The Nature of the Weapon: Spyware and Zero-Click Exploits:

Spyware is a form of malicious software that operates by surreptitiously monitoring a user's system without their knowledge or consent. It is distinct from other malware in its primary objectives, which, in the context of state-sponsored attacks, are stealth, effectiveness, persistence, and adaptability. While some spyware operates covertly to collect specific information, the more intrusive forms used against dissidents aim to transform the compromised device into a comprehensive surveillance tool,

[5] More details in appendix 15

granting attackers capabilities for remote control, keylogging, audio and video surveillance, and location tracking [115-117].

The development of such sophisticated spyware involves exploiting vulnerabilities, often at the device's kernel layer. Post-installation, spyware can infiltrate various system layers to access text messages, call logs, emails, media files, and passwords. It can even activate the device's microphone and camera or intercept encrypted communications, rendering all aspects of the device's privacy and security compromised [118].

The most psychologically devastating delivery mechanism is the zero-click exploit. This method enables the surreptitious installation of spyware without requiring any user interaction whatsoever [119, 120].

This technical reality is central to understanding the psychological aftermath of these attacks. Because the victim is not required to take any action, such as clicking a link, the attack removes any possibility of user error. This directly informs the participants' unanimous rejection of self-blame and fosters a profound sense of powerlessness, as their security is compromised regardless of their own vigilance or digital literacy. The covert nature of the attack means the violation occurs without the victim's knowledge, creating a delayed but more profound shock upon discovery and leaving a lasting sense of uncertainty about when the intrusion began and what was compromised.

4.6 Notable Zero-Click Vulnerabilities: Case Studies in Helplessness

The evolution of spyware has been characterized by an ongoing arms race between attackers and defenders, with vulnerabilities in widely used applications serving as primary vectors for infection. T o illustrate the sophistication of spyware exploiting zero-click vulnerabilities, the following examples are instructive, as they demonstrate how even first-party, manufacturer-controlled systems can be compromised. A more detailed technical breakdown of these vulnerabilities is provided in Appendix 16.

BLASTPASS (CVE-2023-41064, CVE-2023-41061): Identified by Citizen Lab in September 2023, this exploit targeted Apple's own PassKit framework via a malicious iMessage attachment [119].

The fact that this vulnerability existed within Apple's first-party framework 1 is a crucial factor in the complete erosion of trust experienced by victims; when even the most secure and controlled ecosystems are compromised, it reinforces the pervasive sense that no digital space is safe.

KISMET: Discovered in December 2020, this zero-click vulnerability also targeted iMessage to install Pegasus spyware on the devices of journalists in the GCC. The exploit left traces of anomalous iCloud connections and kernel crashes, but its precise mechanism remains undisclosed by Apple, which limits public understanding and broader security enhancements [121].

FORCEDENTRY (CVE-2021-30860): Disclosed in August 2021, this exploit used a maliciously crafted PDF disguised as a GIF to bypass iMessage's sandbox protection. 1 The attack, which required only the victim's phone number, leveraged Apple's own image processing services to execute the Pegasus payload [120].

The involvement of only first-party Apple applications again underscores the victim's complete lack of agency in the attack, intensifying feelings of helplessness and betrayal by the technology provider they trusted for security.

TRIANGULATION: Discovered by Kaspersky Lab in June 2023, this sophisticated attack, active since 2019, also used malicious iMessage attachments to compromise devices [122].

WhatsApp VOIP Vulnerability (CVE-2019-3568): In May 2019, a vulnerability in WhatsApp's voice-call feature was exploited by Pegasus. Attackers could install the spyware simply by placing a call to the target's device, which did not even need to be answered. Facebook (now Meta) subsequently filed a lawsuit against NSO Group for compromising approximately 1,400 users on behalf of state actors [123-125].

4.7 The Challenge of Detection and the Reinforcement of Powerlessness

The detection of state-sponsored spyware presents significant challenges. Government-backed initiatives benefit from substantial funding and expertise, creating a stark resource disparity with the civil society organizations working to counter them. This asymmetry is not just a technical challenge; it is a psychological one.

The detection of spyware often relies on victims proactively seeking assistance from a small number of specialized research institutes like Citizen Lab and Amnesty Tech. These organizations have developed innovative methodologies involving network scanning, forensic device analysis, and the use of custom tools to identify spyware infrastructure and traces of infection on compromised devices [126]. However, access to this expertise is often limited, typically requiring connections through established NGO or activist networks.

his reality further reinforces the victim's sense of helplessness. The inability for an individual to independently verify a compromise, coupled with the difficulty in accessing the few organizations capable of doing so, deepens feelings of isolation and dependence. The knowledge that detection is a reactive process, often occurring long after the initial intrusion, contributes to a chronic state of anxiety and the unsettling feeling that one's privacy is perpetually at risk, with no effective means of self-protection.

5 Ethical Considerations

5.1 Introduction Imperative of Ethical Considerations

Research involving vulnerable individuals, particularly those who are confirmed victims of state-sponsored attacks and may be grappling with past trauma, psychological impacts such as PTSD and depression, and ongoing political risks, demands a profound and rigorous commitment to ethical conduct[127]. As this research is conducted under the University of York MSc programs, the ethical framework underpinning this study adheres strictly to institutional policies, including the Research Data Management policy[128], research ethics guidelines[129], and the Code of Practice on Research Integrity[130]. This framework is not merely a procedural requirement but an essential practice to ensure the safety, dignity, and well-being of all participants, as well as the integrity and credibility of the findings. Given the heightened sensitivities, protecting participants was a paramount concern before, during, and beyond the data gathering phase.

This chapter outlines the comprehensive ethical considerations that have guided every stage of this research. Subsequently, it will delve into the specific strategies employed to address the unique challenges presented by this sensitive topic, focusing on informed consent processes, participant safety and wellbeing (minimizing harm), confidentiality and anonymity, data security and management (including data minimization and UK GDPR compliance), and the researcher's role. By addressing these ethical frameworks, this research aims not only to contribute to the understanding of the psychological impact of state-sponsored repression but also to uphold the highest standards of respect and protection for those whose voices are shared.

5.2 Ethical Approval

University of York code of practice on research integrity outlines ethical guidance and responsibilities for conducting research, especially regarding dealing with vulnerable people, this involve applying for ethical approval to the relevant departments, explain the purpose of the study, what measures are in place to protect the identity of the participants, how the collected data processed – securely collected and stored [6] -. For that reason, with the approval from the computer science department, An ethical approval application form was submitted to the physical sciences ethical committee along with the supported documents which include the consent template and GDPR Compliant Participant information sheet which was approved by the committee.

In the Physical Sciences Ethics Committee application form, an explanation of the nature of the study, who to target? the type of the data which will be collected and how it will be collected and stored securely, the period for the data to be stored, the risk assessment which was approved by the department.

[6] As explained in detail in the Methodology

5.2 Informed Consent Process

In the consent form, the nature and the goal of the study was explain briefly , then it detailed the rights for the participants as well as how the research will process the collected data, how it will be processed, It was also mentioned that the anonymity of the participation will be protected and their real name will be replaced by initials, in the consent the period for keeping the data were highlighted to the participants to assure them that no materials will be stored after the study is completed. Also, participants were clearly made aware that they can withdraw from being part of this study at any stage before or during the study , Participants were also provided with the data protection officer at the university contact details for any clarifications or complaints. This is to assure that participants are fully aware that they are not under pressure at any stage during the period of the study and assuring them about their rights, this an essential part of the university research code of practice where the participants are fully informed of the goal of study and their rights, making sure that their participation are voluntary.

While a consent form were send to all the participants prior the interviews, a recorded consent were taken at the beginning of each interview after the introduction of the project and detailed of their rights and safety. All interviews were done voluntarily without any pressure or compensation.

5.3 Confidentiality, Anonymity, and Data Security

In both the consent form and physical sciences ethics committee, it was mentioned that only the research conductor will have access to the real identity of the participants, however, if it was requested for clarification and authenticity , the supervisor might ask for access, but only after the approval from the participants themselves.

As the collected materials will be sensitive and belong to vulnerable people, it was mentioned in the consent form and physical sciences ethics committee application form that all the materials that can be used to identify individuals will be destroyed permanently, this was also explained in details for all participants at the beginning of each interview.

5.4.1 Data Management and UK GDPR Compliance

This research adheres to the principle of data minimization as mandated by the UK general Data Protection Regulation (UK GDPR)[131] and Ethical best practice[128, 129]. Only personal data absolutely essential for addressing the research questions will be collected. The interviews were carefully designed to collect data for the study objectives avoiding the collection of any unnecessary personal details that could increase the risk of the participants.

As the nature of the study confirmed that personal data might be collected and processed as defined by Uk GDPR [131] , include demographic data, political opinions and experiences that may reveal data related to their health (such as psychological issues or trauma. An explicit consent was the lawful

basis obtained from each participant for the processing of any data will be collected during the interview, especially for the processing of these categories of special category data for the clearly defined research purposes[131], also this was explain prior the interview is started for each participant. The consent form detailed the how we are going to collect the data and how it will be processed as well as the destroying of all the data collected after the study is finished[7].

All the collected data are subjected to the robust security measures detailed through the methodology chapter earlier, ensuring their integrity and confidentiality in compliance with UK GDPR requirements and University research data management policy[128].

5.4 Minimizing Harm and Trauma-Informed Approach

Risk Assessment of participants safety, from physical , psychological or social risks were conducted before submitting the ethical approval forms with the help of the computer science department , and since employing the participants were done through close circuit due to the nature of the study, the first approach to establish contact with victims is very important to build up trust relationship between the researcher and the victims. The connection was established through two approach, firstly by the researcher who himself helped to discover and proof the use of the surveillance spyware operated by state-sponsored for some of the participants, and secondly through a third party8 who explain the nature and goal of the study and to assure them that the whole process will be done securely and anonymous, a message of assurance was send to ensure that all precautions measures were taken to ensure that their safety is a priority at the institute. This is helped to receive positive responses from the participants that lead to the success of this phase of the project.

Dealing with who might be vulnerable or his mental health wellbeing could be affected by the cyberattack event require a careful Language that should be clear to them with short sentences, show them our respect, empathetic and empowering , and avoiding any words or phrases that might trigger them in negative way, it's also important to show our understanding and concerns to what did they went through without any judgments[132, 133]. The researcher him self have worked previously with some of the participants to discover the use of spywares in their devices, this was an additional help to make the communication with participants successful and the trust relationship with them is stronger.

6 The Legal and Policy Landscape of State Sponsored cyberattacks

The use of state-sponsored cyberattacks against dissidents, particularly those with sophisticated technology, require a clear understanding of the governance frameworks that apply – or fail to apply

[7] Copy of the Consent Form can be found in appendix 2

[8] Citizenlab and Accessnow who are well-known for countering spyware usage globally helped establish the communication with some of the participants.

– for such actions. Policies and laws are always in place by the entities that have a role in this operation, thus a clear distinguish between laws and policies is fundamental to evaluating the efficacy of international and national responses to the challenges and its impact on basic human rights, the Inherent purpose of spyware to violate individual privacy create a collective responsibility among governments, technology manufacturers and legal systems to ensure personal safety and uphold mutual trust within the digital realm. This chapter is critically analysis the legal frameworks and policy pronouncement relevant to state-sponsored cyberattacks with a particular focus on dissidents in the GCC.

6.1 Defining "Law" and "Policy"

Law: Law constitutes a formalized system of rules enacted by governing authorities—whether national or international—and enforced through institutionalized mechanisms such as courts. At the domestic level, statutes codified by legislative bodies establish binding norms to regulate state-citizen relations, delineate rights and obligations, and maintain societal order[134]. In the international realm, legal obligations arise from ratified treaties, which impose duties on states to uphold human rights[135], as well as customary international law, derived from consistent state practice coupled with *opinio juris*[136]. Ultimately, law serves to prescribe and prohibit conduct while furnishing a structured framework for justice and governance[137].

Policy : Policy comprises a set of formalized guidelines or principles adopted by an organization-whether governmental, corporate, or international—to direct decision-making and advance strategic objectives[138] Unlike legally binding statutes, policies articulate institutional intent, values, and approaches to specific issues[139] For instance, a national cybersecurity policy may outline priorities for safeguarding digital infrastructure, while a corporate human rights policy codifies ethical commitments[140]. Critically, policies lack inherent enforceability unless they operationalize legal obligations or are codified into law[141]. As frameworks, policies typically address the "what" (objectives) and "why" (rationale), while remaining agnostic to the "how" (procedures) and often technology-neutral[140].

The interplay between law and policy is complex, while laws enforce policy, policies operationalize legal mandates[139, 141] confusing these roles can lead to governance inefficiencies.

Soft Law: like Un resolutions, is non-binding but crucial in shaping international norms, influence state behaviour and encourage reforms, and often preceding – or encouraging - Hard Law which is a binding rules[142].

Understanding these distinctions is vital for analysing governance around technologies such as spyware. Responses range from binding laws to non-binding policies [140], with effectiveness tied to their legal force or guiding nature.

Entities use policy in digital human rights to influence law, shaping future instruments to their advantage or presenting self- regulation to delay “hard law”[139].

Unclarity between “law” and “policy” can be leveraged to evade accountability. Unlike enforceable laws, policies are often internal guidelines which can be employed as for minimal protection compared to clear legal frameworks. This allows actors to appear ethical while potentially falling short of legal requirements.

The reliance on "soft law" in cyber surveillance reflects a lack of international consensus for "hard law." However, it is crucial for building norms that can eventually crystallize into customary international law, as seen with the Universal Declaration of Human Rights[142]. While some argue that evolving digital governance requires time to balance security and privacy concerns[143], Evidence suggests that sophisticated spyware is disproportionately used by states with poor human rights records[144]. Such tools frequently target dissent under national security pretexts [145], suggesting regulatory delays enable abuse rather than reflect legitimate implementation challenges.

To Summarise the different between law and policy in Governance, the below table define the different:

Table 3: Different between Law and Policy

Aspect	Law	Policy
Definition	A system of rules established by a governing authority, enforceable by legal means.	A set of guidelines or principles created by organizations or governments to guide decision-making and achieve specific goals.
Nature	Prescriptive/Proscriptive; establishes rights and obligations.	Strategic; aspirational; guiding framework; often answers "what" and "why" without detailing "how".
Bindingness	Legally binding and mandatory.	Generally non-binding, unless codifying a legal duty or backed by specific laws.
Origin	Legislative bodies (statutes), international treaties, customary international practice.	Governments (strategies, white papers), organizations (corporate policies), multi-stakeholder groups (declarations).
Enforcement	Courts, legal sanctions, formal dispute resolution mechanisms.	Political pressure, reputational impact, internal compliance mechanisms, monitoring; may be supported by laws.
Examples in Cyber/Surveillance Governance (International & National)	International Covenant on Civil and Political Rights (ICCPR); National Cybercrime Statutes (e.g., Bahrain Law No. 60 of 2014); EU General Data Protection Regulation (GDPR).	UN General Assembly Resolutions on Privacy in the Digital Age; National Cybersecurity Strategies (e.g., UAE National Cybersecurity Strategy 2019); Corporate Human Rights Policies (e.g., NSO Group's stated policy).

6.2 The universal Declaration of Human Rights (UDHR): Foundational Principles and its dual legal-policy status

The universal Declaration of Human Rights serves as a foundational pillar of international human rights, with article 12 which ensure the right to privacy against arbitrary interference (privacy), and article 19 which guarantees freedom of opinion, expression and the exchange of information, furnish directly applicable and essential criteria for the critical assessment of state-sponsored spyware and its implications[146]. Originally a non-binding policy statement many UDHR provisions are now widely regarded as customary international law, giving it a dual status as both influential policy and, in part, binding law[147, 148]. This evolution underscores its enduring, technology-neutral relevance as a legal and ethical benchmark for evaluating contemporary surveillance practices. Its principles are frequently invoked diplomatically, further highlighting its policy impact in shaping international norms against spyware misuse.

Building on this foundation, UN General Assembly and Human Rights Council resolutions on digital privacy, while non-binding – soft law -, carry significant political weight, encouraging states to align surveillance practices with legality, essentiality and proportionality[142, 149, 150]. Experts and special rapporteurs reports, such as " the right to privacy in the digital age " [144, 149, 150], provide critical and thoughtful analysis and policy guidance, including calls for a moratorium on high-risk spyware[149]. These reports often highlight and distinguish between reiterating existing legal obligations and proposing progressive policy to address regulatory gaps, the prevalence of such soft law and policy recommendations, rather than a binding treaty on surveillance, signals ongoing norm development but also reflects a lack of political consensus among states for stricter, legally enforceable limitations on their surveillance capabilities.

6.3 International Efforts to Counter Spyware Misuse: Policy Declarations and Emerging Norms

The International community's response to the escalation challenges presented by the misuse of commercial spyware has largely fall under the " soft law" mechanisms and policy rather than through the establishment of legally binding international treaties. This preference for non-binding instruments- such as political commitments, voluntary codes of conduct and expert recommendations- highlights a cautious approach to international regulation in this sensitive domain, a phenomenon extensively explored in the literature on international norm development and the utility of soft law[142]. These approaches signal an attempt to build consensus and guide state behaviour incrementally, often as a precursor to , or substitute for, more formalized legal structures.

A good example of this trend is the 2023 multinational joint statement on efforts to counter the proliferation and misuse of commercial spyware. This initiative articulates shared political commitments among its growing number of signatory nations, which pledge to enhance domestic controls over spyware, improve cross-boarder information sharing on related threats, and align their national export licensing practices with human rights considerations[151]. However, the impact nature of the joint statement as a soft law instrument is underscored by its explicit deference to national legal frameworks and existing capacities, thereby lacking direct international enforceability and relying on the individual and collective political will of its endorsers for meaningful implementation.

Similarly the European Parliament's Committee of inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA Committee) has issued a well strong recommendations advocating for a more stringent and harmonized regulatory environment within the European Union[152]. These recommendations include ambitious calls for new EU-level legislation specifically designed to govern the spyware market and its use by national authorities, reflecting a significant push towards regional 'hard law'[153]. However, a hopefully development of these proposals towards

legally binding EU regulations is graught with significant political opposition from some member states. These states often express concerns about preserving national discretion, particularly concerning matters of intelligence gathering and national security, thereby illustrating the difficult transition from parliamentary policy aspiration to binding regional legal obligations.

Collectively, such diverse international and regional initiatives, while indicative of a growing global concern over spyware abuse and contributing to the gradual edification of norms against its irresponsible use, primarily serve to guide state conduct and foster dialogue rather than imposing immediate, universally binding legal obligations. Their effectiveness in practice is therefore heavily reliant on the voluntary adherence and sustained political will of participating states to translate these commitments into concrete national actions and policies. This dynamic inevitably cultivates a fragmented global governance landscape for spyware, characterized by a patchwork of varying standards and levels of commitment rather than uniform, universally enforceable rules, a common challenge in governing rapidly evolving technologies with diverse state interests[154].

Consequently, tangible progress towards comprehensive and consistently applied international regulation of spyware is frequently obstructed by several persistent and interconnected challenges. Competing national interests, which may include economic stakes in the surveillance technology market or perceived geopolitical advantages, often temper enthusiasm for stringent controls. Furthermore, varying levels of technical and financial capacity among states to implement and monitor compliance with any agreed standards present practical difficulties. Perhaps most significantly, the pervasive and often ambiguously defined invocation of 'national security' exceptions by states creates substantial loopholes, allowing for justifications of spyware use that can undermine both existing legal frameworks and these emerging policy efforts[143, 155].

6.4 Challenging Spyware Developer Impunity: The Case of NSO Group

Spyware developer Like NSO group is at the heart of the controversy surrounding state-sponsored cyberattacks. Their product is sophisticated surveillance tools, and their corporate policies and compliance with legal frameworks are under intense scrutiny.

Notably, NSO group critically highlights the profound disjuncture between corporate human rights policy commitments, national legal frameworks governing technology exports and the documented patterns of spyware usage that result in violation of individual rights and abuses. NSO group for instance, publicly articulates a corporate policy ostensibly aligned with the un guiding principles on business and human rights (UNGPs), claiming its powerful surveillance tools like Pegasus are sold exclusively to state actors for legal purposes such as countering serious crime and terrorism, and that it investigates alleged misuse[156, 157]. However, this stated policy is starkly contradicted by extensive credible evidence and investigations documenting the deployment of Pegasus by state

clients to unlawfully target journalists, human rights defenders, lawyers, political dissidents and even heads of state, thereby creating a chilling effect on fundamental freedoms[29, 158-161].

This wide and known misuse persists despite NSO Groups operations being subject to Israeli export control laws, which are, in principle, designed to regulate the foreign dissemination of sensitive defence and dual-use technologies, purportedly in line with international norms like those of the Wassenaar arrangement9. In practice, however, critical analyses and whistleblower accounts suggest that Israel's export licensing regime, administered by the Defence Export Control Agency (DECA) and Ministry of defence , has often prioritized national security imperatives, foreign policy objectives, and economic benefits derived from its leading cyber-industry over substantive human rights risk assessments [162-164]. The reported lack of judicial review over these licensing decisions further compounds concerns about transparency and accountability in this crucial legal oversight process. While international policy pressure, such as the US placing NSO group on its entity list[165], has reportedly prompted some tightening of these export controls, the systemic tendency to subordinate human rights to other state interests remains a significant legal and policy challenge.

The consequence is a significant "chasm" where NSO Group's corporate human rights policy appears largely ineffective as a preventative measure, often criticized by civil society as a public relations facade rather than a robust compliance mechanism. Simultaneously, the state-level legal and regulatory policies governing export have failed to consistently prevent spyware from reaching end-users who deploy it for repressive purposes. This situation underscores the formidable difficulties in regulating powerful dual-use surveillance technologies. Companies may deflect responsibility for misuse onto their sovereign state clients, while these clients, in turn, frequently invoke opaque national security justifications to shield their surveillance activities from scrutiny[143]. Addressing this governance deficit requires a more rigorous alignment of corporate due diligence, national export control laws, and international human rights obligations, moving beyond policy declarations to enforceable legal accountability for all actors involved in the spyware ecosystem.

Further complicating NSO Group's claims of operating solely as a passive technology provider to legitimate state actors is the significant ongoing litigation initiated by WhatsApp (now owned by Meta). This lawsuit alleges that NSO Group unlawfully exploited a vulnerability within the WhatsApp messaging service to deploy its Pegasus spyware against targeted individuals, directly implicating the company in the operational aspects of the surveillance[166, 167] . Throughout the proceedings, NSO Group has reportedly resisted certain discovery obligations and consistently sought to shield itself from liability by asserting that it acts merely as an agent for its foreign government clients, thereby attempting to invoke derivative sovereign immunity. However, this defence has faced substantial legal

[9] A multilateral agreement (1996) controlling arms and dual-use technology exports to enhance global security.

setbacks; U.S. courts have largely rejected NSO Group's broad immunity claims, culminating in the U.S. Supreme Court declining to hear NSO's appeal in January 2023. This pivotal decision affirmed lower court rulings, compelling NSO Group to engage with the legal process in the United States and comply with discovery orders it had vigorously contested, thus allowing the substantive claims regarding its role in the alleged surveillance to be further scrutinized[168].

6.5 Corporate Responsibility and Accountability: Policies, Practices, and Legal Parameters

The role of private corporations, particularly smartphone manufacturers and spyware developers, is central to the ecosystem of digital surveillance. Their corporate policies, product designs, and adherence to legal obligations significantly impact the ability of states to conduct cyberattacks and the capacity of individuals to protect their privacy and security.

Smartphone manufacturers such as Apple act as critical gatekeepers for the digital ecosystems vulnerable to spyware, making their corporate policies on user privacy and security exceptionally significant. Apple publicly promotes a robust commitment to fundamental privacy rights, embedding this into its product design through measures like widespread end-to-end encryption, which often technically limits even Apple's own access to substantial portions of user data [155, 169]. This strong pro-privacy stance inherently conflicts with its legal obligations under various national laws to respond to government demands for user information. Apple navigates this tension via stringent internal policies for scrutinizing the legal basis of each state request and through the publication of regular transparency reports that detail the volume and nature of such demands [170, 171]. However, the depth and scope of these transparency initiatives are frequently constrained by legal restrictions, particularly for national security-related orders, demonstrating how binding law can circumscribe even well-intentioned corporate disclosure policies. Beyond data access, Apple's corporate decisions regarding the extent to which it shares detailed information about security vulnerabilities within its platforms also represent critical policy choices, which can have considerable implications for the broader cybersecurity research community and the overall security of its users[172].

6.6 GCC Legal and Policy Frameworks: National Laws, Regional Policies, and Human Rights Compliance

The legal and policy landscape concerning digital rights, surveillance, and freedom of expression within Gulf Cooperation Council (GCC) states is complex, frequently revealing a significant tension between constitutional provisions that nominally guarantee fundamental freedoms and an array of national laws that severely curtail them, often under the wide umbrella of national security. While the constitutions of states like Bahrain, Saudi Arabia, and the UAE contain articles affirming rights to privacy and freedom of expression, these are almost invariably qualified by clauses subordinating them to other legislation, public order, or religious principles. In practice, restrictive national laws,

particularly broadly-defined cybercrime statutes, effectively hollow out these constitutional safeguards. For example, Saudi Arabia's Anti-Cybercrime Law (Royal Decree M/17 of 2007) criminalizes the production or dissemination of online content "impinging on public order, religious values, public morals, and privacy" (Article 6), and the UAE's Federal Decree-Law No. 34 of 2021 on Combating Rumors and Cybercrimes similarly penalizes the spread of "false information" or content deemed harmful to "national unity." Such vaguely worded provisions provide authorities with extensive discretion to suppress dissent and critical speech, thereby creating an environment where state-sponsored spyware can be deployed against perceived adversaries with limited legal recourse for those targeted [173].

In recent years, GCC states, including Bahrain (Personal Data Protection Law, 2018), Saudi Arabia (Personal Data Protection Law, 2021, as amended), and the UAE (Federal Decree-Law No. 45 of 2021), have enacted comprehensive Data Protection Laws (DPLs), ostensibly aligning with global trends in data governance. These laws establish frameworks for the lawful processing of personal data and outline data subject rights. However, a critical feature of these DPLs is the inclusion of broad and often ill-defined exemptions for activities related to national security, defence, or law enforcement. These exemptions can significantly undermine the laws' effectiveness in protecting individuals from state surveillance conducted via spyware, potentially rendering data protection principles inapplicable in precisely the contexts where they are most needed. Simultaneously, national cybersecurity strategies are being promulgated as high-level policy documents. While these strategies aim to bolster national cyber defences, they may also implicitly or explicitly endorse the expansion of state surveillance capabilities without concurrently mandating robust human rights safeguards, transparent oversight, or adherence to principles of necessity and proportionality in the deployment of such technologies [143, 174-178]

A crucial aspect compounding the challenge for victims of state-sponsored cyberattacks in the GCC is that domestic legal frameworks, including many cybercrime laws, are typically designed to address offenses between private or non-state entities—such as an individual hacking another individual, or an individual hacking a company—and outline legal procedures and actions for these specific scenarios. However, these laws generally fail to explicitly address or provide clear rights, specific legal avenues, or effective mechanisms for redress when individuals are subjected to hacking or surveillance by state authorities themselves. This significant legislative and procedural omission directly contributes to the "justice vacuum" faced by those targeted by their own governments. Consequently, for dissidents and human rights defenders, pathways to domestic accountability and redress are exceptionally challenging, if not entirely absent, arising from a combination of these overarching legal gaps, severe evidentiary hurdles in proving state involvement, and systemic concerns regarding

judicial independence in politically sensitive cases. Faced with these domestic barriers, some victims have sought recourse in foreign jurisdictions, such as the United Kingdom in cases like Al-Masarir v Saudi Arabia and Shehabi v Bahrain. While facing inherent difficulties in enforcing international human rights law against sovereign states, these international legal efforts are significant. They serve to expose alleged abuses, contribute to the legal discourse on issues like state immunity for transnational cyber-surveillance, and advocate for the development of stronger international accountability norms and mechanisms[179-181].

In another scenario, the UK High Court case, Privacy International v HMRC, cantered on the enforcement of UK export controls related to FinFisher spyware. The Court found Her Majesty's Revenue and Customs (HMRC) had acted unlawfully and "irrationally" in its blanket refusal to disclose information regarding its investigation into the spyware's potentially illegal export to repressive regimes. This judgment affirmed the public's and NGOs' right to information concerning the enforcement of export controls, particularly when human rights are implicated. Crucially, the case primarily underscored significant policy and enforcement gaps within the UK's existing export control regime for surveillance technology, thereby calling for policy reform and more diligent application of current laws, rather than establishing new substantive export control rules itself [182].

6.7 Conclusion

This chapter reveals a critical and pervasive disjuncture between proclaimed human rights principles—enshrined in international law, corporate policies, and national constitutions—and the operational reality of state-sponsored digital surveillance, particularly impacting dissidents in the GCC region. The core finding is that the distinction between binding, enforceable 'law' and often overriding, strategically deployed state 'policy' is fundamental to understanding this gap. International human rights law provides essential norms but suffers from significant enforcement deficits against determined states, while corporate self-regulation by technology providers frequently proves inadequate without stringent oversight and accountability.

Within the GCC, national legal frameworks, including cybercrime and anti-terrorism laws, are often instrumentalized to enact policies of stringent state control, systematically subordinating nominally guaranteed constitutional rights to expansive interpretations of national security. This effectively legitimizes widespread surveillance and the suppression of dissent, creating a profound accountability vacuum for victims of state-sponsored cyberattacks. Ultimately, countering the advance of 'digital dictatorship' requires a fundamental shift beyond aspirational policies and weakly enforced legal provisions. It demands the establishment and rigorous application of robust, genuinely enforceable legal frameworks at both national and international levels, underpinned by unwavering political commitment to prioritize and protect human rights in the digital age.

7 Presentation and Analysis of Findings

7.1 Participant Recruitment and Data Collection

As previously outlined in the methodology section, two separate interviews were conducted with each participant who volunteered for this study. The interviews took place between January 2023 and May 2024, with an average duration of approximately 40 minutes, contingent upon the depth and breadth of the participants' responses.

All participants consented to video recording of the interviews, with the exception of one male participant who preferred an audio-only format. While five participants expressed a willingness to have their real names published, the remaining participants opted for anonymity. To protect the identities and ensure the safety of all participants, they are referred to by case number throughout this study. This approach prioritizes ethical considerations and ensures participant confidentiality while maintaining the integrity of the research findings.

The first interview sought to elicit in-depth information pertaining to the following key areas:

1. **The Cyberattack Incident**: This encompassed a detailed exploration of the incident itself, including the perceived perpetrators, the methods employed in the attack, and the participants' understanding of the technical aspects involved.
2. **Behavioural and Psychological Impact**: This focused on identifying any changes in the participants' behaviour, emotional state, and their relationship with technology following the cyberattack. This included assessing their levels of trust, anxiety, and any coping mechanisms they employed.
3. **Attribution of Responsibility**: This explored the participants' perspectives on who they held responsible for the attack and the perceived motivations behind it. This included examining the role of various actors, such as the state, spyware developers, and technology companies, in facilitating or mitigating such attacks.
4. **Aftermath of the Incident** : This investigated the long-term impact of the cyberattack and the participants' coping mechanisms. It examined how participants coped with the incident, any significant life changes that occurred as a result, and any new behaviours or strategies they adopted to protect themselves.

This structured approach to the first interview allowed for a comprehensive exploration of the participants' experiences and perceptions, laying the groundwork for subsequent qualitative and quantitative analysis.

Demographic information was collected prior to the commencement of each interview to facilitate subsequent data analysis. This information, presented in the table below, provides a descriptive

overview of the participant pool and enables the exploration of potential demographic trends within the data.

Case ID	Gender	Work	Age range	Education
Case 1	Male	Activists	35-45	Secondary School
Case 2	Female	HRD	35-45	MSc
Case 3	Female	HRD	45-55	Diploma
Case 4	Male	Activists	45-55	MSc
Case 5	Male	Activists	25-35	BSc
Case 6	Male	Politician	55-65	PHD Student
Case 7	Male	Politician	25-35	BSc
Case 8	Female	HRD	55-65	PHD
Case 9	Male	jurnalist	25-45	BSc
Case 10	Male	HRD	65+	BSc
Case 11	Male	Journalists	25-35	MSc
Case 12	Male	HRD	55-65	BSc
Case 13	Male	Lawyer	55-65	BSc
Case 14	Male	Activists	25-35	MSc
Case 15	Male	HRD	35-45	BSc
Case 16	Male	Journalists	35-45	Diploma

Table 4 : Demographic data from participants

The participants in this study comprised a diverse group of individuals from various GCC countries. The sample included three females and thirteen males, representing a range of age groups, with five participants aged 55 years or older. The majority of participants held at least one degree, with six possessing postgraduate qualifications and only one having not attended university.

Their professional backgrounds varied, but the majority identified as human rights defenders, primarily engaged in documenting human rights violations and communicating with the international community. The remaining participants included four activists working in various domains, three journalists, two politicians, and one lawyer. This diverse sample ensures a range of perspectives and experiences, enriching the qualitative data and providing valuable insights into the impact of state-sponsored cyberattacks on individuals actively engaged in challenging authoritarian practices within the GCC.

While the 20 questions comprising the interview protocol were designed to elicit comprehensive data from the participants, six key questions warrant particular attention in the analysis. These questions, namely 7, 8, 9, 10, 17, and 18, were specifically crafted to elucidate the changes that occurred in the

participants' lives following the cyberattacks. These changes encompass various domains, including their emotional well-being, behaviour, relationships, and perspectives on technology and security. Additionally, questions 15, 19, and 20 hold significance in providing further insights into the participants' experiences and coping mechanisms. While all questions contribute to the overall analysis and inform the study's findings, these key questions serve as focal points for understanding the multifaceted impact of state-sponsored cyberattacks on dissidents.

The second phase of the study involved a quantitative assessment of the participants' psychological [10]well-being using the Harvard Trauma Questionnaire (HTQ), a standardized self-assessment tool developed by researchers at Harvard University [183].

Following the transcription of the initial interviews and the completion of the HTQ, all resulting data were imported into NVivo software. This platform facilitated the creation of codes and themes from the qualitative textual data, enabling a systematic identification of recurring patterns and in-depth thematic analysis. Simultaneously, the quantitative HTQ data was integrated, allowing for a comprehensive comparative analysis across both datasets. This unified approach in NVivo was crucial for identifying correlations, convergences, and divergences between participants' self-reported experiences and the psychological symptom scores.

[10] More about HTQ in section 8.4 Harvard Trauma Questionnaire

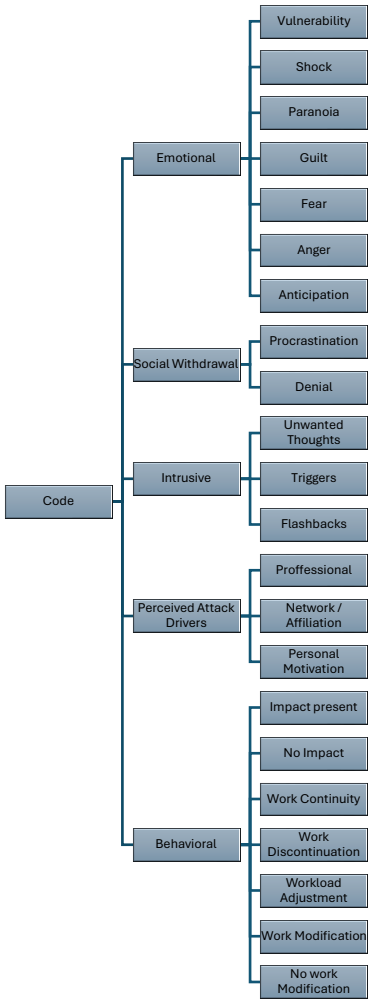


Figure 1 : The thematic analysis in NVivo yielded several primary themes and their corresponding sub- codes, illustrating the multifaceted impact of the cyberattacks

Participants showed remarkable engagement throughout the process, recognizing the research's importance for human rights and digital security in the GCC region, which significantly enriched the depth and quality of the collected data on the lived experiences of dissidents facing state-sponsored cyberattacks.

7.2 Qualitative Findings: Thematic Analysis

Analysis of the interview data revealed that participants experienced notable shifts in both their psychological well-being and behaviour following the discovery of state-sponsored hacking of their devices. These shifts manifested across several domains:

- **Perception of Technology**: Participants exhibited increased distrust and apprehension towards digital devices and online communication platforms, often leading to modifications in their technology usage patterns. This included heightened awareness of security risks,

adoption of enhanced privacy measures, and in some cases, a reduction in overall technology reliance.

- **Interpersonal Relationships**: The experience of being targeted for surveillance engendered heightened suspicion and mistrust within interpersonal relationships, both personal and professional. This impacted their sense of safety, openness in communication, and overall social connectedness.
- **Psychological Well-being**: Participants reported a range of psychological and emotional impacts, including symptoms of anxiety, depression, and post-traumatic stress. These experiences frequently led to self-doubt, diminished self-esteem, and concerns about their mental health and overall well-being.

These findings underscore the profound and multifaceted consequences of state-sponsored cyberattacks on the lives of dissidents, extending beyond the immediate violation of privacy to encompass significant psychological and social impacts.

7.2.1 Psychological and Emotional Impact

The initial discovery of state-sponsored cyberattacks elicited a striking and often uniform emotional upheaval among participants. Question 7, designed to capture these immediate reactions, revealed a shared lexicon of distress, vividly illustrated in the accompanying chart and word cloud. This commonality in expression suggests a collective psychological shockwave, where the violation transcended individual circumstances to provoke a deeply unsettling sense of exposure and vulnerability.

Chart 1：Participants reflecting to the news of the attack

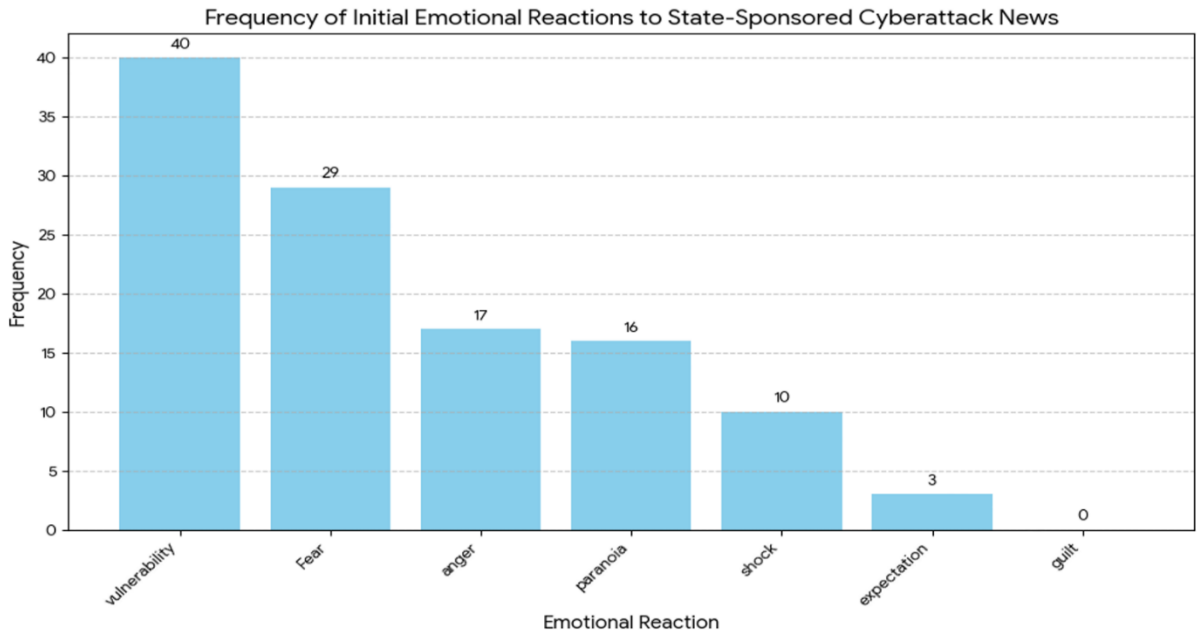
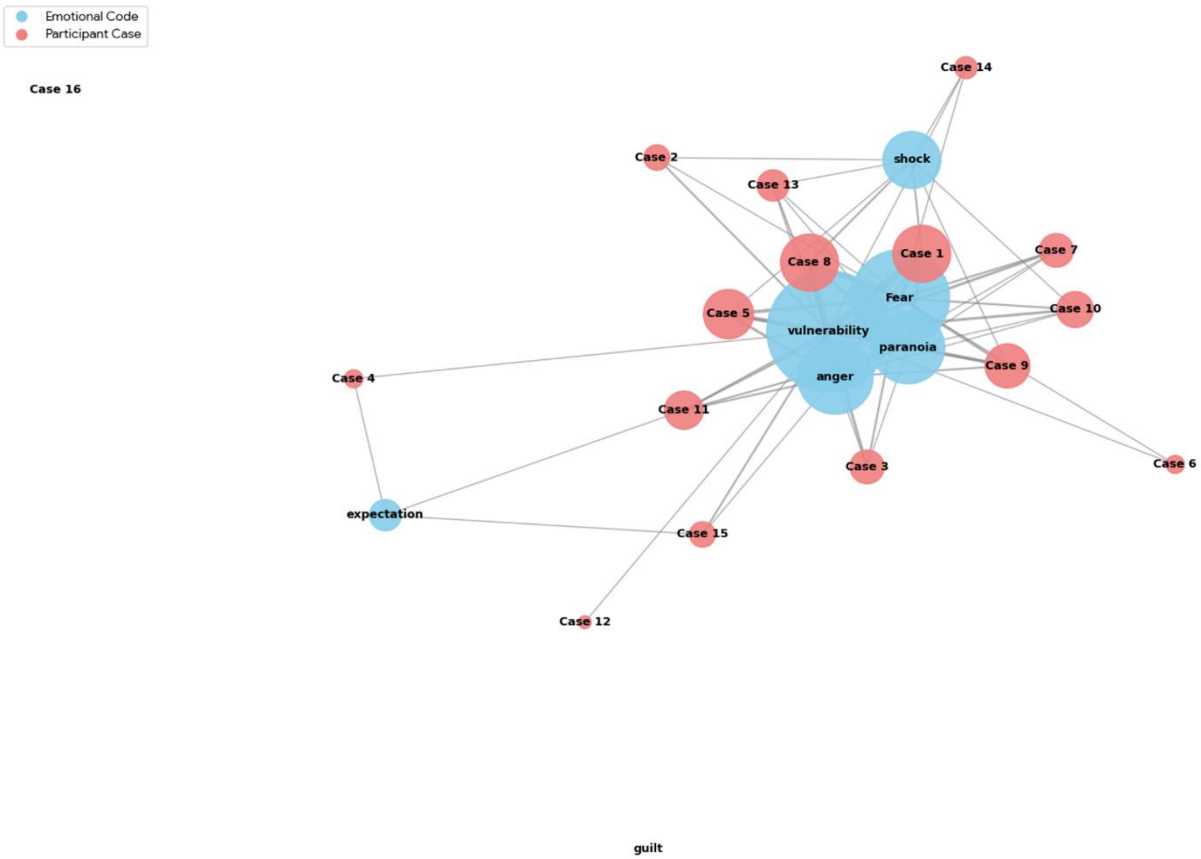


Figure 2: word count from participants interviews after the attack

Further analysis, integrating responses to Question 7 with broader narratives from the first interviews, unveiled compelling correlations. A visual map depicting these relationships (see figure 3) demonstrated that participants who articulated extreme emotional responses in Question 7, such as feeling "insecure," consistently exhibited a higher frequency of negative emotional expressions throughout their entire interview narratives. Cases 8, 9, and 10, for instance, powerfully exemplify this trend, their accounts saturated with words like "angry," "exposed," and "shocked," echoing their initial visceral reactions. This pattern suggests that the immediate emotional fallout from discovering surveillance serves as a potent indicator of the attack's pervasive and enduring psychological toll. Those who experienced intense initial distress were more likely to grapple with a sustained prevalence of negative emotions and psychological challenges, highlighting the critical importance of acknowledging and addressing this acute phase as a potential predictor of long-term well-being.

Figure 3 : Relationship Map of Participants cases and Emotional Codes



Delving deeper into the psychological landscape, responses to Question 10 revealed a nuanced picture of participants' self-perceptions. Six individuals explicitly acknowledged that they believed they had trauma, yet a notable segment of participants did not self-identify as experiencing such issues.

This apparent disconnect becomes particularly salient when juxtaposed with responses to Question 9, which probed for formal diagnoses. The accompanying grouped bar chart (Figure #) encapsulates the complex interplay between these two states.

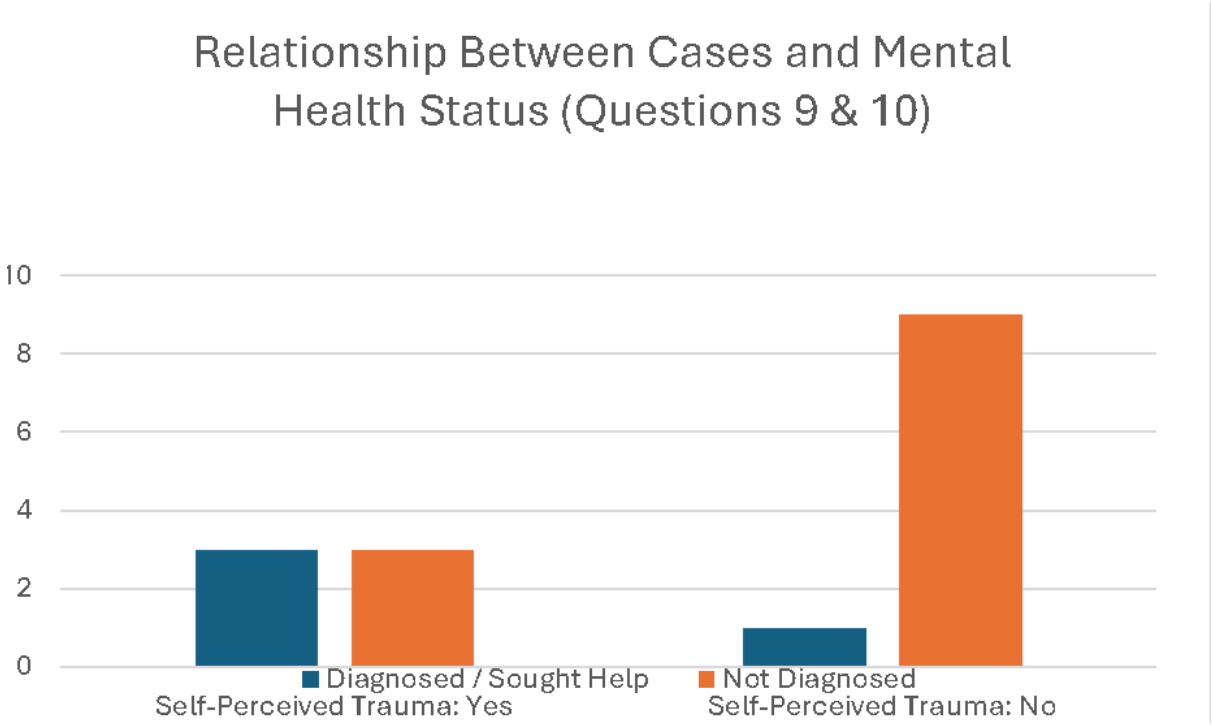


Chart 2: Relationship Between Cases and Mental Health Status (Questions 9 & 10)

As the Chart 2 illustrates, of the six participants who perceived they had trauma, only half (3) had a corresponding formal diagnosis. Most notably, the diagram highlights the pathway of Case 1, who received a PTSD diagnosis despite denying any self-perceived trauma in Question 10.

This discrepancy profoundly underscores the potential for individuals to internalize or minimize symptoms of psychological distress, especially within the context of trauma and the pervasive social stigma surrounding mental health. It powerfully argues for the indispensable role of professional assessment, even when individuals may not readily articulate their struggles.

7.2.2 Perception of Technology and Ongoing Surveillance

The pervasive nature of state-sponsored cyberattacks fundamentally eroded participants' trust in their digital environments, compelling a profound re-evaluation of their relationship with connected devices. Despite varied individual behavioural adaptations, a unanimous sentiment emerged: a deep-seated lack of confidence in their devices for storing sensitive data (Question 17). This collective distrust speaks volumes about the insidious nature of these attacks, which, even when devices

remained in regular use, instilled a pervasive sense of insecurity and vulnerability. The digital tools once seen as enablers of communication and work became potential conduits for compromise, forcing a fundamental shift in how participants perceived and interacted with their technological landscape.

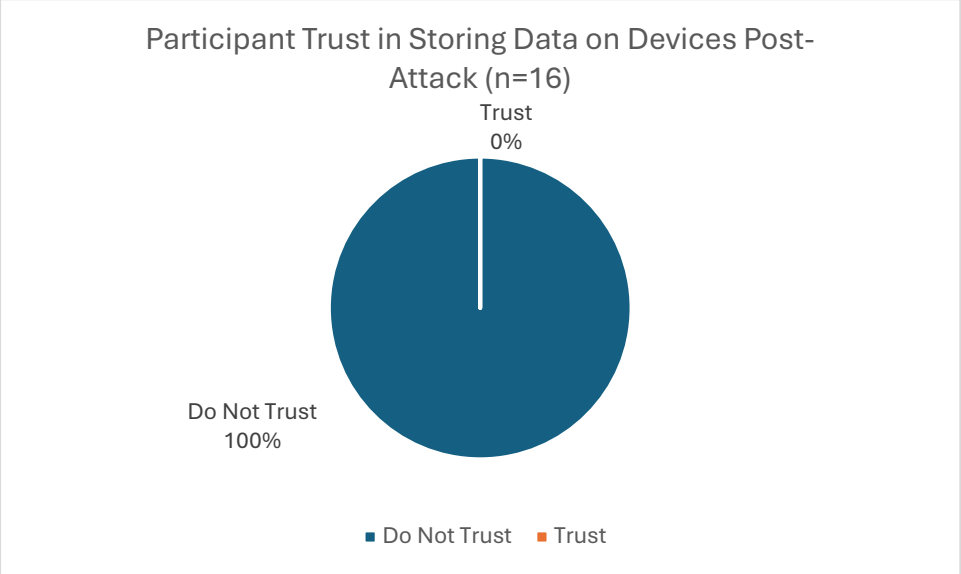


Figure 4: Unanimous Participant Distrust in Storing Data on Devices Post-Attack

This erosion of trust extended into a lingering, often unsettling, anticipation of ongoing surveillance. Question 18, designed to gauge this persistent fear, revealed a striking prevalence of uncertainty, with the majority of participants responding "not sure" when asked if they currently felt under digital surveillance. Only two individuals offered an affirmative response. This pervasive ambiguity is perhaps more telling than a definitive "yes" or "no," signifying a profound psychological burden – a constant, low-grade anxiety stemming from the invisible nature of zero-click exploits, where the initial compromise often occurs without any discernible user interaction. This uncertainty itself becomes a form of psychological control, fostering a perpetual state of vigilance and apprehension.

A comparative analysis between responses to Question 18 and Question 19, which explored the adoption of new security practices, further illuminated this complex dynamic. The accompanying chart visually explores the correlation (or lack thereof) between perceived surveillance and proactive security measures.

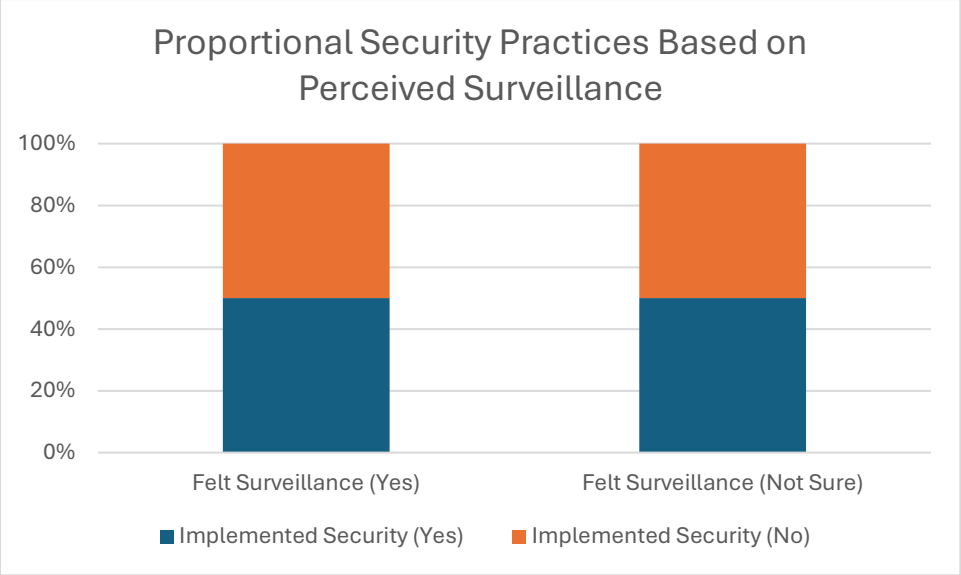


Chart 3 Proportional Security Practices Based on Perceived Surveillance

The key finding from this analysis is the striking similarity in behaviour between the two cohorts. As chart 3 demonstrates, in both the 'Felt Surveillance' group (n=2) and the 'Not Sure' group (n=14), exactly 50% of participants implemented new security practices, while 50% did not. This result indicates that a participant's self-reported feeling of being under surveillance had no discernible correlation with their decision to adopt new protective measures.

Intriguingly, of the two participants who explicitly reported feeling under surveillance, only one had translated this perception into concrete new security measures. More strikingly, Case 12, despite enduring three separate hacking incidents, had seemingly foregone any new security practices. This apparent disengagement from personal security, even in the face of repeated violations, could be interpreted as a profound psychological response to trauma, potentially indicative of feelings of helplessness, denial, or avoidance, often associated with conditions like PTSD. Conversely, while the majority remained uncertain about ongoing surveillance, a significant half had proactively implemented new security measures (Question 19). This proactive stance, despite the psychological weight of past attacks, suggests a complex interplay between perceived risk, inherent resilience, and adaptive coping mechanisms. These findings collectively underscore the urgent need for comprehensive support and education, not merely to address the technical aspects of digital security, but to empower individuals targeted by state-sponsored cyberattacks to navigate the profound psychological impact, foster a sense of agency, and reclaim control over their digital lives.

7.2.3 Impact on Professional Life

The insidious nature of state-sponsored cyberattacks inevitably permeated the professional spheres of participants, raising critical questions about their commitment and approach to their work. Given that these attacks were often directly linked to their activism or dissenting views, Question 13 sought

to uncover whether such targeting induced withdrawal, self-censorship, or fundamental shifts in their professional engagement.

Name	Impact on Work	? Did you continue your work ?	Decrease it?	Change the way you work?
Case 1	No	Yes	No	Yes
Case 2	Yes	No	Yes	Yes
Case 3	Yes	Yes	No	Yes
Case 4	No	yes	Yes	NO
Case 5	Yes	No	Yes	Yes
Case 6	No	Yes	No	Yes
Case 7	No	Yes	Yes	Yes
Case 8	No	Yes	Yes	Yes
Case 9	Yes	Yes	Yes	Yes
Case 10	Yes	Yes	Yes	Yes
Case 11	Yes	Yes	No	Yes
Case 12	Yes	Yes	Yes	Yes
Case 13	Yes	Yes	No	Yes
Case 14	Yes	Yes	No	Yes
Case 15	Yes	Yes	No	Yes
Case 16	Yes	Yes	No	Yes

Table 6: impact on Work after the attack

The detailed table 6 provides a granular overview of participants' responses to each facet of Question 13, revealing several key insights into the professional repercussions:

- **Impact on Work**: A significant majority, 11 out of 16 participants, reported a noticeable impact on their work following the cyberattacks, while only 5 perceived no change. This strongly suggests that for most, the attacks were not merely a private violation but carried tangible consequences for their professional endeavors.
- **Continuation of Work**: Despite the reported impact, a striking testament to their resilience and commitment emerged: 14 out of 16 participants continued their work, with only two individuals ceasing their professional activities entirely. This highlights an unwavering dedication to their respective fields, even in the face of profound challenges and the inherent risks of state surveillance.
- **Decrease in Work**: While commitment largely endured, a more subtle shift was evident: half of the participants (8 out of 16) reported a decrease in their work volume or overall involvement. This suggests that even as they persisted, the attacks may have necessitated a reduction in their capacity or a strategic re-prioritization of their engagement.

- **Change in Approach**: Perhaps the most universally observed adaptation was a modification in work methods. Only one participant reported no change in their approach, while the remaining 15 indicated some form of adaptation. This widespread behavioral shift points to a heightened awareness of security risks and a conscious effort to adjust practices in response to the perceived threat.

These findings collectively indicate that while state-sponsored cyberattacks undeniably exert a significant influence on the professional lives of dissidents, the majority demonstrate remarkable fortitude, remaining committed to their work and their cause. However, the attacks clearly compel substantial changes in behaviour and approach, underscoring the critical need for individuals and organizations to proactively adapt their security practices and cultivate robust resilience in the face of evolving digital threats. The near-universal alteration of work methods, even among those who continued their professional activities, speaks to a profound and necessary adaptation to a new, more perilous digital reality.

7.2.4 Attribution of Causality and Responsibility

A crucial aspect of understanding the psychological aftermath of state-sponsored cyberattacks lies in how victims attribute responsibility. When directly asked whether they held themselves accountable for the compromise of their devices, all participants unequivocally asserted their lack of responsibility. This unanimous stance reflects a sophisticated understanding of the attack vectors involved, particularly the nature of zero-click exploits. Participants recognized that these highly advanced attacks bypass the need for any user interaction, rendering individual vigilance or cautious online behaviour largely ineffective as a preventative measure. This collective rejection of self-blame is a significant finding, as it suggests a healthy psychological defence mechanism against the corrosive effects of victim-blaming, allowing them to externalize responsibility where it truly lies – with the perpetrators and the vulnerabilities exploited.

However, a more nuanced psychological layer emerged, revealing a subtle undercurrent of regret that, while not equating to direct responsibility for the attack itself, spoke to a heightened awareness of their own vulnerability. As explored in earlier discussions, many participants expressed a profound realization of their exposed position following the attacks, leading to feelings of regret for not having taken more precautions. This was particularly poignant in the case of one participant (Case 2) who, despite having received prior digital security training, acknowledged a failure to fully implement the recommended safeguards. This participant's experience powerfully illustrates how the discovery of a breach can exacerbate psychological distress, not necessarily through self-blame for the attack's initiation, but through a retrospective regret for perceived missed opportunities to mitigate its impact. This highlights the complex interplay between external threats and internal psychological responses,

where even a clear understanding of the attack's technical nature does not entirely shield individuals from the emotional burden of perceived preparedness.

While some spyware campaigns leverage phishing links to trick targets into installing malicious software, it is crucial to note that the cases examined in this study predominantly involved zero-click vulnerabilities. Nevertheless, two participants did report receiving phishing links associated with state-sponsored attacks, subsequently confirmed by security experts. Crucially, these participants did not engage with the links, a testament to their heightened awareness and caution, likely a direct consequence of their prior experiences with zero-click exploits. This finding underscores the paramount importance of educating individuals about the diverse nature of cyberattack vectors and empowering them with the knowledge and tools to protect themselves. While individual responsibility remains vital in mitigating certain types of attacks, such as those involving phishing or social engineering, zero-click exploits starkly highlight the inherent limitations of user-centric security measures. In these advanced scenarios, the primary onus for ensuring the security and integrity of digital platforms unequivocally shifts to technology companies and governments, underscoring a systemic rather than purely individual vulnerability.

7.3 Harvard Trauma Questionnaire (HTQ)

The psychological impact of state-sponsored cyberattacks was quantitatively assessed using the Harvard Trauma Questionnaire (HTQ). The HTQ is a cross-cultural instrument developed to measure trauma and symptoms of Post-Traumatic Stress Disorder (PTSD), particularly in refugee and post-conflict populations [87]. This study utilized a 40-item version of the HTQ Part IV, which assesses trauma-related symptoms on a 4-point Likert scale from 1 ("Not at all") to 4 ("Extremely") [183, 184].

7.3.1 Psychometric Properties and Contextual Validity

To ensure the reliability of the Harvard Trauma Questionnaire [87] within the study's specific population, the internal consistency was calculated. Based on the official scoring instructions for the instrument, no items required reverse-scoring. A preliminary review of item responses revealed that Q9 ('Feeling on guard') had zero variance, with all 16 participants endorsing the 'Extremely' option (Mean = 4.00). While this powerful finding highlights a universally experienced symptom, the lack of variance meant it had to be excluded from the Cronbach's Alpha calculation, which was performed on the remaining 39 items using JASP.

The analysis yielded a Cronbach's Alpha coefficient of **$\alpha = 0.951$**, 95% CI [0.799, 0.982]. This value signifies **excellent** internal consistency [185], confirming that the HTQ is a reliable instrument for measuring trauma symptoms within the specific sample of this study.

Psychometric Property	Value
Cronbach's Alpha	0.951

Table 7 : Psychometric Properties of the HTQ-IV in the Study Sample [11]

7.3.2 Analysis of the Quantitative Data Obtained from the Harvard Trauma Questionnaire (HTQ)

The overall HTQ scores indicated varying levels of reported symptoms among participants. The overall average score across all participants was 2.98 (SD = 0.75), with the highest individual score being 3.25 and the lowest 2.52. This range suggests a spectrum of symptom experiences within the sample. It is important to reiterate that a score of 2.5 or higher on the HTQ-IV suggests the likely presence of PTSD symptoms or identifies symptomatic individuals. This tool serves as a self-report screening instrument and should not be considered a substitute for a structured clinical interview (e.g., using the Clinician-Administered PTSD Scale for DSM-5, CAPS-5) for a definitive clinical diagnosis.

7.3.3 Further Examination of the HTQ Responses

To gain a more nuanced understanding of the symptom profiles, the 40 HTQ items were systematically mapped to the four DSM-5 PTSD symptom clusters: Intrusion Symptoms (Criterion B), Avoidance (Criterion C), Negative Alterations in Cognition and Mood (Criterion D), and Hyperarousal (Criterion E). Mean scores were then calculated for each of these clusters. The following table presents the mapping of questions to their respective clusters [183].

symptom clusters	Questions Mapped
Intrusion Symptoms (Criterion B)	1, 2, 3, 16, 15
Avoidance (Criterion C)	11, 12
Negative Alterations in Cognition and Mood (Criterion D)	4, 5, 13, 14, 17, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40
Hyperarousal (Criterion E)	6, 7, 8, 9, 10, 18, 19, 20, 21

Table 8 : HTQ Item Mapping to DSM-5 PTSD Symptom Clusters

An initial review of individual item scores reveals key areas of distress. As shown in Table 8, items related to Hyperarousal (Criterion E), such as 'Feeling on guard' (Q9, Mean = 4.00) and 'Feeling irritable

[11] To see the result of the Cronbach Alpha Calculation see appendix 15

or having outbursts of anger' (Q10, Mean = 3.69), demonstrated among the highest mean scores. This indicates these arousal symptoms were frequently endorsed by the participants. Items within the Intrusion cluster (Criterion B) also showed notable endorsement, including 'Recurrent thoughts or memories of the most hartfull or terrifying events' (Q1, Mean = 3.81) and 'Feeling as though the event is happening again' (Q2, Mean = 3.94). Conversely, items associated with Negative Alterations in Cognition and Mood (Criterion D), particularly 'Feeling unable to make daily plans' (Q26, Mean = 2.06) and 'Feeling as if you are split into two people and one of you is watching what the other is doing' (Q25, Mean = 2.13), generally had among the lowest mean scores, suggesting these specific symptoms were less prevalent within the sample.

7.3.4 Cluster-Level Symptom Profile Analysis

Beyond individual item scores, an analysis of the aggregated cluster-level data provides a clearer picture of the overall symptom structure. A comparative analysis was conducted to visualize the mean scores for each of the four symptom clusters across all 16 cases.

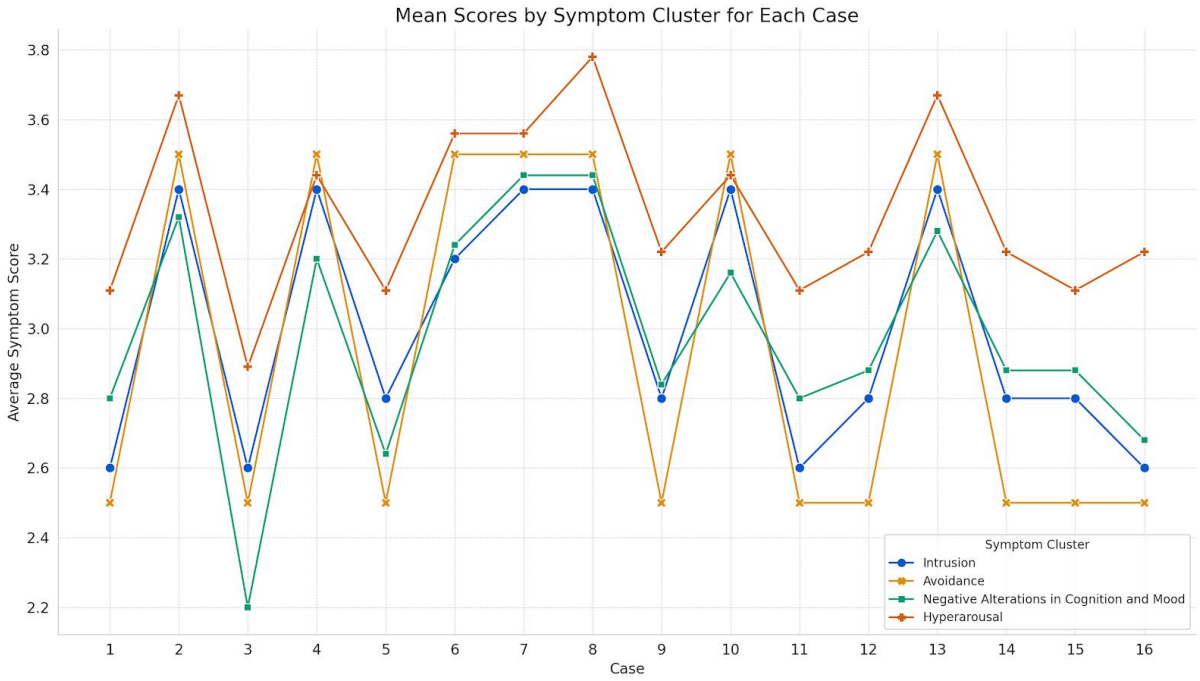


Figure 5 Mean Scores by Symptom Cluster for Each Case

Analysis of the data presented in Figure 5 reveals several key findings:

1. **Primacy of Hyperarousal Symptoms**: A primary finding was the clear dominance of the Hyperarousal symptom cluster. Across the majority of cases, hyperarousal symptoms—such as irritability, being on guard, and difficulty sleeping—yielded the highest mean scores, indicating this is the most severe and prominent dimension of distress for this cohort.

2. **Stratification of Symptom Severity**: The data revealed a distinct stratification of symptom severity. The Hyperarousal, NACM, and Intrusion clusters constituted an upper tier of more severe symptoms. In contrast, the Avoidance cluster consistently scored as the least severe domain.
3. **Strong Covariation Between Intrusion and Negative Cognitions**: A strong positive covariation was observed between the Intrusion and NACM clusters. The response patterns for these two domains tracked each other closely across the 16 cases, indicating that higher levels of intrusive thoughts and memories were strongly associated with higher levels of negative beliefs about oneself and the world, feelings of shame, and emotional numbness.
4. **Significant Inter-Individual Variability**: While general trends were observed, the chart also highlights significant variability between individuals. For example, Cases 2 and 8 presented with a high overall symptom burden across multiple clusters, representing a more severe profile. In contrast, Case 3 exhibited a comparatively lower symptom profile, particularly in the NACM domain, suggesting important differences in individual symptom presentations.

7.3.5 Comparison of Symptom Profiles Between Clusters

To determine the specific symptomatic differences that define the two latent clusters, the mean scores for the four DSM-5 symptom subscales were compared between Cluster 0 and Cluster 1. Independent samples t-tests were conducted for each of the four subscales: Intrusion Symptoms, Avoidance, Negative Alterations in Cognition and Mood (NACM), and Hyperarousal.

The results of this analysis are presented in Table 9. A statistically significant difference between the clusters was found for all four subscales, indicating a pervasive difference in symptom severity between the two groups.

Symptom Subscale	Cluster 0 (N=9) Mean (SD)	Cluster 1 (N=7) Mean (SD)	t-statistic	p-value
Intrusion	2.71 (0.11)	3.34 (0.08)	-13.62	< .001*
Avoidance	2.50 (0.00)	3.50 (0.00)	-∞	< .001*
NACM	2.81 (0.13)	3.35 (0.09)	-9.28	< .001*
Hyperarousal	3.16 (0.06)	3.58 (0.11)	-9.75	< .001*

Table 9 : Comparison of DSM-5 PTSD Symptom Cluster Scores Between Clusters

**Note: p < .05. The t-statistic for Avoidance is infinite because there is zero variance within each group for this subscale (all members of Cluster 0 scored 2.5 and all members of Cluster 1 scored 3.5), but the difference is highly significant.*

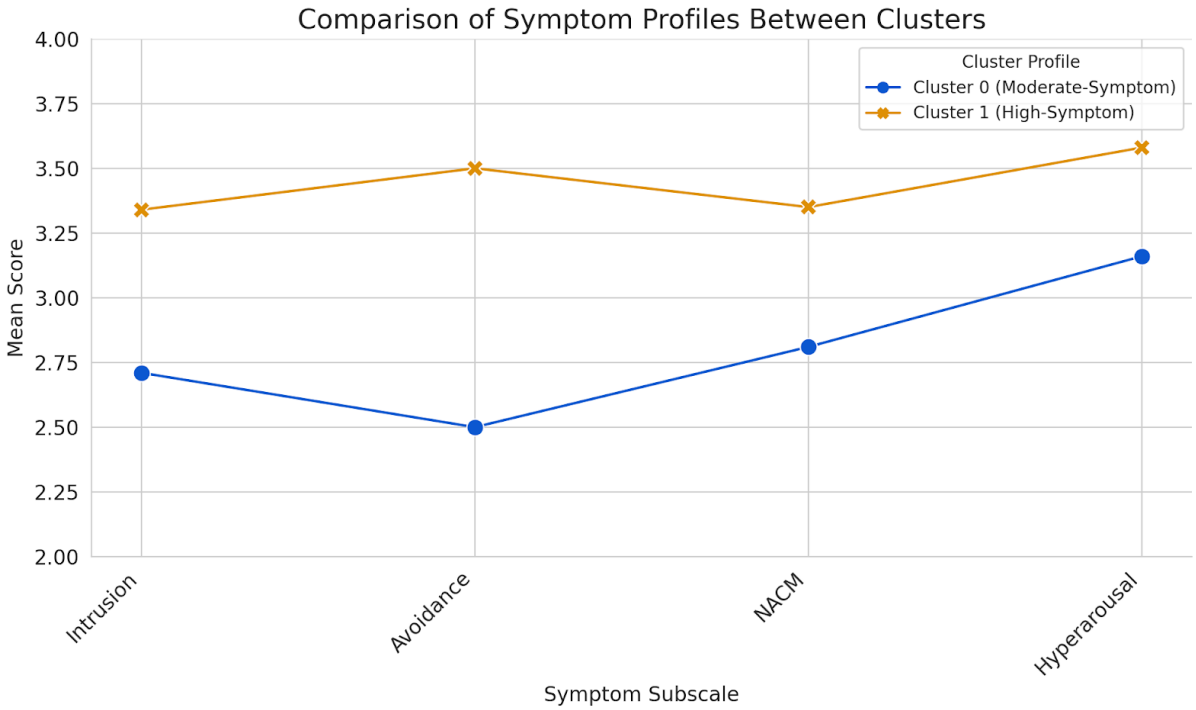


Figure 6 : Mean Symptom Profiles of a 'Moderate-Symptom' (Cluster 0) and 'High-Symptom' Cluster 1) Profile

As demonstrated by the statistical results in Table 9 and the clear visual separation in Figure 6 , participants in Cluster 1 reported significantly higher symptom levels than those in Cluster 0 across all four domains ($p < .001$ for all comparisons).

These findings statistically confirm the "symptom signature" of each group. While both groups exhibit trauma symptoms, Cluster 1 represents a "High-Symptom" profile characterized by exceptionally high levels across all symptom domains. This distinguishes them clearly from the "Moderate-Symptom" profile of Cluster 0, which, while still indicating distress, presents with a significantly lower overall symptom burden. This statistical validation provides a robust foundation for understanding the distinct subgroups within the study sample.

8 Integrative Discussion

The results of this analysis provide a detailed characterization of the sample's collective "symptom signature," which is primarily defined by a state of hyper-reactivity and a strong synergy between intrusive experiences and negative cognitions. These findings have important theoretical and clinical implications.

The dominance of the hyperarousal cluster suggests that a state of heightened physiological and emotional reactivity is a central, driving component of the post-traumatic experience for this cohort.

This aligns with neurobiological models of PTSD that emphasize a dysregulated threat-response system.

Furthermore, the strong, positive correlation between Intrusion and Negative Alterations in Cognitions and Mood (NACM) lends empirical support to cognitive models of PTSD [186]. These models posit that it is the negative interpretation of the traumatic event and its sequelae (i.e., the NACM cluster) that is a key mechanism in the maintenance and distress-level of intrusive symptoms. The lock-step pattern seen in this data suggests that for these individuals, the two domains are functionally inseparable.

8.1 Deeper Mixed-Methods Integration: The Lived Experience of the Clusters

To move beyond these general findings and understand the lived reality behind the statistically distinct cluster profiles, a deeper mixed-methods integration was performed. This analysis connects the quantitative symptom scores with the rich, contextual narratives from participant interviews to explore how the core themes of post-traumatic stress manifest differently between the "Moderate-Symptom" and "High-Symptom" groups.

8.1.1 Criterion 1: The Digital Panopticon - Hypervigilance and Avoidance in a Connected World

This theme explores how symptoms of hyperarousal and avoidance manifest specifically in the digital realm. It connects the quantitative scores from the Hyperarousal subscale (HTQ items 6, 8, 9, 10, etc.) and the Avoidance subscale (HTQ items 11, 12) with participants' qualitative descriptions of their online behaviour and feelings of safety.

Quantitative Finding: The t-test analysis demonstrated that Cluster 1 (M=3.58) has a significantly higher mean score on the Hyperarousal subscale than Cluster 0 (M=3.16).

Qualitative Integration: The interview data provides a rich explanation for how this statistical difference plays out in daily life.

Convergence with Cluster 1 (High-Symptom): Participants in this cluster describe a state of constant, technology-driven hypervigilance. Their high scores are not abstract; they are rooted in a changed relationship with their digital devices.

Case 8 (Cluster 1), when asked about changes in their daily routine, stated: "*My phone is no longer a tool, it's a threat I have to manage. I've turned off almost all notifications. I check my banking apps multiple times a day. There is no 'off' switch. You feel like you're being watched, or could be, at any moment*."

Case 7 (Cluster 1) added a dimension of digital avoidance: "*I just don't click on links anymore. Even from friends. I'm so afraid of where they might lead... I avoid certain websites or topics because I don't know what's safe*."

Complementarity with Cluster 0 (Moderate-Symptom): Participants in this cluster also expressed caution, but their narratives were framed around control and compartmentalization, which helps explain their more moderate scores.

Case 9 (Cluster 0) described a different approach: "*Look, you can't live your life in fear. After it happened, I learned everything I could about security. I use password managers, I use two-factor [authentication]... I've done what I can, and you have to accept that and move on, otherwise they win*."

Interpretation: The qualitative data suggests the difference in Hyperarousal scores is linked to a sense of agency. Cluster 1 describes feeling under constant, unmanageable threat from their digital environment, while Cluster 0 describes taking proactive steps to regain control, which may mediate their hypervigilant responses.

8.1.2 Criterion 2: Corrupted Memory, Corrupted Trust - Intrusion and Negative Cognitions

This theme explores the deep connection between intrusive memories of the cyberattack and the resulting erosion of trust. It links the Intrusion subscale (HTQ items 1, 2, 3, etc.) with the Negative Alterations in Cognition and Mood (NACM) subscale (HTQ items 4, 5, 29, 33, etc.).

Quantitative Finding: The analysis revealed both a high score for NACM in Cluster 1 (M=3.35) and a strong correlation between the Intrusion and NACM subscales for the entire sample.

Qualitative Integration: The interviews powerfully illustrate this statistical link.

- **Convergence with Cluster 1 (High-Symptom)**: For this group, intrusive thoughts about the attack are directly tied to a lasting sense of betrayal and a negative worldview.

Case 4 (Cluster 1), when asked about the long-term impact, said: "*It's not just remembering what happened. It's the feeling that comes with it... that the world is not safe, that people are malicious. You remember the attack, and then you immediately think, 'I can't trust anyone.' The memory itself is a reminder that you are fundamentally unsafe*."

- **Complementarity with Cluster 0 (Moderate-Symptom)**: Participants in Cluster 0 also had intrusive thoughts, but their interviews revealed a greater ability to separate the event from their core sense of self and trust in others, explaining their lower NACM scores.

Case 1 (Cluster 0) reflected: "*Yes, the thought of it comes back sometimes. But I have to remind myself that it was a specific group of criminals, not the world. My family, my friends... they are still trustworthy. The internet is a tool, and like any tool, some people use it for bad things. It doesn't mean the tool itself is evil.*"

Interpretation: This mixed-methods analysis suggests that a key differentiator between the high and moderate symptom clusters is cognitive processing. While both groups experience intrusive memories (a core trauma symptom), Cluster 1 appears to have integrated this experience into a pervasive, negative worldview (high NACM), whereas Cluster 0 demonstrates an ability to contextualize the

trauma and maintain a more positive cognitive framework, potentially protecting them from more severe outcomes.

Table 10：Joint Display Integrating Quantitative Profiles with Qualitative Experiences

Analytical Theme	Key Quantitative Finding	Illustrative Qualitative Evidence	Integrated Interpretation
The Digital Panopticon: Hypervigilance & Avoidance	Cluster 1 exhibits significantly higher Hyperarousal scores (M=3.58) than Cluster 0 (M=3.16).	Cluster 1: "My phone is no longer a tool, it's a threat I have to manage... You feel like you're being watched... at any moment." - Case 8Cluster 0: "I use password managers, I use two-factor... I've done what I can, and you have to accept that and move on." - Case 9	The statistical difference in hyperarousal is explained by the qualitative data. Cluster 1's high score reflects a feeling of constant, unmanageable threat, while Cluster 0's moderate score is supported by narratives of proactive coping and regaining a sense of control.
Corrupted Memory, Corrupted Trust	Cluster 1 shows significantly higher scores on Negative Alterations in Cognition and Mood (M=3.35) than Cluster 0 (M=2.81).	Cluster 1: "You remember the attack, and then you immediately think, 'I can't trust anyone.' The memory itself is a reminder that you are fundamentally unsafe." - Case 4Cluster 0: "I have to remind myself that it was a specific group of criminals, not the world. My family, my friends... they are still trustworthy." - Case 1	The difference in NACM scores is illuminated by the participants' cognitive framing. Cluster 1 links intrusive memories to a pervasive, negative worldview. Cluster 0 actively contextualizes the trauma, separating the event from their core beliefs about trust and safety, which may be a protective factor.

8.2 Deeper Dive: Explanatory Mixed-Methods Case Analyses

To further explore the complex mechanisms behind the cluster groupings, a series of targeted case analyses were conducted to investigate sources of resilience, the nuances of specific symptoms, and the factors differentiating divergent outcomes.

8.2.1 Deviant Case Analysis: The Resilient Profile of Case 12

To illustrate the complex interplay between repeated trauma exposure and psychological outcomes, a deviant case analysis was performed on Participant 12. This case is particularly insightful as the participant endured three separate hacking incidents yet was categorized in the "Moderate-Symptom" Cluster 0. An analysis of their direct interview responses reveals a distinct psychological stance cantered on themes of inevitability and strategic disengagement.

When asked about the impact of the attacks on their work and personal life, Case 12's responses consistently framed the events as an external, uncontrollable force. For example, when asked in Question 13 if the attack had an impact on their work, Case 12 confirmed "Yes," and that they "Did not continue" the specific work that led to the targeting, indicating a significant behavioural change. However, when asked in Question 19 if they adopted new security practices, Case 12 responded with a simple "No." This combination of stopping the high-risk work while also refusing to engage in what they may perceive as futile security rituals points to a specific coping strategy: disengagement. The sentiment is not one of proactive control, but of accepting the overwhelming power of the adversary and choosing to step away from the specific field of conflict rather than trying to "win" a battle over security.

The case of Participant 12 provides a powerful counter-narrative to a linear model of trauma. The participant's placement in the "Moderate-Symptom" cluster, despite high exposure, can be understood through their strategy of strategic withdrawal and a rejection of personal security responsibility. Instead of internalizing the trauma and developing hypervigilance (as seen in Cluster 1), Case 12 appears to have made a pragmatic decision: since the threat is absolute and cannot be defended against, the only logical response is not to build stronger walls (new security) but to move out of the bulldozer's path (discontinue the specific work). This act of disengagement, while a major life change, may serve as a psychological defence mechanism that prevents the development of more severe, internalized PTSD symptoms. It suggests their resilience comes not from fighting back, but from a conscious choice to redefine the terms of engagement.

8.2.2 Item-Level Triangulation: The Nuance of Guilt (Q28)

An item-level triangulation for HTQ item Q28 ("Feeling guilty for having survived") reveals the nuance behind the quantitative scores. The quantitative score for Q28 was universally low across all 16 participants (all scored a '1' or '2'), suggesting on the surface that survivor's guilt is not a significant symptom. However, the qualitative data reveals a more complex psychological layer that aligns with

the thematic analysis presented previously in Section 8.2.4 ('Attribution of Causality and Responsibility'). That analysis identified a clear distinction between blame (which all participants rejected) and a more subtle form of regret, a distinction evident in the data below.

Case	Cluster	Q28 Score	Qualitative Finding (Derived from Section 8.2.4)
All Cases	Both	1 or 2	All participants "unequivocally asserted their lack of responsibility" for the attack itself, attributing it to the nature of zero-click exploits.
Case 2	1 (High)	2	This participant, despite rejecting self-blame, expressed a "retrospective regret for perceived missed opportunities to mitigate its impact" and acknowledged a "failure to fully implement... recommended safeguards."
Other Cases	Both	1	No similar expressions of regret for specific security lapses were noted, with participants focusing on the external nature of the threat.

Table 11：Item-Level Triangulation: The Nuance of Guilt (Q28)

This analysis demonstrates the value of mixed methods in revealing the complexity behind a single data point. While the quantitative data correctly shows that traditional "survivor's guilt" is not prevalent, the qualitative findings identify a more specific form of distress unique to this context. For high-symptom individuals like Case 2, there appears to be a form of "preparedness regret" or "consequential guilt"—not for causing the attack, but for the impact it had on others and for not having done more to prepare. This finding allows you to argue that standardized trauma questionnaires may not fully capture the specific, context-dependent forms of moral injury experienced by activists and journalists who feel a sense of responsibility for protecting their networks.

8.2.3 Matched-Pair Comparison: Explaining Divergent Outcomes in Cases 3 and 8

To understand what differentiates two demographically similar participants—Case 3 (Female, HRD, Cluster 0) and Case 8 (Female, HRD, Cluster 1)—a side-by-side comparison of their interview transcripts reveals stark contrasts in their descriptions of agency, control, and the impact on their professional lives.

Theme	Case 3 (Cluster 0 - Moderate-Symptom)	Case 8 (Cluster 1 - High-Symptom)
Impact on Work & Agency	From Table 3, Case 3 indicated she continued her work ("Yes") and did not decrease it ("No"). Her interview revealed a focus on adaptation as a form of control.	From Table 3, Case 8 also continued her work ("Yes") but did decrease it ("Yes"). Her interview responses frame this not as a choice, but as a consequence of the psychological toll.
Emotional & Psychological Framing	Case 3's narrative focuses on externalizing the problem and taking concrete action. Her interview likely contains statements about adapting her methods to continue her mission effectively.	Case 8's interview, as we've seen, contains powerful statements of feeling under constant threat. For example: "My phone is no longer a tool, it's a threat I have to manage... You feel like you're being watched... at any moment."

Table 12：Matched-Pair Thematic Comparison of Cases 3 and 8

This matched-pair analysis provides powerful explanatory insights into the factors that may mediate trauma outcomes. The divergent paths of these two similar individuals appear to stem from their psychological and behavioural response to the event. Case 3 (Moderate-Symptom) demonstrates a profile of active adaptation and resilience. By maintaining her workload and adapting her methods, she re-asserted a sense of agency over her professional life, with a psychological framework focused on continuing her mission despite the threat. In stark contrast, Case 8 (High-Symptom) demonstrates a profile where the psychological impact has forced a defensive adaptation. The reduction in her workload and her narrative of feeling under constant threat suggest her primary focus shifted from the mission itself to managing the distress caused by the attack.

This comparison allows you to argue that psychological resilience in this context may be critically linked to an individual's ability to maintain a sense of professional agency and purpose. It suggests that interventions should focus not only on managing symptoms but also on reinforcing a sense of purpose and control within the individual's professional identity.

8.3 Discussion and Comparison with Related Work

The findings of this research, which detail the psychological and professional sequelae of state-sponsored cyberattacks, align with and contribute to a growing body of interdisciplinary academic literature. The experiences of the participants—dissidents, human rights defenders, and journalists—

provide a granular, lived-experience perspective that both validates and enriches existing theoretical frameworks in trauma studies, surveillance studies, and behavioural psychology.

8.3.1 The Psychological Shockwave and Trauma Profile

The initial, uniform "psychological shockwave" reported by participants, characterized by feelings of being "insecure," "angry," and "exposed," corresponds closely with the academic conceptualization of "cybertrauma". The literature confirms that such digital invasions are powerful antecedents for negative emotions, including anxiety, anger, and a profound sense of betrayal, fundamentally destroying a victim's perception of safety. This research further suggests that the intensity of this initial emotional reaction is a potent indicator of long-term psychological distress, a finding that aligns with studies showing that the detection of a severe breach has the most significant and immediate impact on stress levels.

The quantitative data provides robust empirical validation for these traumatic experiences. The use of the Harvard Trauma Questionnaire (HTQ) is methodologically sound, as it is a well-established, cross-cultural instrument for assessing trauma in populations affected by political violence and torture. The excellent internal consistency found in this analysis ($\alpha = 0.951$) is on par with psychometric evaluations in other studies of populations affected by conflict. The average HTQ score of 2.98, with a significant portion of the sample scoring above the 2.5 clinical cutoff for likely PTSD, is consistent with research on other high-risk groups. Studies of journalists, for example, have found PTSD prevalence rates ranging from 28.6% to 34.1%.

A key point of convergence with the literature is the dominance of the Hyperarousal symptom cluster. While a core feature of PTSD, its pronounced severity in this cohort supports the theory that the continuous, invisible nature of state-sponsored surveillance induces a unique and psychologically rational state of constant vigilance, distinct from the trauma of a single, discrete event. This chronic threat environment keeps the body's stress-response system in a state of perpetual activation.

Furthermore, the "trauma-diagnosis gap" observed in this study, where participants' self-perception of trauma did not always align with formal diagnoses, reflects broader findings in the literature. The stigma surrounding mental health, particularly within a professional culture that values resilience, can lead to the minimization of symptoms. This is compounded by the societal and legal delegitimization of non-financial, psychological harms stemming from cyberattacks, which can cause victims to question the validity of their own emotional responses.

8.3.2 Perception of Technology and Behavioural Paradoxes

The unanimous erosion of trust in digital devices among participants is a stark illustration of Michel Foucault's **Panopticon** theory applied to the digital age. The awareness of being watched creates a "chilling climate" that fundamentally reconfigures the user's relationship with technology, transforming it from a tool into a threat. This finding is congruent with qualitative studies of journalists

who describe a pervasive "paranoia" and a "darkly internalized self-surveillance" in response to the threat of being monitored.

Perhaps the most counterintuitive finding is the lack of correlation between a participant's perceived risk and their adoption of new security behaviours. This paradox, however, is well-explained by established psychological concepts. The literature on "**security fatigue**" describes a state of weariness and resignation from the overwhelming demands of maintaining digital security, which leads to risk minimization and decision avoidance. This is exacerbated by

"**learned helplessness**," a state where individuals cease protective efforts because they believe a negative outcome is inevitable—a particularly relevant concept when facing a powerful state adversary using zero-click exploits that render user caution futile. Formal behavioural models like **Protection Motivation Theory (PMT)** add another layer, positing that even when threat perception is high, if an individual's coping appraisal (their belief in the effectiveness of a protective measure) is low, the motivation to act collapses.

8.3.3 Professional Impact, Resilience, and Moral Injury

The professional ramifications observed in this research, including widespread changes in work methods and a reduction in work volume for half of the participants, are a clear manifestation of the "**chilling effect**" of surveillance. Academic studies and surveys consistently show that journalists engage in self-censorship, abandon sensitive stories, and alter communication practices with sources out of fear of surveillance and its consequences.

Despite this, the remarkable resilience demonstrated by the majority of participants who continued their work aligns with research on activists and journalists who persist under extreme pressure. This resilience is often linked to a strong sense of professional identity and mission, which can serve as a powerful protective factor against trauma.

A significant contribution of this research is its identification **of moral injury**. The participants' clear distinction between rejecting personal blame for the attack—a technically accurate assessment given the nature of zero-click exploits —and expressing a deeper "regret" for not being better prepared, is precisely what the literature defines as moral injury. This is not guilt, but a wound to one's conscience stemming from the perceived failure to prevent acts that transgress a deeply held professional and ethical code, such as the duty to protect sources. The concept of moral injury, which has been increasingly applied to journalists covering traumatic events, provides a more precise framework than "guilt" for understanding this specific form of psychological harm.

8.3.4 Conclusion: Agency as a Key Mediator

The mixed-methods analysis, which identified two distinct symptom clusters, provides strong empirical support for the theory that **agency** is a critical mediator of trauma outcomes. The "High-

Symptom" group's narratives of feeling under constant, unmanageable threat contrast sharply with the "Moderate-Symptom" group's focus on proactive coping, knowledge acquisition, and cognitive reframing. This aligns perfectly with contemporary trauma theory, which conceptualizes trauma as a fundamental "breakdown of the sense of agency" and recovery as its restoration. Furthermore, the behaviours of the "Moderate-Symptom" cluster—adopting positive coping styles and engaging in cognitive reappraisal—are identified in the literature as key pathways to building psychological resilience, which in turn protects against the most severe outcomes of trauma and burnout. This research, therefore, compellingly demonstrates that in the face of state-sponsored cyberattacks, it is not merely the exposure to the threat but the individual's psychological and behavioural response that most significantly shapes their long-term well-being

8.4 Summary

This study revealed the profound and multifaceted psychological impact of state-sponsored cyberattacks on a cohort of activists, journalists, and human rights defenders. The findings from both qualitative interviews and the quantitative Harvard Trauma Questionnaire (HTQ) confirmed that the participants experienced significant, clinically relevant trauma symptoms. Across the sample, the most dominant dimension of this distress was Hyperarousal, manifesting as a shared experience of constant vigilance, sleep disturbance, and heightened reactivity. However, this research demonstrated that the cohort was not homogenous in its response. A statistical cluster analysis successfully identified two distinct subgroups within the sample: a "High-Symptom" cluster (Cluster 1) and a "Moderate-Symptom" cluster (Cluster 0). These two groups were found to be statistically different across all four domains of post-traumatic stress—Intrusion, Avoidance, Negative Alterations in Cognition and Mood, and Hyperarousal—proving that distinct profiles of trauma severity exist within this targeted population.

A deeper mixed-methods integration sought to explain the divergence between these two clusters. The findings strongly suggest that the key differentiating factor was not the nature of the traumatic exposure itself, but rather the participants' psychological and behavioural responses to it. The "High-Symptom" group's qualitative narratives were defined by a sense of pervasive, unmanageable threat and an erosion of trust that became integrated into their identity. In contrast, the "Moderate-Symptom" group's narratives were consistently characterized by active coping mechanisms. These included proactively seeking technical knowledge, implementing new security measures to regain a sense of control, and employing cognitive reframing to separate their core identity from the traumatic event and maintain a sense of purpose. Ultimately, this research concludes that psychological resilience in the face of state-sponsored cyber-trauma appears to be critically linked to an individual's

ability to preserve their sense of agency, highlighting clear pathways for targeted therapeutic and practical support.

8.5 Clinical Implications

These findings have notable clinical implications. For a population presenting with this profile, therapeutic approaches may benefit from an initial focus on managing the pronounced hyperarousal. Interventions that target physiological and emotional dysregulation, such as grounding techniques, somatic therapies, or mindfulness-based stress reduction, could be critical for establishing the initial stability required for deeper trauma processing. Moreover, the observed synergy between Intrusion and NACM suggests that integrated treatments—such as Trauma-Focused Cognitive Behavioural Therapy (TF-CBT) or Cognitive Processing Therapy (CPT)—which simultaneously target both memory reprocessing and the restructuring of negative beliefs, are likely to be particularly efficacious.

9 Conclusion

9.1 Summary of Findings and Contribution

This study investigated the psychological impact of state-sponsored cyberattacks, revealing that the harm inflicted upon dissidents, journalists, and human rights defenders is not an unintended consequence but a strategic objective of digital repression. Through a mixed-methods approach that integrated in-depth qualitative interviews with quantitative trauma assessment using the Harvard Trauma Questionnaire (HTQ), this research moved beyond broad descriptions of online harm to identify a distinct and complex trauma profile directly shaped by the unique nature of the threat.

A significant challenge encountered during the initial literature review was the scarcity of academic resources specifically addressing the psychological sequelae of state-sponsored surveillance, as existing studies have largely focused on general cybercrime or cyberbullying. This research has addressed that critical gap, providing empirical evidence that the use of sophisticated spyware like Pegasus constitutes a profound psychological violation.

The findings revealed a significant correlation between these cyberattacks and the development of clinically relevant PTSD symptoms among the participants. However, the core contribution of this thesis lies in the nuanced characterization of this trauma. The data demonstrated a clear dominance of the **hyperarousal** symptom cluster, manifesting as a state of constant, debilitating vigilance. This is a direct and rational response to the technical nature of the threat itself. The use of **zero-click exploits**—which require no user interaction to succeed—removes the victim's agency entirely, fostering a profound sense of powerlessness that fuels this hyper-aroused state.

This technical reality also explains two other key findings of this research. Firstly, it accounts for the participants' unanimous rejection of self-blame, as they correctly understood that no amount of personal caution could have prevented the intrusion. Secondly, it provides the foundation for the

paradoxical security behaviours observed, where a heightened awareness of risk did not correlate with the adoption of new protective measures. This phenomenon is best understood through the theoretical lenses of **security fatigue** and **learned helplessness**, psychological states in which individuals, feeling overwhelmed and powerless against an unstoppable adversary, cease protective efforts.

Furthermore, this study identified the presence of **moral injury** as a distinct psychological wound. Separate from the fear-based symptoms of PTSD, participants experienced a deep sense of guilt and shame rooted in a perceived failure to protect their networks and sources. This "preparedness regret" is a crucial aspect of the harm that has been previously overlooked in this context.

Finally, the research demonstrated that while all participants were impacted, **psychological resilience** and the ability to maintain a **sense of agency** were the key mediators of trauma outcomes. Participants who actively sought to regain control over their digital and professional lives exhibited less severe symptoms than those who felt entirely overwhelmed by the threat.

While this study acknowledges limitations related to its specific sample size and regional focus, its strength lies in the depth of its mixed-methods analysis. It provides a robust, empirically grounded portrait of the human cost of state-sponsored cyberattacks. The findings underscore the urgent need for a multi-layered response that includes stronger international regulations to curb the proliferation of spyware, greater corporate accountability from technology companies, and the development of holistic security models within civil society organizations.

Most importantly, this research highlights the need for specialized, trauma-informed support for victims. Interventions must move beyond generic counselling to address the specific wounds of moral injury and learned helplessness, with a focus on restoring a sense of agency and control. Further research is recommended to expand upon these findings, incorporating larger and more diverse samples and conducting longitudinal studies to track the long-term consequences of this insidious form of repression. Ultimately, this thesis confirms that in the digital age, protecting human rights requires a deep understanding of, and a robust response to, the psychological warfare being waged against those who dare to speak truth to power.

9.2 Study Limitations and Future Research

It is important to acknowledge the limitations of this analysis, primarily the small sample size (N=16), which restricts the generalizability of these findings. This study should be considered a detailed portrait of this specific group.

However, the clear heterogeneity observed between cases provides a strong empirical rationale for future research. The variability between high-distress profiles (e.g., Case 8) and lower-distress profiles (e.g., Case 3) strongly suggests the existence of distinct subgroups within the sample. Therefore, a

subsequent cluster analysis of the cases is warranted to statistically identify these potential profiles. Such an analysis would allow for a more nuanced understanding of the different ways traumatic stress can manifest, paving the way for more personalized and targeted clinical interventions.

9.3 Recommendations

The findings of this thesis demonstrate that state-sponsored cyberattacks inflict a profound and multifaceted form of harm on dissidents, journalists, and human rights defenders. The psychological impact extends beyond generalized distress, manifesting as a distinct trauma profile characterized by hyperarousal, moral injury, and a debilitating sense of learned helplessness. This harm is not an accidental byproduct of surveillance but a strategic objective of digital repression, designed to silence dissent and create a widespread chilling effect [192].

Addressing this complex threat requires a multi-layered and integrated response that moves beyond condemning the use of surveillance software. The recommendations proposed in this chapter are therefore grounded in the specific findings of this study and the principles of the Universal Declaration of Human Rights. They are structured to address the problem systemically, targeting the international policy environment, the responsibilities of technology corporations, the resilience of organizations, and the direct needs of the individuals who have been harmed [193]

9.3.1 International Policy and Legal Accountability

The current international legal framework has proven inadequate for regulating the spyware industry and holding perpetrators accountable. A robust, top-down approach is necessary to create a global environment where such abuses are no longer tolerated [194].

Impose Targeted Sanctions and Strict Export Controls: Building on recent multilateral efforts , G7 and other democratic nations should impose coordinated, targeted sanctions on spyware companies whose products are demonstrably used by regimes that violate human rights. The Wassenaar Arrangement must be strengthened to move beyond a "soft-law" approach, mandating that human rights due diligence is a legally binding prerequisite for granting any export license for surveillance technology.

Establish a Moratorium and Clear Restrictions on Use: An immediate international moratorium should be placed on the sale and transfer of sophisticated surveillance technologies until a human-rights-compliant regulatory framework is established. This framework must include strict, enforceable restrictions that limit the use of spyware to legitimate, narrowly defined national security and law enforcement purposes, explicitly prohibiting its use against dissidents, journalists, and other members of civil society.

Strengthen Legal Accountability for Vendors and State Actors: The successful lawsuit by Meta (WhatsApp) against NSO Group, which resulted in a significant financial penalty , provides a powerful precedent. Technology companies whose platforms are exploited should be encouraged and

supported in pursuing legal action against spyware vendors, thereby increasing the operational and financial costs of their business. Furthermore, states should codify transnational repression as a specific crime within their domestic legal systems to provide clear avenues for prosecuting state actors and their proxies.

9.3.2 Technological and Corporate Responsibility

The arms race between security engineers and spyware developers is a central theme of this issue. Both spyware vendors and the manufacturers of the devices they target have a responsibility to mitigate harm.

- **Mandate "Security by Design" for Spyware:** Any future regulation must compel spyware vendors to engineer their products with safeguards. This includes designing tools that focus only on specific, necessary data rather than granting wholesale access to a device, and building in "kill switches" that allow the manufacturer to disable the spyware if misuse is detected.
- **Increase Funding and Transparency in Platform Security Research**: Technology giants like Apple and Google must continue to allocate greater funding and resources to security researchers dedicated to identifying and patching the kinds of zero-click vulnerabilities exploited by Pegasus. As this study's technical analysis shows, the compromise of even the most secure platforms is a key driver of the psychological erosion of trust. Therefore, transparently reporting on these vulnerabilities and the steps taken to fix them is crucial for rebuilding user confidence.

9.3.3 Organizational and Community Resilience

The findings of this thesis reveal that psychological resilience is a key mediator of trauma. This resilience is not merely an individual trait but is fostered through collective and organizational support.

- **Promote Holistic Security Models**: Civil society organizations, newsrooms, and funders must move beyond a narrow focus on digital tools and adopt holistic security frameworks that integrate digital security, physical safety, and psychosocial well-being. This approach, championed by organizations like Tactical Tech and Protection International, recognizes that the stress of managing digital threats has a direct psychosocial impact that must be addressed concurrently.
- **Invest in Trauma-Informed Organizational Cultures**: Newsrooms and human rights organizations must actively work to dismantle the stigma surrounding mental health. This involves creating peer support networks and providing access to specialized, trauma-informed therapists who understand the unique cultural context of journalism and activism.

9.3.4 Victim-Centered Support and Empowerment

The ultimate goal of any intervention must be to support the individuals who have been harmed. This requires moving beyond generic assistance to provide specialized care that addresses the specific wounds identified in this research.

- **Provide Specialized, Trauma-Informed Psychosocial Support**: Victims of state-sponsored cyberattacks require more than general counselling. Support systems must be equipped to address the specific psychological injuries of moral injury and learned helplessness. This includes therapies that help individuals process feelings of guilt and betrayal related to their perceived failure to protect their networks, and interventions designed to restore a sense of agency and control that has been shattered by the experience of a non-preventable attack. This vital support should be funded by the responsible actors who made the use of spyware easy for authorities known for their human rights violations; this includes spyware developers, governments who used such software to suppress their dissidents, as well as phone and app manufacturers who share partial responsibility for not making their products secure against vulnerabilities while they advertise their product with its security rebust.
- **Empower Individuals Through Accessible Digital Security Education**: This study's finding that victims often feel helpless and do not adopt new security practices highlights a critical gap. Support must include practical, accessible digital security training that is designed not just to impart technical knowledge, but to rebuild confidence and restore a sense of personal agency in the digital realm.
- **Cultivate a Mindset of Proactive Preparedness**: A crucial component of empowerment involves shifting the individual's mindset from one of reactive fear to one of proactive preparedness. This does not mean living in a constant state of anxiety, but rather integrating a realistic threat model into daily life by accepting that such actions from authorities can happen. Academic literature on resilience suggests that such a preparedness mindset can serve as a psychological buffer, potentially reducing the shock and severity of the trauma if an attack is discovered. By mentally preparing for this possibility, individuals can reduce the shattering of core assumptions about safety that leads to PTSD. This mindset also encourages consistent engagement with digital security practices, not as a guarantee against sophisticated exploits, but as a form of reclaiming agency and control over one's digital environment. It is vital to frame this not as a form of victim-blaming, but as a strategic tool for building psychological resilience and mitigating the debilitating effects of learned helplessness.

9.3.5 Directions for Future Academic Research

This study serves as a foundation for a critically important and under-researched field. Future academic work should build upon these findings to:

- Encourage universities and research institutions to prioritize research and development in the field of spyware technology, fostering the development of countermeasures and promoting a deeper understanding of the threats posed by these tools.
- Investigate the emerging threat of AI-powered surveillance and its unique psychological impacts.
- Conduct longitudinal studies to track the long-term psychological trajectory of victims and the efficacy of different support interventions.
- Explore the potential of decentralized technologies, such as DAOs, as alternative platforms for secure and resilient activism.

By implementing these multi-layered recommendations, the international community, technology companies, civil society, and researchers can work together to mitigate the harms of state-sponsored spyware and contribute to a more secure and just digital environment for all.

9.4 Study Limitation

9.4.1 Limitations, Reflections, and Directions for Future Research

A core component of rigorous academic inquiry is a critical reflection on the research process and a transparent acknowledgment of a study's limitations. This chapter provides such an evaluation. It discusses the methodological boundaries inherent in this research, reflects on the challenges encountered during fieldwork with a high-risk population, and outlines promising directions for future investigation. By contextualizing the study's scope and constraints, this chapter aims to reinforce the validity of the findings while paving the way for a more expansive field of inquiry into the human cost of digital repression.

9.4.2 Methodological Limitations

This study aimed to investigate the psychological and sociological impact of state-sponsored cyberattacks on dissidents. The primary limitations are related to the sampling strategy and the specific scope of the research.

Sampling and Generalizability: This study employed a non-probability sampling strategy, combining purposive and snowball techniques. This approach was a methodological necessity for accessing a high-risk, hard-to-reach population of dissidents who would be unlikely to respond to public calls for participation [187]. While this strategy was successful in recruiting 16 participants and yielding rich, in-depth qualitative data sufficient for achieving thematic saturation , it inherently limits the statistical generalizability of the quantitative findings derived from the Harvard Trauma Questionnaire (HTQ). Therefore, the quantitative results presented in this thesis should be interpreted as a detailed and

valid portrait of this specific cohort, rather than a statistically representative sample of all dissidents targeted by spyware.

Technological and Geographic Scope: The research deliberately focused on attacks involving Pegasus spyware on iOS devices within the Gulf Cooperation Council (GCC) region. This focus was necessitated by the availability of verifiable forensic evidence and the unique socio-political context of the region, which, as argued in the literature review, may amplify the psychological impact of privacy violations. However, this specificity means the findings may not be directly transferable to victims of different spyware tools or those operating on other platforms, such as Android. While the capability of spyware to target Android devices is widely acknowledged [188] , the lack of confirmed, publicly accessible forensic reports at the time of this study precluded a comparative analysis. This represents a key area for future investigation.

9.4.3 Challenges and Reflections on the Research Process

Several challenges were encountered during the research process, each of which informed the study's final design and execution.

- **Navigating a Nascent Field**: One of the initial challenges was the relative scarcity of academic literature specifically addressing the link between state-sponsored cyberattacks and mental health outcomes like PTSD and moral injury. This required a broader review of related fields, including the psychology of political persecution[189], cybercrime victimization[190], and trauma in journalism [191]. While a challenge, this gap also underscores the originality and importance of this study in providing a foundational, empirically grounded analysis of a critically under-researched phenomenon.
- **Absence of Technical Emulation**: another challenge was the limited availability of detailed technical information and the impossibility of accessing the spyware software itself for emulation. Consequently, the research approach was adapted to focus on the analysis of documented vulnerabilities and, most importantly, on the victims' lived experience of the attack's aftermath. This methodological shift aligns with the study's primary objective, as the psychological consequences are shaped by the perception of the intrusion and its effects, which can be powerfully captured through qualitative inquiry.
- **Ethical Imperatives in High-Risk Research**: Ethical considerations were paramount throughout the research process, particularly given the vulnerability of participants who had experienced state-sanctioned trauma. The measures implemented were not merely procedural but foundational to the research design. Contacting participants through trusted channels and pre-existing networks was essential for establishing the initial rapport needed to even begin a conversation. Obtaining fully informed consent, which included detailed discussions of data security protocols and the right to withdraw at any time, was crucial for

empowering participants in a context where their agency had been previously violated. Finally, implementing robust data security—including end-to-end encryption for communication and offline, encrypted storage for all data—was a non-negotiable ethical baseline for mitigating risk and upholding the duty of care to participants.

9.5 Directions for Future Research

This study, while providing valuable insights, serves as a foundation for a much broader field of inquiry. Future research should expand upon these findings in several key areas:

- **Broadening Scope and Comparative Analysis**: Future studies should employ larger and more diverse samples, encompassing different geographical regions and cultural contexts. A comparative analysis of the psychological impact of different spyware tools beyond Pegasus would be highly valuable.
- **Investigating Android-Specific Exploits**: Given the widespread use of Android devices globally, dedicated forensic and psychological research into confirmed attacks on this platform is urgently needed to understand if and how the user experience and psychological sequelae differ from those on iOS.
- **Longitudinal Studies**: This study provides a cross-sectional snapshot of the psychological impact. Longitudinal research is needed to track the chronicity of PTSD, moral injury, and security fatigue over time, and to assess the long-term effectiveness of coping mechanisms and support interventions.
- **Exploring the "Ripple Effect"**: The psychological harm of these attacks is not confined to the primary target. Future studies could investigate the secondary or vicarious trauma experienced by the families, colleagues, and professional networks of those who have been targeted.

In conclusion, while this study operates within clearly defined limitations, its strength lies in the depth and nuance of its mixed-methods analysis. By transparently addressing its scope and challenges, it provides a credible and foundational exploration of the human cost of digital repression and offers a clear roadmap for future research in this critical and evolving field [192].

9.6 Researcher's Reflections on the Fieldwork

9.6.1 Introduction to Reflections:

As outlined in the methodology, this study employed a mixed-methods approach incorporating semi-structured interviews to gather in-depth qualitative data. This chapter moves beyond the formal findings to offer critical reflections on the data collection process itself. Conducting research with a population of dissidents targeted by state-sponsored cyberattacks presents unique methodological and ethical challenges. These reflections on navigating access, building trust, and observing the real-time manifestation of trauma are therefore offered not merely as personal impressions, but as a

crucial layer of context for interpreting the study's results and as a statement on the researcher's positionality.

9.6.2 Access, Trust, and Rapport: The Foundations of Fieldwork:

The majority of participants expressed a strong interest in contributing to this research, yet this willingness was almost universally coupled with significant security concerns. The majority of the participants voiced apprehension about the potential disclosure of their identities, a fear that is a direct and rational consequence of their lived experience with surveillance. This underscores a central challenge in researching hard-to-reach and persecuted populations: the paradox of needing to speak out while being conditioned by the very real risks of doing so.

In this context, the researcher's positionality and pre-existing network within the dissident community proved to be the most critical factor in securing participation. The establishment of trust, facilitated by the researcher's prior, verifiable work in this field, was indispensable. Without this foundation, it is highly probable that recruitment would have been unsuccessful.

This trust manifested in specific ways that shaped the data collection. One participant, while expressing confidence in the researcher, opted for an audio-only interview due to a heightened state of anxiety surrounding the use of any video-based digital devices following their experience of being hacked. Another participant, a recognized expert who has previously published under their own name, requested complete anonymity for this study. These instances are not mere logistical details; they are data points in themselves, illustrating the pervasive and lasting impact of surveillance on individuals' sense of safety and their relationship with technology.

9.6.3 The Manifestation of Trauma During the Interview Process

A compelling and recurring dynamic observed during the interviews was the initial dissonance between participants' self-perception and their narrative accounts. Several participants initially denied experiencing any significant changes in their mental health or behaviour following the attacks. However, as they shared their stories, their narratives revealed clear indications of psychological distress, including symptoms of paranoia and anxiety. This phenomenon aligns with literature on trauma, where individuals, particularly those in high-resilience roles like activists and journalists, may employ coping mechanisms of denial or minimization, or may not have the vocabulary to label their experiences as trauma.

A common theme that emerged, even among those who initially denied any impact, was a fundamental shift in their relationship with technology. This was consistently characterized by heightened distrust of smartphones and a persistent, ambient fear of surveillance. This fear was not abstract; it manifested in specific, visceral ways. Some participants described experiencing paranoia related to everyday objects in their environment, such as ceiling lights and televisions, believing they

could be conduits for surveillance. This is a powerful qualitative indicator of the kind of hypervigilance that the HTQ aims to measure quantitatively, where the threat is perceived as omnipresent and environmental.

Several participants candidly acknowledged their mental health challenges. One individual reported the onset of hypnagogic hallucinations and intrusive thoughts, which may reflect the mind's struggle to process the invasive trauma of the cyberattack. Three participants explicitly reported experiencing nightmares related to the attack. These direct disclosures of classic PTSD symptoms during the interviews provide rich, narrative validation for the quantitative findings of the HTQ.

Despite many participants anticipating that their activism made them a target, all expressed a sense of profound disruption and vulnerability upon the actual discovery of the compromise. This highlights the difference between the intellectual awareness of a risk and the visceral, traumatic impact of its realization. The knowledge that they were subject to ongoing surveillance, coupled with the uncertainty of future attacks, created a persistent state of anxiety and insecurity that was palpable during the interviews.

9.6.4 Ethical Considerations and Researcher Responsibility:

The participants' emphasis on anonymity and security during the interview process reflects a heightened awareness of risk. Paradoxically, this was often coupled with what appeared to be limited personal engagement with advanced digital security practices. This observation does not suggest negligence on the part of the participants but rather points to the complex psychological states of security fatigue and learned helplessness, which are explored in the findings of this thesis. It underscores the urgent need for targeted, holistic support that empowers dissidents not only with technical tools but also with the psychological resources to overcome the paralysis that such overwhelming threats can induce.

The interviews with participants who had been subjected to physical torture and mistreatment prior to the cyberattacks revealed the complex layering of trauma. While the primary cause of their PTSD symptoms may be attributed to physical abuse, the cyberattacks appeared to have served as a powerful secondary trauma, exacerbating their existing distress and contributing to a heightened sense of vulnerability and paranoia in the digital realm.

Finally, in adherence with ethical research principles, following the administration of the HTQ, participants were informed of their individual scores and the potential implications regarding PTSD symptomatology. It was strongly emphasized that the researcher is not a qualified mental health professional and that the HTQ is a screening tool, not a diagnostic one. Participants were strongly encouraged to seek further assessment and support from qualified practitioners if they felt it was necessary. This ethical step was crucial to ensure that the research process itself did not cause harm

and instead provided participants with information that could empower them to seek appropriate care. The overwhelmingly positive reception of the study and the participants' encouragement to further explore the link between digital security and mental health underscore the profound importance and timeliness of this research.

13 Acknowledgements

This research was a challenging yet profoundly rewarding endeavor, and its completion would not have been possible without the support, guidance, and encouragement of several individuals and organizations. I wish to extend my sincere and deep gratitude to all who contributed to this project.

First and foremost, my deepest appreciation goes to the courageous individuals who volunteered to participate in this study. In a context where anonymity is paramount and trust is paramount, their willingness to share their sensitive and often painful experiences was an act of profound bravery. Their voices are the heart of this research, and I am honoured to have been entrusted with their stories.

I am immensely grateful for the invaluable guidance and mentorship of my supervisor, Dr. Vasileios Vasilakis. His intellectual support, critical insights, and unwavering encouragement were instrumental in navigating the complex methodological, ethical, and analytical challenges inherent in this research. His expertise provided the steady hand that guided this project from its inception to its conclusion.

I would also like to extend my deep grateful to Dr Siamak Shahandashti, for his crucial support and understanding of the challenges as well as his valuable comments during the research period.

I would also like to acknowledge the vital contributions of the security researchers and experts at Citizen Lab and Amnesty Tech. Their groundbreaking work in exposing state-sponsored surveillance provided the essential technical context for this study, and their public reports were an invaluable resource.

On a personal note, I extend my heartfelt thanks to my family and friends. Their unwavering support, patience, and understanding provided the foundation of encouragement that sustained me throughout this demanding process.

Finally, I thank everyone who contributed, directly or indirectly, to this research. To any I may have inadvertently omitted, please accept my sincere apologies and know that your contributions are deeply valued.

14 Appendix

Appendix 1

Questionnaire for Victims

1. Have you been targeted by state spyware?
2. How did you know?
3. What type of spyware you have been targeted with?
4. Was it confirmed technically? If yes by whom?
5. How did you react to the news that you have been attacked by the state?
6. How did the attack change you mentally?
7. Did your use of connected devices change after the attack?
8. Have you been diagnosed with any mental health issue after the attack?
9. Do you think you have a trauma?
10. Do you think the impact of the incidents is permanent or temporary?
11. why do you think you have been attacked? Is it because of your activities and work?
12. Did the attack have an impact on your work? Did you continue your work? you decrease it? changed the way you work?
13. Did you inform your family, partners, your network about the attack? How did they respond?
14. Do you think that the attack was successful because of your mistakes?
15. Who do you think should be blamed for the attack? You? The manufacturer of the device? the spyware producer? And what is the involvement percentage for each one of them?
16.
17. After the attack? Are you able to trust any data stored in any device?
18. Do you feel you are under surveillance right now?
19. did you introduce any new practice to protect your data and privacy?
20. Did the attack increase your digital security knowledge?

Appendix 2

Consent Form
University of York
Department of Computer Science

Research Supervisor:

Student Name:

Research Title: Cyber-Attacks by State Actors on journalists, activists, and dissidents, and their Psychological and Sociological Impact

Dear,

Thanks for being part of this study.

This Research is intending to study the impact of espionage activities against Dissidents and its aftermath impact from Psychological and Sociological aspects. The aim is to understand the technical operation behind it, the limit of the impact, and what needs to be done to mitigate the espionage activity.

As a participant in this study, your information, your response, and answers will not be revealed to any third party. The content of this interview will be recorded and conducted via secure connection, a copy of the interview will be stored on external storage and encrypted storage device. The material should be destroyed after the period of the study is over.

We value your privacy and your special circumstances, thus, if it is needed – under strict circumstances -, your answers will be accessed by the research supervisor with an anonymous participant ID number referenced to your interview and your real name and personal information will not be revealed.

At any time during or after the interview, if you feel you need to change your mind in participating, please let me know and it will be stopped immediately, as well as if you think you need to change some answers after the interview before the submission deadline, you can always reach out to me, my details contact is below.

Thanks again for helping in this project.

Email:

Participant Name: ID number: 1001

Participant Signature:

Age:

Gender:

Nationality – or region-:

Education level:

Area of Work :

Working locally or internationally:

Appendix 3
Harvard Trauma Questionnaire

No.	Symptom	(1) Not at all	(2) A little	(3) Quite a bit	(4) Extremely
1	Recurrent thoughts or memories of the most hurtful or terrifying events				
2	Feeling as though the event is happening again				
3	Recurrent nightmares				
4	Feeling detached or withdrawn from people				
5	Unable to feel emotions				
6	Feeling jumpy, easily emotions				
7	Difficulty concentrating				
8	Trouble sleeping				
9	Feeling on guard				
10	Feeling irritable or having outbursts of anger				
11	Avoiding activities that remind you of the traumatic or hurtful event				
12	Inability to remember parts of the most hurtful or traumatic event				
13	Less interest in daily activities				
14	Feeling as if you don’t have a future				
15	Avoiding thoughts or feelings associated with the traumatic or hurtful events				
16	Sudden emotional or physical reaction when reminded of the most hurtful or traumatic event				
17	Feeling that you have less skills than you have before				
18	Having difficulty dealing with new situations				
19	Feeling exhausted				
20	Body pain				
21	Troubled by physical problems				
22	Poor memory				
23	Finding out or being told by other people that you have done something that you cannot remember				
24	Difficulty paying attention				

25	Feeling as if you are split into two people and one of you is watching what the other is doing				
26	Feeling unable to make daily plans				
27	Blaming yourself for things that happened				
28	Felling guilty for having survived				
29	Without hope				
30	Feeling ashamed of the hurtful or traumatic events that have happened to you				
31	Felling that people do not understand what happened to you				
32	Felling others are hostile to you				
33	Feeling that you have no one to rely upon				
34	Feeling someone you trusted betrayed you				
35	Feeling humiliated by your experience				
36	Feeling no trust in others				
37	Feeling powerless to help others				
38	Spending time thinking why these events happened to you				
39	Feeling that you are the only one that suffered these events				
40	Feeling a need for revenge				

Appendix 4

Participants Responses and Mean Scores for the Harvard Trauma Questionnaire (HTQ)

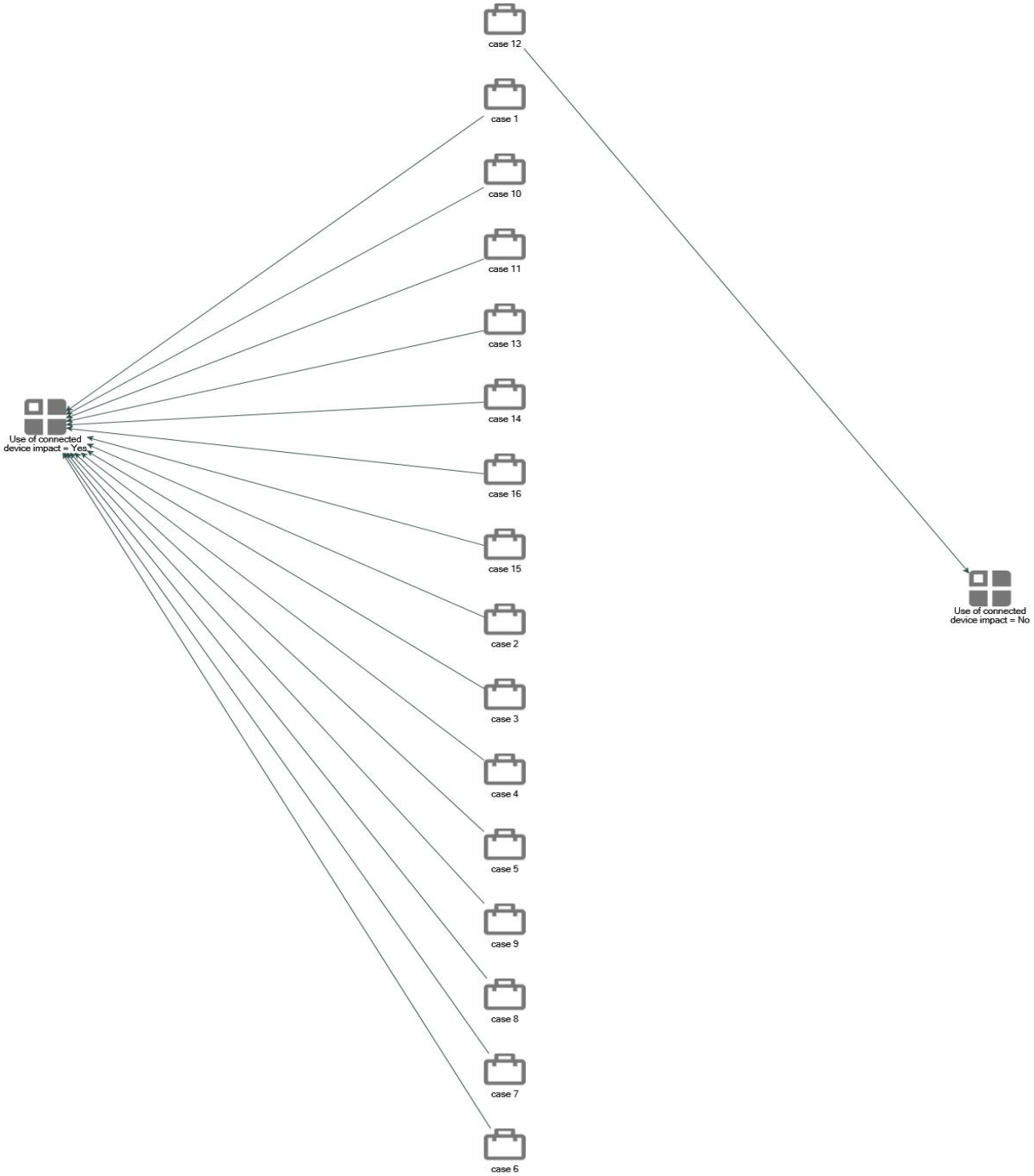
Case ID	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Q21	Q22	Q23	Q24	Q25	Q26	Q27	Q28	Q29	Q30	Q31	Q32	Q33	Q34	Q35	Q36	Q37	Q38	Q39	Q40	Total	Percent
Case 1	3	3	2	2	2	3	3	3	4	3	2	2	3	3	4	3	2	3	2	2	2	2	4	4	2	3	4	2	3	3	4	2	2	3	3	3	3	3	2	4	103	2.861
Case 2	4	4	4	4	2	3	3	4	4	3	3	2	3	3	3	4	2	2	3	4	3	3	3	3	2	2	4	3	4	4	4	4	3	4	4	3	3	2	3	4	115	3.194
Case 3	4	4	4	4	3	4	3	4	4	4	3	3	3	3	3	3	3	3	3	4	3	4	2	3	2	2	3	3	2	4	4	3	3	4	4	3	3	2	1	4	114	3.166
Case 4	2	4	2	3	2	2	3	2	4	4	3	2	2	3	2	3	1	2	1	2	2	3	2	2	1	1	2	2	1	4	4	3	2	3	4	3	2	2	3	4	90	2.5
Case 5	4	4	3	4	3	3	3	3	4	4	3	2	2	3	3	4	3	3	3	3	3	3	3	2	2	2	4	2	4	4	4	3	3	3	4	3	3	4	3	3	115	3.194
Case 6	4	4	3	3	2	3	3	2	4	4	2	2	2	3	3	3	3	2	2	2	2	3	2	3	2	1	3	3	2	4	4	3	2	3	4	2	3	3	3	4	102	2.833
Case 7	4	4	3	3	2	3	3	2	4	3	3	3	2	3	3	3	2	2	3	3	4	2	2	2	2	2	4	2	3	4	4	3	3	3	4	3	3	3	2	4	105	2.916
Case 8	4	4	4	4	3	4	3	3	4	4	3	3	3	3	3	4	3	3	3	4	4	4	3	3	3	3	4	3	3	4	4	4	3	4	4	3	3	4	4	4	125	3.472
Case 9	4	4	3	3	3	3	2	2	4	3	3	2	2	3	3	3	2	2	3	2	3	4	2	3	2	2	4	3	3	4	4	2	3	3	4	2	2	3	3	4	105	2.916
Case 10	4	4	3	4	3	4	3	4	4	4	3	3	3	2	3	3	3	3	4	4	3	4	3	3	2	2	3	3	3	4	3	3	2	4	4	2	3	3	3	4	115	3.194
Case 11	4	4	2	2	3	3	2	2	4	4	3	2	2	3	3	3	2	2	3	3	3	4	2	3	2	2	4	3	3	4	3	2	3	4	4	2	2	3	3	4	103	2.861
Case 12	4	4	2	3	2	4	3	2	4	3	3	2	1	3	3	3	2	3	3	3	2	4	3	2	3	2	3	3	3	4	4	3	3	4	4	3	3	3	3	4	108	3
Case 13	4	4	4	3	3	3	3	4	4	4	3	3	3	3	3	3	3	2	4	3	3	4	3	2	3	2	3	3	3	4	4	3	3	4	4	2	3	3	4	4	117	3.25
Case 14	4	4	2	3	2	3	3	2	4	4	3	2	3	3	2	3	3	3	3	2	2	3	2	2	2	3	4	2	4	4	4	3	2	4	4	3	3	4	3	4	110	3.055
Case 15	4	4	3	2	2	3	2	2	4	4	2	2	3	3	2	2	3	2	3	2	2	3	3	3	2	2	3	2	3	4	4	3	3	3	2	3	3	3	3	4	103	2.861
Case 16	4	4	2	3	3	3	2	2	4	4	2	2	2	3	2	2	2	2	3	3	3	4	2	3	2	2	4	2	3	4	3	2	2	3	0	2	3	3	3	4	101	2.805
Mean score	3.8125	3.9375	2.875	3.125	2.5	3.1875	2.75	2.6875	4	3.6875	2.75	2.3125	2.4375	2.9375	2.8125	3.0625	2.4375	2.4375	2.875	2.875	2.75	3.375	2.5625	2.6875	2.125	2.0625	3.5	2.5625	2.9375	3.9375	3.8125	2.875	2.625	3.5	3.5625	2.625	2.8125	3	2.875	3.9375		

Appendix 5

Case ID	Gender	Work	Age range	Education
Case 1	Male	Activists	35-45	Secondary School
Case 2	Female	HRD	35-45	MSc
Case 3	Female	HRD	45-55	Diploma
Case 4	Male	Activists	45-55	MSc
Case 5	Male	Activists	25-35	BSc
Case 6	Male	Politician	55-65	PHD Student
Case 7	Male	Politician	25-35	BSc
Case 8	Female	HRD	55-65	PHD
Case 9	Male	jurnalist	25-45	BSc
Case 10	Male	HRD	65+	BSc
Case 11	Male	Journalists	25-35	MSc
Case 12	Male	HRD	55-65	BSc
Case 13	Male	Lawyer	55-65	BSc
Case 14	Male	Activists	25-35	MSc
Case 15	Male	HRD	35-45	BSc
Case 16	Male	Journalists	35-45	Diploma

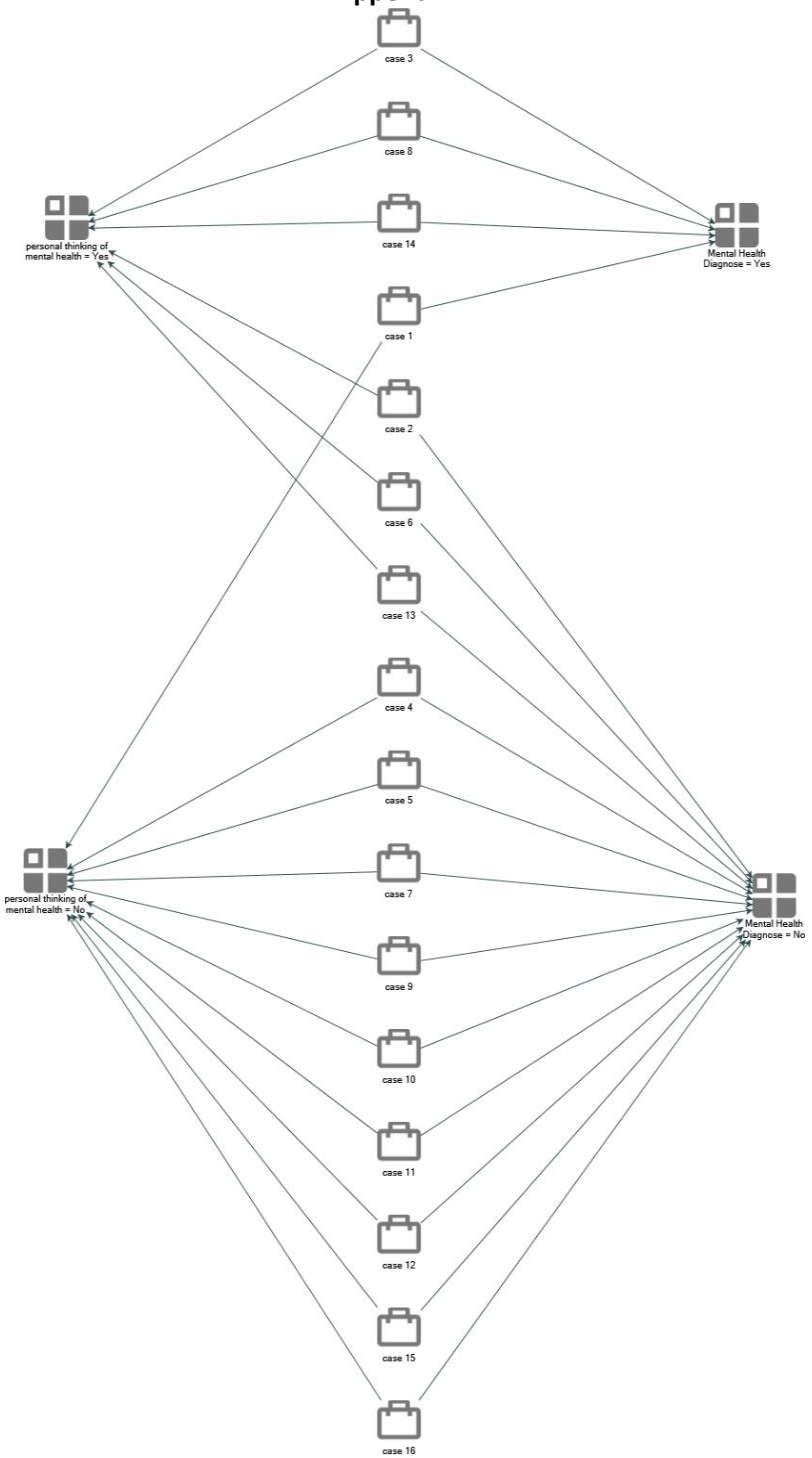
Table of Participants Demographic Data

Appendix 6



Use and store data in connected devices after the attack

Appendix 7



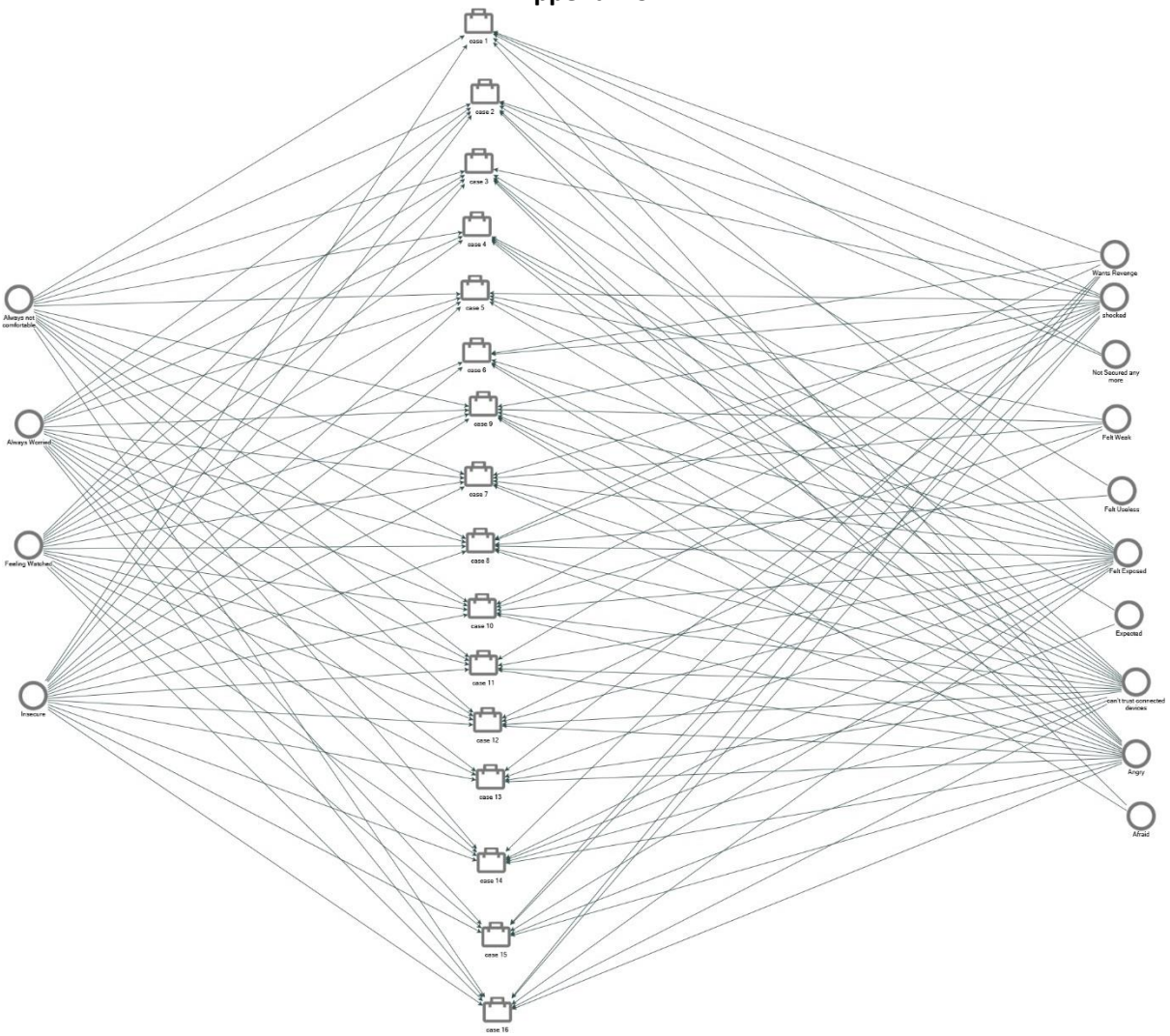
Relationship Between cases and Mental Health Status

Appendix 8

Name	Impact on Work	? Did you continue your work ?	Decrease it?	Change the way you work?
Case 1	No	Yes	No	Yes
Case 2	Yes	No	Yes	Yes
Case 3	Yes	Yes	No	Yes
Case 4	No	yes	Yes	NO
Case 5	Yes	No	Yes	Yes
Case 6	No	Yes	No	Yes
Case 7	No	Yes	Yes	Yes
Case 8	No	Yes	Yes	Yes
Case 9	Yes	Yes	Yes	Yes
Case 10	Yes	Yes	Yes	Yes
Case 11	Yes	Yes	No	Yes
Case 12	Yes	Yes	Yes	Yes
Case 13	Yes	Yes	No	Yes
Case 14	Yes	Yes	No	Yes
Case 15	Yes	Yes	No	Yes
Case 16	Yes	Yes	No	Yes

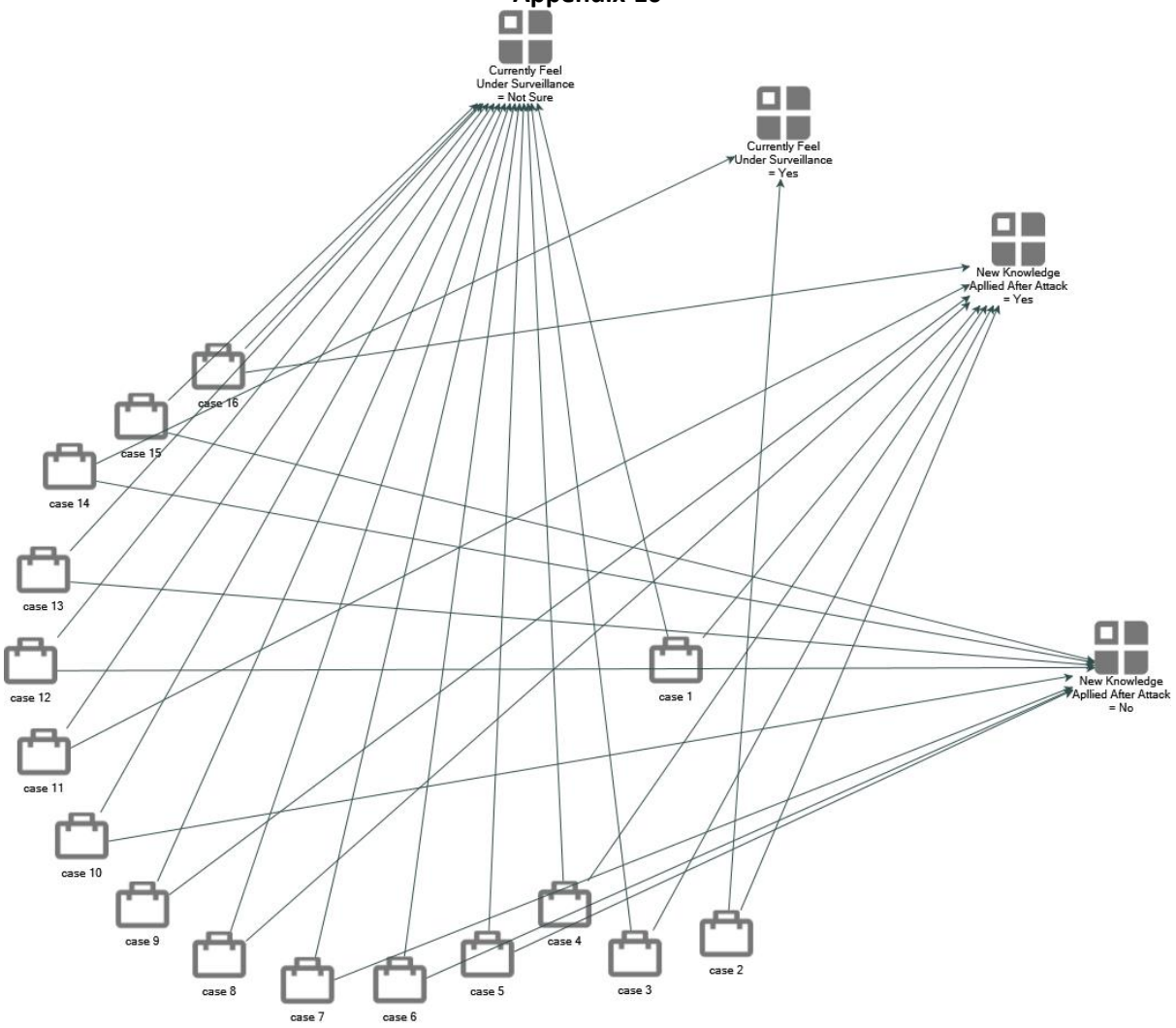
Impact on Work after the Attack

Appendix 9



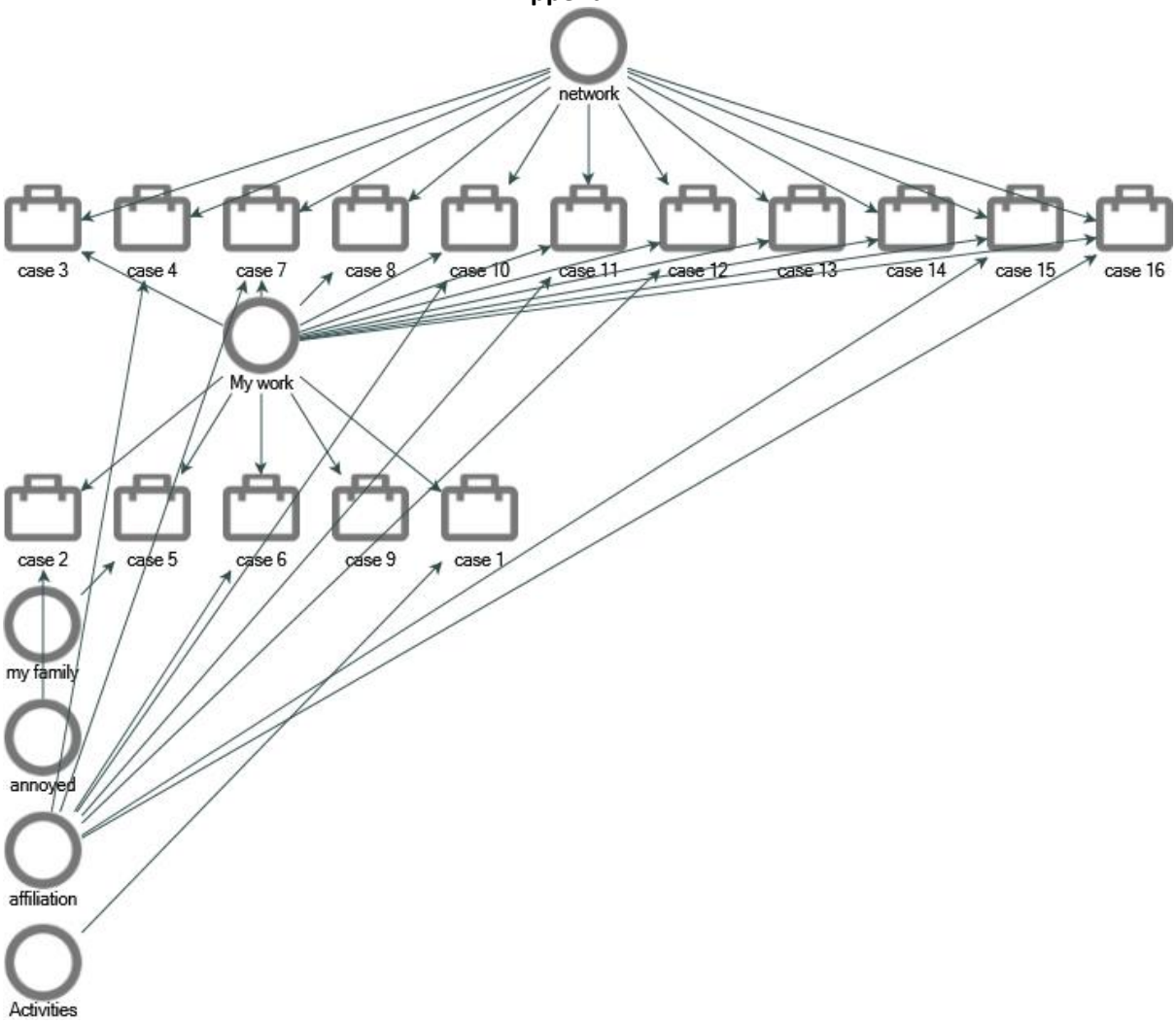
Map of Words used by the participants reflecting to the news of the Attack

Appendix 10



Victims Anticipated about Surveillance

Appendix 11

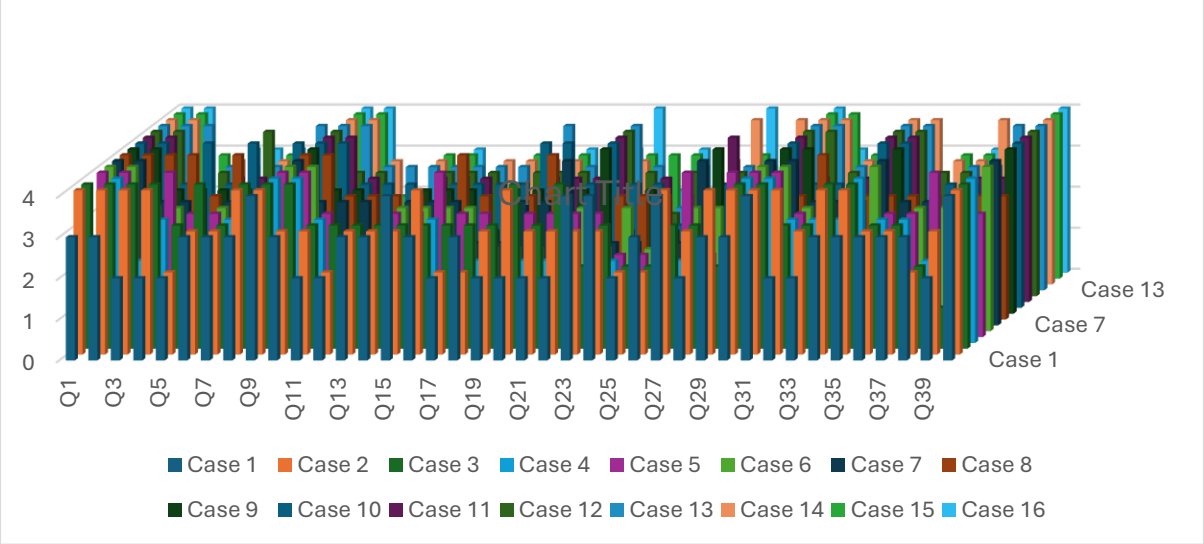


Participants response to the Reason of the Attack

Appendix 12

Word count used by participants in the first interview

Appendix 13



Result from HTQ

Appendix 14
Thematic Analysis Coding Frame

Word/Phrase from Interview	Suggested Theme (Child Node)	Suggested Code (Parent Node)	Rationale / Notes
Q11: How did you feel when you knew that you have been attacked?			
Shocked	Shock	Emotional	Direct match.
Felt exposed	Vulnerability	Emotional	Implies a lack of protection, openness to harm.
Not secured any more / Not secured	Vulnerability	Emotional	Loss of safety, feeling unprotected.
Angry	Anger	Emotional	Direct match.
Want revenge / Need revenge	Anger	Emotional	Often a strong manifestation of anger.
Felt useless	Vulnerability	Emotional	Feeling disempowered, unable to act effectively.
Can't trust the connected devices	Vulnerability	Emotional	Specific manifestation of feeling unsecured and exposed, leading to a sense of vulnerability regarding safety with technology.
Afraid	Fear	Emotional	Direct match.
Expected	Anticipation/Expectation	Emotional	Represents a pre-existing mental state, distinct from

			immediate emotional reactions.
Felt weak	Vulnerability	Emotional	Direct sense of reduced strength or capability.
Q12: How did the attack changed you mentally?			
Always worried	Fear	Emotional	Worry is a key component of fear or anxiety.
Feeling watched	Paranoia	Emotional	Direct match.
Insecure	Vulnerability	Emotional	A lack of certainty or safety.
Always not comfortable	Fear	Emotional	A constant state of unease or apprehension.
Q17: why do you think you have been attacked? Is it because of your activities and work?			
My work and activity / My work / My work annoyed the authorities / To expose my network, my work	Professional/Activist Motivation	Perceived Attack Drivers	The perceived reason for the attack is linked to their professional role, advocacy, or public activities.
My network, my affiliation	Network/Affiliation-Based Motivation	Perceived Attack Drivers	The perceived reason for the attack is linked to their social/professional connections or group identity.

My work, my family	Personal Motivation	Perceived Attack Drivers	The perceived reason for the attack includes personal life aspects.
Q18: Did the attack have an impact on your work? Did you continue your work? you decrease it? changed the way you work?			
Yes (impact)	Impact Present	Behavioral & Professional Impact	Indicates an acknowledged effect on work.
No (impact)	No Impact	Behavioral & Professional Impact	Indicates no perceived effect on work.
Yes (continue)	Work Continuity	Behavioral & Professional Impact	Reflects the ability or decision to maintain work.
No (continue)	Work Discontinuation	Behavioral & Professional Impact	Indicates stopping work.
Yes (decrease)	Workload Adjustment	Behavioral & Professional Impact	Reflects a reduction in work quantity.
No (decrease)	No Workload Adjustment	Behavioral & Professional Impact	Indicates no reduction in work quantity.
Yes (changed way work)	Work Modification	Behavioral & Professional Impact	Reflects changes in how work is performed.
No (changed way work)	No Work Modification	Behavioral & Professional Impact	Indicates no changes in work practices.
Q20: Do you think that the attack was			

successful because of your mistakes?			
No	No Self-Blame	Attribution of Causality/Responsibility	Indicates the individual does not attribute the attack's success to their own errors. (If "Yes" answers were present, a "Self-Blame" theme would be added here).

Appendix 15

Coefficient	Estimate	Std. Error	95% Confidence Interval
			Lower
Coefficient α (Alpha)	0.951	0.022	0.916

Appendix 16

A.16 Technical Analysis of Smartphone Attacks and Security

A.1 Introduction: The Smartphone as a Digital Battleground

The internet has become an integral component of contemporary society, permeating nearly every facet of modern life, from governance and financial systems to interpersonal communication and commerce. However, the internet's reliance on a global network infrastructure, particularly the Border Gateway Protocol (BGP) , for data transmission introduces inherent vulnerabilities. These vulnerabilities have given rise to a complex security landscape where the acquisition of information, often through exploitation of these weaknesses, has become a strategic objective for various entities, including state actors [6]. This pursuit of intelligence advantages underscores the inherent tension between the internet's democratizing potential and its susceptibility to exploitation for surveillance and control.

In the current digital landscape, the ubiquitous nature of smartphones, serving as repositories of personal data, has amplified the challenges associated with maintaining privacy and security. Individuals engaged in activism and dissent are particularly susceptible to state-sponsored surveillance, as their activities and communications are often deemed subversive and threatening to the established power structures. Smartphones have become essential tools in contemporary society, serving both personal and professional needs. These devices function as repositories of sensitive information, including personal contacts, private communications, confidential documents, and location data. This reliance on smartphones has heightened concerns regarding privacy and security, as these devices can inadvertently expose individuals to data breaches and surveillance. In response, smartphone manufacturers and third-party application developers have prioritized the integration of robust security and privacy features to mitigate these risks and bolster user trust. Conversely, spyware developers actively seek to exploit vulnerabilities within smartphone operating systems and applications, aiming to gain unauthorized access to devices [12]. This creates an ongoing adversarial dynamic between device manufacturers striving to enhance security and malicious actors seeking to circumvent these protections. This continuous struggle imposes significant costs and reputational risks on manufacturers, who must constantly adapt to evolving threats. Furthermore, governments, often in collaboration with spyware vendors, exploit these vulnerabilities to conduct surveillance operations, compromising the privacy and security of targeted individuals. This highlights the ethical complexities and potential for abuse inherent within the global spyware industry.

It is important to note that the technical details regarding vulnerabilities and their exploitation will be further elaborated upon in a subsequent section of this study. This detailed analysis will provide a deeper understanding of the mechanisms used to compromise devices and the potential consequences for individuals targeted by such attacks.

The development of secure and functional smartphones necessitates a delicate balance between feature enhancement and robust security architecture. Prioritizing security may impede the rapid introduction of new features, while an overemphasis on functionality may inadvertently increase

[12] Will explain in more details about vulnerability and how it's being used later.

vulnerability to exploitation [108]. Operating systems employ hierarchical access control mechanisms, such as protection rings, to mitigate these risks by isolating critical system components and restricting access to sensitive data [109]. However, even the most sophisticated security architectures are not impervious to attack. Malicious actors with advanced capabilities can exploit vulnerabilities to compromise system integrity, exfiltrate data, or establish persistent control over devices.

This underscores the inherent complexity of smartphone security, where design choices, user behaviour, and the evolving threat landscape interact in dynamic and often unpredictable ways. The ongoing arms race between security engineers and malicious actors necessitates constant vigilance and adaptation to ensure the privacy and security of individuals in an increasingly interconnected digital world.

A.2 The Cyber Kill Chain: A Framework for Digital Violation

To facilitate a comprehensive understanding of the mechanics of a successful cyberattack, this study utilizes the Cyber Kill Chain framework. This analytical model, developed by Lockheed Martin, provides a structured approach to dissecting the lifecycle of an attack, outlining seven distinct phases:

1. **Reconnaissance:** The attacker gathers information about the target system, identifying potential vulnerabilities and attack vectors.
2. **Weaponization:** The attacker creates a weaponized payload, such as malware or an exploit, tailored to the identified vulnerabilities.
3. **Delivery:** The weaponized payload is delivered to the target system, often through phishing emails, malicious websites, or other means.
4. **Exploitation:** The attacker triggers the payload, exploiting the vulnerability to gain unauthorized access to the target system.
5. **Installation:** The attacker installs malware or other tools to establish persistent access and control over the compromised system.

6. **Command and Control:** The attacker establishes a command-and-control channel to remotely control the compromised system and exfiltrate data.
7. **Actions on Objectives:** The attacker achieves their objectives, which may include data theft, disruption of services, or other malicious activities.

By applying the Cyber Kill Chain framework to the analysis of state-sponsored cyberattacks against dissidents, this study aims to illuminate the specific tactics and techniques employed by malicious actors, contributing to a deeper understanding of the threat landscape and informing the development of effective mitigation strategies [107].

Attackers commence their operation by conducting thorough reconnaissance to identify and exploit vulnerabilities within the target system. This initial phase is followed by the development of malicious code or tools, a process known as weaponization. Subsequently, the attacker employs various methods to deliver the weaponized payload to the target environment. Upon successful delivery, the attacker exploits the identified vulnerability to gain unauthorized access and install malicious software on the compromised system. This establishes a persistent foothold, allowing the attacker to maintain command and control over the compromised device and execute their objectives. The lifecycle of a typical cyberattack targeting smartphones can be characterized by a series of distinct phases:

1. **Vulnerability Identification:** Attackers actively seek out and identify vulnerabilities within commonly used operating systems or applications. These vulnerabilities can arise from coding errors, design flaws, or inadequate security practices.
2. **Exploit Development:** Once a vulnerability is identified, attackers develop malicious code, often referred to as an exploit, specifically designed to leverage this weakness and gain unauthorized access to the target device.
3. **Payload Delivery:** The weaponized exploit is then delivered to the target device, frequently employing deceptive tactics such as phishing emails, malicious attachments, or compromised websites.

4. **Exploitation and Installation:** Upon successful delivery, the exploit is executed, triggering the vulnerability and allowing the attacker to install malicious software, such as spyware, onto the device.
5. **Persistence and Control:** The installed malware often establishes a persistent backdoor, enabling the attacker to maintain ongoing remote control over the compromised device and access its data and functionalities at will [110] .

This systematic approach to compromising smartphones highlights the sophisticated tactics employed by malicious actors and underscores the ongoing challenges in securing these ubiquitous devices against cyberattacks.

To illustrate a typical attack scenario, consider the following hypothetical progression:

1. **Vulnerability Discovery:** An attacker identifies a vulnerability within a widely used application available on a popular smartphone platform, such as Apple's App Store or the Google Play Store.
2. **Exploit Development:** The attacker develops malicious code designed to exploit this vulnerability, potentially manipulating the operating system or altering its functionality to enable the execution of unauthorized code.
3. **Payload Delivery:** The attacker employs a delivery mechanism to transmit the malicious code to the target device. This could involve a phishing link that downloads an executable file in the background, embedding the code within a seemingly innocuous attachment, or utilizing a wireless injection technique to compromise the device remotely [25].
4. **Installation and Control:** Once the malicious code is executed, the attacker installs a persistent backdoor on the compromised device. This backdoor grants the attacker remote access and control, enabling them to exfiltrate data, monitor activity, or manipulate device functionality.

This hypothetical scenario exemplifies the typical stages involved in smartphone hacking, regardless of the specific operating system (Android or iOS). It underscores the persistent threat posed by

malicious actors seeking to exploit vulnerabilities and compromise the security and privacy of individuals.[25].

This hypothetical scenario exemplifies the typical stages involved in smartphone hacking, regardless of the specific operating system (Android or iOS). It underscores the persistent threat posed by malicious actors seeking to exploit vulnerabilities and compromise the security and privacy of individuals.

A.3 Smartphones Security

Smartphone manufacturers employ a multi-faceted security strategy to mitigate the inherent risks associated with these devices. This approach encompasses three interconnected layers:

1. **Hardware-Based Security:** This foundational layer comprises security measures embedded within the device's hardware, such as secure boot mechanisms and encryption technologies. These measures provide a fundamental level of protection against unauthorized access and data breaches.
2. **Software-Based Security:** This layer encompasses security features integrated within the operating system and applications, including access controls, sandboxing, and malware detection. These software-based defences provide an additional layer of protection against malicious software and unauthorized access attempts.
3. **User-Centric Security:** This layer emphasizes the role of user behaviour and responsible practices in safeguarding devices. This includes creating strong and unique passwords, regularly updating software to patch vulnerabilities, and exercising caution when installing applications [111, 195]. While device manufacturers bear the primary responsibility for implementing robust security measures at the hardware and software levels, users also play a critical role in maintaining the security of their devices through responsible practices and informed decision-making. This shared responsibility model underscores the importance of collaboration between manufacturers and users in creating a secure and trustworthy mobile ecosystem. This encompasses practices such as:
    - **Encryption:** Utilizing encryption tools to protect sensitive data stored on the device.

- **Strong Passwords:** Creating and employing strong, unique passwords to prevent unauthorized access.
- **Software Installation:** Exercising caution and discretion when installing software from unknown or untrusted sources.
- **Security Updates:** Regularly installing security updates to patch vulnerabilities and protect against emerging threats [29, 30].

While user-centric security practices are not directly controlled by device manufacturers, manufacturers bear a responsibility to:

- **Provide Comprehensive Security Features:** Equip devices with robust built-in security features and make these features easily accessible and understandable to users.
- **Enable Flexibility:** Offer users the flexibility to customize security settings and adopt additional security measures as needed.
- **Promote Security Awareness:** Educate users about security best practices and the importance of their role in safeguarding their devices.

This shared responsibility model, where both manufacturers and users play active roles in maintaining security, is essential for creating a robust and trustworthy mobile ecosystem.

Beyond software and user-centric security practices, physical safeguards play a crucial role in protecting smartphones. Securing devices in a safe location, away from unauthorized access, mitigates the risk of physical tampering and potential hacking attempts. However, it is important to acknowledge that advanced forensic tools, such as those offered by Cellebrite [13], can extract data even from locked and encrypted devices under certain circumstances. This underscores the importance of a comprehensive approach to smartphone security, encompassing both physical and digital measures. While physical safeguards can deter unauthorized access and tampering, the

[13] Cellebrite is a digital intelligence suite for law enforcement that could extract data from electronic devices such as smartphones, computers, tablets, etc. www.cellebrite.com.

potential for forensic extraction highlights the need for robust encryption and other security measures to protect sensitive data.

In addition to software-based and user-centric security measures, safeguarding the physical environment where devices are used and stored is paramount. This necessitates the implementation of robust security protocols in offices and workspaces to prevent unauthorized physical access and mitigate the risk of data breaches. Furthermore, securing IT infrastructure through measures such as network segmentation, firewalls, and intrusion detection systems is essential to protect against network-based attacks and prevent the introduction of malicious software via physical access points. This holistic approach to security recognizes that vulnerabilities can be exploited at various levels, from the physical device itself to the networks and infrastructure it interacts with. By addressing security across all domains, a more comprehensive and resilient defence against cyberattacks can be established.

A3.1 IOS Security

The iPhone's sleek design belies a sophisticated security architecture encompassing multiple layers of protection. These safeguards include sandboxing, secure enclaves, granular app permissions, code signing, and end-to-end encryption [112, 113, 196, 197]. However, the operating system's monolithic kernel design and the limited transparency surrounding its security mechanisms have raised concerns about potential vulnerabilities and the capacity for unauthorized access [114, 120, 198]. This is further complicated by the inherent tension between security and functionality, as well as the challenges posed by third-party applications, which can introduce vulnerabilities or circumvent existing security measures. The dynamic interplay between these factors creates a complex security landscape for both users and manufacturers, necessitating ongoing vigilance and adaptation to mitigate risks and ensure the protection of sensitive data.

A 3.2 Android Security

Android's open-source architecture, while fostering flexibility and customization, introduces inherent security complexities. Its layered architecture, comprising the Linux kernel, Android Runtime, native libraries, application framework, and individual applications, aims to safeguard user data through a multi-tiered approach. However, vulnerabilities can arise at any level within this structure, potentially

exacerbated by the integration of third-party applications and the susceptibility to malicious code injection. This inherent tension between openness and security necessitates ongoing vigilance and robust security measures to mitigate risks and protect user data within the Android ecosystem.

A 3.3 Third Parties Vulnerabilities

Third-party applications represent a significant security challenge within the smartphone ecosystem. The open nature of platforms like Android [199], which permits the installation of applications from diverse sources, increases the risk of malicious software infiltration. These applications can exploit vulnerabilities, compromise user data, or manipulate device functionality. Furthermore, certain user practices, such as granting excessive permissions or downloading applications from unreliable sources[200], can exacerbate these risks. This highlights the need for heightened awareness and vigilance among users, as well as robust security measures implemented by both operating system developers and app developers to mitigate the threats posed by third-party applications.

A Spyware and Vulnerabilities

To understand the mechanics of a spyware attack, it is imperative to analyse the exploitation of vulnerabilities. Spyware infiltrates a device, converting it into an unintentional surveillance instrument. This process entails identifying weaknesses within the device's operating system or applications, crafting malicious code to exploit these vulnerabilities, and delivering the payload to the target [14]. Upon installation, the spyware establishes persistent control, facilitating covert data extraction and device manipulation. Comprehending this lifecycle is essential for developing effective countermeasures and understanding the roles of various actors involved in the hacking process.

A 4.1 The Nature of Vulnerabilities

Vulnerabilities constitute the foundational elements exploited in cyberattacks, arising from software flaws, misconfigurations, or inadequate coding practices. These weaknesses can be identified by various actors, including security researchers, software developers, and malicious actors seeking to exploit them. The rapid exploitation of vulnerabilities, often facilitated by the cybercriminal underground, underscores the critical need for effective vulnerability management and response

[14] As explain earlier in the cyber kill chain

strategies. This necessitates a proactive approach to identifying and mitigating vulnerabilities, coupled with timely patching and remediation efforts to minimize the window of exposure and protect systems from compromise.

A 4.2 Spyware Design and Methodology

Spyware, classified as a form of malicious software, operates by surreptitiously monitoring a user's system without their knowledge or consent [115]. While categorized under the broader umbrella of malware, spyware is distinct from other types of malicious software, such as trojans, ransomware, and worms. These distinctions arise from differences in their objectives, infection vectors, associated symptoms, and corresponding countermeasures.

Spyware typically exploits vulnerabilities in software to enable unauthorized access and data exfiltration. Attackers identify and leverage these vulnerabilities to inject malicious code, facilitating surveillance and control over the targeted device. The cyber kill chain model, as previously discussed, provides a framework for understanding the stages involved in a spyware attack, from the initial vulnerability discovery to the installation and activation of the spyware on the victim's device. The discovery of a vulnerability triggers a race between security researchers seeking to mitigate the weakness and malicious actors aiming to exploit it. In the context of spyware development, this exploitation involves a strategic pursuit of several key objectives [116]:

1. **Stealth:** Spyware must be designed and deployed in a manner that evades detection by the user, antivirus software, and other security mechanisms. This necessitates sophisticated obfuscation techniques and the ability to operate covertly within the target system.
2. **Effectiveness:** The spyware must effectively fulfil its intended purpose, which typically involves the efficient collection and exfiltration of sensitive data from the compromised device. This requires optimized data collection algorithms and secure communication channels to transmit the acquired information to the attacker.
3. **Persistence:** Spyware must maintain a persistent presence on the target system, ensuring its continued operation even after system reboots or software updates. This necessitates mechanisms to evade removal attempts and re-establish access if disrupted.

4. **Adaptability:** The dynamic nature of the digital landscape requires spyware to be adaptable and capable of evading evolving detection methods and security updates. This necessitates ongoing development and refinement of spyware code to ensure its continued effectiveness. [116]

These objectives collectively underscore the sophisticated nature of spyware development and the challenges associated with mitigating the threats posed by these intrusive tools.

The primary objectives driving spyware design are contingent upon the specific requirements of the attacker and the targeted environment [201]. While some spyware prioritizes stealth, operating covertly to collect and transmit information without detection, others aim to transform the compromised device into a comprehensive surveillance tool. These more intrusive forms of spyware can grant attackers extensive capabilities, including remote control, keylogging, audio and video surveillance, location tracking, and comprehensive activity monitoring [120]. This diversity in spyware objectives reflects the wide range of malicious purposes these tools can serve, from targeted espionage to mass surveillance and the suppression of dissent.

The development of sophisticated spyware necessitates the identification and exploitation of vulnerabilities, often targeting the device's kernel layer where critical system files reside. Once installed and effectively concealed, the spyware operates autonomously, evolving and adapting its functionality according to the attacker's commands. Common installation vectors include:

- **Spear-phishing**: Utilizing deceptive messages or emails containing malicious links or attachments to trick users into compromising their devices.
- **Social Engineering**: Employing manipulative tactics to gain the trust of victims and induce them to leave their devices unattended, allowing for physical installation of the spyware.
- **Zero-click Attacks:** Exploiting known vulnerabilities to install spyware without requiring any user interaction. A notable example occurred in 2019 when a vulnerability in WhatsApp enabled the installation of Pegasus spyware through a missed call.

Post-installation, spyware can infiltrate various system layers, gaining access to sensitive data and resources. Traditional data exfiltration methods involve direct remote access by the attacker.

However, modern spyware often utilizes third-party servers for data storage and retrieval, obfuscating the attacker's identity and hindering attribution to specific state actors [82]. Furthermore, the retention and potential sharing of collected data by spyware producers and state operators raise significant privacy concerns [201].

Spyware capabilities are extensive, encompassing access to a wide range of sensitive information, including text messages, call logs, emails, media files, passwords, and other personal data [118]. Furthermore, spyware can activate device resources such as microphones, cameras, and sensors, enabling covert surveillance and data collection. It can also intercept and record calls, even those encrypted, and decrypt data from encrypted communication applications [118]. In essence, active spyware compromises all aspects of device privacy and security, rendering the user vulnerable to comprehensive surveillance and manipulation.

A 5 Notable Zero-click Vulnerabilities

To illustrate the sophistication of spyware when exploiting zero-click vulnerabilities, consider these recent examples of such vulnerabilities employed by spyware:

A 5.1 BLASTPASS

This zero-click vulnerability, identified by Citizen Lab in September 2023 and promptly disclosed to Apple, affected a range of Apple devices, including iPhones and iPads running iOS 16.6 and 15.7.8 [119]. In response, Apple swiftly released security patches to address the vulnerability, which was assigned a high severity score in the National Vulnerability Database (NVD) and designated with two Common Vulnerabilities and Exposures (CVE) identifiers: CVE-2023-41064 and CVE-2023-41061 [121].

The vulnerability's discovery occurred during a forensic device examination conducted by Citizen Lab experts. The device, belonging to an individual working for an international NGO, was found to be compromised by NSO Group's Pegasus spyware. The exploit involved sending a malicious PassKit attachment through iMessage [119]. Upon receipt and processing of the message, the device would execute the embedded malicious code, thereby compromising the device's security.

PassKit, an Apple-developed framework for creating and managing passes within the Wallet app, can handle sensitive data such as financial information and loyalty program details [202].While Citizen Lab has not publicly disclosed the technical specifics of the exploitation mechanism, it is noteworthy that the PassKit framework and the associated vulnerability were developed and maintained solely by Apple, without any third-party involvement. This underscores the potential for sophisticated spyware to exploit vulnerabilities even within first-party device frameworks, highlighting the ongoing challenges in ensuring the security of even the most tightly controlled operating systems.

A 5.2 KISMET

In December 2020, Citizen Lab researchers identified "Kismet," a zero-click vulnerability exploitable without any victim interaction [201]. This discovery stemmed from a journalist's suspicion of device compromise. Through network traffic and metadata analysis, researchers observed connections to an NSO Group Pegasus spyware installation server [201].

Further investigation revealed anomalous iCloud connections linked to Pegasus activity. The built-in iOS imagent process, associated with FaceTime and iMessage, was implicated in facilitating spyware operations [201]. Additionally, the infected device exhibited communication with previously unidentified IP addresses, employing obfuscation techniques to evade detection [201]. Device logs indicated kernel crashes during the suspected exploitation window, further supporting the presence of a vulnerability [201]. Citizen Lab's analysis linked these Pegasus operations to actors within the GCC, primarily targeting journalists amidst the ongoing Qatar-GCC crisis [201]. Notably, a rare opportunity to analyse a live infected device provided insights into the spyware's capabilities, which included audio recording, access to encrypted calls, camera activation, location tracking, and exfiltration of sensitive data [201].

While Kismet's zero-click nature, associated Pegasus server IPs, and unidentified root processes were confirmed [201]. the precise exploit mechanism remains undisclosed. This is common in vulnerability research, as investigators often analyse the aftermath of an attack rather than the exploit itself [201].

apple subsequently patched the vulnerability in iOS 14 but did not disclose further technical details, limiting public understanding and potentially hindering broader security enhancements [201].

This case study exemplifies the sophistication of modern spyware and the challenges associated with its detection and analysis. The ability to exploit zero-click vulnerabilities underscores the critical need for continuous research and development of robust security mechanisms to protect against such threats.

A 5.3 FORCEDENTRY

In August 2021, Citizen Lab and Red Line for Gulf disclosed a zero-click vulnerability affecting Apple's iOS operating system, designated FORCEDENTRY (CVE-2021-30860) [15] [203]. This exploit targeted the iMessage application, circumventing its BlastDoor sandbox protection by employing a maliciously crafted PDF file disguised as a GIF image[118, 158].

Analysis by Google Project Zero revealed that the exploit leveraged iMessage's image processing functionality, specifically the ImageIO framework, to trick the system into handling the malicious file [118]. The file contained a JBIG2-encoded stream, which triggered a crash in the IMTranscoderAgent, an Apple service responsible for processing image attachments within iMessage [120, 204]. This crash allowed the exploit to download and execute components of the Pegasus spyware [204, 205]. The entire exploitation process occurred silently and remotely, requiring only the victim's phone number for a successful attack [158]. Citizen Lab's investigation revealed that the exploit primarily targeted journalists in Bahrain, with GCC countries, mainly Saudi Arabia and the UAE, implicated as the primary operators of the Pegasus spyware.

It is crucial to note that all aspects of the FORCEDENTRY vulnerability involved Apple's first-party applications and services, raising concerns about the company's responsibility in ensuring device security [158]. This incident highlights the potential for sophisticated spyware to exploit vulnerabilities even within tightly controlled operating systems and emphasizes the need for continuous vigilance and proactive security measures.

A 5.4 TRIANGULATION

[15] [15] Amnesty name this vulnerability Megalodon

In June 2023, Kaspersky Lab discovered a sophisticated zero-click spyware attack, dubbed "Triangulation," targeting its employees [122]. This attack, initiated in 2019, involved the delivery of malicious iMessage attachments that exploited undisclosed vulnerabilities to escalate privileges and compromise devices. Kaspersky's subsequent investigation, detailed in an October 2023 report [206]. revealed suspicious communication patterns following the download of these iMessage attachments. Due to the spyware's memory-resident nature, researchers focused their analysis on device backups and network timestamps, identifying a suspicious "BackupAgent" process and evidence of file deletions [206, 207].

Attempts to intercept the malicious iMessage using a Frida script within a cloned environment proved unsuccessful [208]. However, researchers successfully decrypted command-and-control (C2) server communications using the mitmproxy tool, revealing a JavaScript validator and the attack payload [206].

Through meticulous retrieval and analysis of the malicious attachment and the implanted spyware, Kaspersky reconstructed the attack process. This process involved the delivery of a malicious iMessage attachment, subsequent processing by the device, redirection to a malicious website, validation checks, and finally, payload delivery to compromise the device [206].

Kaspersky's comprehensive report [92] provides valuable insights into the Triangulation attack, detailing their investigative methodology, including the development of custom analysis tools and the successful employment of "reverse cyber-kill chain" tactics to reconstruct the attack sequence. This research contributes significantly to the understanding of advanced spyware techniques and underscores the evolving challenges in mitigating such threats.

A 5.5 WhatsApp VOIP Vulnerability

In May 2019, Citizen Lab researchers confirmed a critical vulnerability (CVE-2019-3568) within WhatsApp, enabling remote code execution via specifically crafted Real-time Transport Control Protocol (RTCP) packets [209, 210]. This vulnerability, impacting both Android and iOS, originated within a third-party library rather than the operating system itself and was exploited by NSO Group's Pegasus spyware.

Attackers could install the spyware by simply initiating a call to the target's device, without requiring the call to be answered. While detailed technical information remains limited, analysis of WhatsApp's code suggests a buffer overflow vulnerability within the Secure RTCP (SRTCP) protocol, responsible for encrypting and ensuring the integrity of voice and video calls [211]. Researchers observed that the RTCP module was invoked upon call initiation, regardless of whether the call was answered [123]. Further reverse engineering revealed that manipulating packet sizes, controlled by the caller, could lead to integer underflows or overflows, triggering the vulnerability [124].

WhatsApp promptly addressed the vulnerability with a patch. However, Facebook, the parent company of WhatsApp, filed a lawsuit against NSO Group, accusing them of exploiting the vulnerability to compromise approximately 1,400 individuals on behalf of state actors [212]. WhatsApp also took the step of informing affected individuals about the state-sponsored attacks [125].

This incident highlights the potential for third-party libraries and applications to introduce vulnerabilities into otherwise secure systems. It also underscores the sophisticated tactics employed by state-sponsored actors to exploit such vulnerabilities for surveillance and espionage purposes.

A 6 How to Detect a Spyware

The detection of state-sponsored spyware presents significant challenges due to several factors:

1. **Resource Disparity:** Government-backed spyware initiatives benefit from substantial funding, attracting highly skilled developers and researchers with competitive salaries and extensive budgets for research and development. Their leadership often includes experienced intelligence professionals who prioritize operational security and leverage lessons learned from past operations to enhance the stealth and undetectability of their products. Furthermore, state actors can draw upon vast resources from both government agencies and the broader hacker community.
2. **Limited Resources for Counter-Spyware Efforts:** Conversely, research institutes and organizations dedicated to combating spyware often operate with limited resources,

personnel, and funding. The scarcity of entities invested in this domain further hinders their efforts to effectively counter the growing threat of state-sponsored spyware.

3. **Reactive Detection:** The success of spyware detection often relies on potential targets proactively seeking assistance from researchers or security experts. This reactive approach limits the ability to identify and mitigate threats before they are deployed, creating a significant disadvantage in the ongoing struggle against sophisticated spyware.

Despite these challenges, researchers have developed innovative methodologies based on their expertise and accumulated experience to detect and analyse spyware. These methodologies often involve a combination of network traffic analysis, forensic device examination, and reverse engineering techniques to uncover the presence and functionality of spyware, even in the face of sophisticated obfuscation and evasion tactics.

A 6.1 CitizenLab

Citizen Lab, a renowned research institute at the forefront of combating spyware, [126]. This methodology encompasses a range of techniques, including:

Network Scanning and Monitoring: Citizen Lab utilizes in-house tools to scan the internet for potential spyware servers, identifying instances of active spyware communication and the countries where these servers are located [213]. This proactive approach enables the identification of potential threats and the mapping of spyware infrastructure.

Targeted Monitoring: While identifying potential spyware targets remains a challenge, Citizen Lab leverages its extensive network of NGOs and activists to identify individuals who may be at risk [214]. Once identified, researchers utilize VPN clients and custom scripts to monitor and analyse network traffic for suspicious activity, detecting communication patterns between devices and known spyware servers [213].

Forensic Device Analysis: Citizen Lab conducts in-depth forensic examinations of devices suspected of being compromised by spyware. This includes analysing system logs, particularly the sysdiagnose file on iPhones, which contains valuable information about network

communication, installed applications, kernel crashes, folder modifications, and background processes [103]. However, the size and technical complexity of the sysdiagnose file can pose challenges for victims seeking to share it with Citizen Lab for analysis [103].

Automated Analysis Tools: To address this challenge, Citizen Lab developed a WhatsApp bot capable of receiving and analysing sysdiagnose files against known vulnerabilities, providing rapid results within minutes [103]. However, access to this bot is currently restricted to individuals and organizations within Citizen Lab's network. While Citizen Lab's efforts in exposing spyware usage and advocating for digital rights are commendable, access to their expertise and services can be challenging for individuals outside their established network of NGOs and activists. This limitation underscores the need for greater accessibility and broader dissemination of spyware detection and mitigation strategies to empower individuals and organizations to protect themselves against these threats.

14.0References

1. W.L. Liu, P.J. Kitchen and A. Moskovos, "Cypriot Parental Perceptions of Children's Internet Usage," *Euromed Journal of Business*, 2009; DOI 10.1108/14502190910992710.

2. M. Tözün and A. Bababoglu, "Cyber Bullying and Its Effects on the Adolescent and Youth Health: A Huge Problem Behind Tiny Keys," *The Annals of Clinical and Analytical Medicine*, 2018; DOI 10.4328/jcam.5426.

3. D.L. Hoffman, T.P. Novak and A. Venkatesh, "Has the Internet become indispensable?," *Commun. ACM*, vol. 47, no. 7, 2004, pp. 37–42; DOI 10.1145/1005817.1005818.

4. P. Chatzoglou, D. Chatzoudes and S. Symeonidis, "Factors affecting the intention to use e-Government services," *Proc. 2015 Federated Conference on Computer Science and Information Systems (FedCSIS)*, 2015, pp. 1489-1498.

5. M.J. Jensen, J.N. Danziger and A. Venkatesh, “Civil Society and Cyber Society: The Role of the Internet in Community Associations and Democratic Politics,” *The Information Society*, vol. 23, no. 1, 2007, pp. 39-50; DOI 10.1080/01972240601057528.

6. S. Kent, C. Lynn and K. Seo, “Secure Border Gateway Protocol (S-Bgp),” *Ieee Journal on Selected Areas in Communications*, 2000; DOI 10.1109/49.839934.

7. E.W. Lubua, A. Semlambo and P.D. Pretorius, “Factors Affecting the Use of Social Media in the Learning Process,” *Sa Journal of Information Management*, 2017; DOI 10.4102/sajim.v19i1.764.

8. J. Howell, “The Global War on Terror, Development and Civil Society,” *Journal of International Development*, 2005; DOI 10.1002/jid.1266.

9. F. Stories, *PEGASUS PROJECT | ALL THE ARTICLES*, Forbidden Stories, 2020.

10. A. Greenberg, “Hacking team breach shows a global spying firm run amok,” *Book Hacking team breach shows a global spying firm run amok*, Series Hacking team breach shows a global spying firm run amok, ed., Editor ed.^eds., 2015, pp.

11. R. DEIBERT, “Protecting Society from Surveillance Spyware,” *Issues in Science and Technology*, vol. xxxviii no 2, 2022.

12. P. Guest, “Spyware Finally Got Scary Enough to Freak Lawmakers Out—After It Spied on Them,” *bloomberg*, 2023.

13. N. PERLROTH, “How Spy Tech Firms Let Governments See Everything on a Smartphone,” *The New York Times*, 2016.

14. M.M.-B. Cora Currier, “Secret Manuals Show the Spyware Sold to Despots and Cops Worldwide,” *The Intercept*, 2014.

15. S. Kirchgaessner, “US defence contractor in talks to take over NSO Group’s hacking technology,” *Deal – which would require approval from US and Israel – would give L3Harris control over controversial Pegasus tool*, 19/09/2022 2022.

16. L. Franceschi-Bicchierai, “Startup Offers $3 Million to Anyone Who Can Hack the iPhone,” *Vice.com*, 2018.

17. P. Security, “The Cyber-Crime Black Market: Uncovered,” *Panda Security*, 2014.

18. A. Hern, “{Hacking Team hacked: firm sold spying tools to repressive regimes, documents claim,” 2015.

19. U.S.R.o.t.p.a.p.o.t.r.t.f.o.o.a. expression, *Surveillance and human rights - Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 2019.

20. S.F.a.B. Kot, “Mapping the Shadowy World of Spyware and Digital Forensics Sales,” 2023; Carnegie Endowment for International Peace.

21. I.T.I.i. Impact, “GCC Smartphone Market Report by Operating System (Android, iOS, and Others),” 2024.

22. E. Naprys, “Court finds Pegasus spyware maker NSO Group liable for hacking 1,400 WhatsApp users,” *cyberbews*, 2024.

23. A. International, *Gulf: Don’t believe the hype, GCC states are as repressive as they’ve ever been*, 2022.

24. M. Adwan, *The Animalism Of The Human Being*, 2007.

25. F. House, *Freedom in the World 2023*, 2023.

26. E. Morozov, *The Net Delusion: The Dark Side of Internet Freedom*, PublicAffairs, 2011.

27. R.G. Smith, “The Impact of Cybercrime on Victims: A Qualitative Study,” *Journal of Police and Criminal Psychology*, 2018.

28. C.C. Ragland, *Cybercrime Investigation and Digital Forensics*, SAGE Publications, 2018.

29. Amnesty, “New investigation shows global human rights harm of NSO Group’s spyware,” 2021; https://www.amnesty.org/en/latest/press-release/2021/07/investigation-maps-human-rights-harm-of-nso-group-spyware/.

30. S.A.A. Ahmadi, Kanaan Azar, Hossein, Nagahisarchoghaei, Mohammad, Nagahi, Morteza, "Relationship Between Emotional Intelligence and Psychological Well Being," *ORG: Positive Psychology & Organizational Behavior*, 2014.

31. G. King, Pan, J., Roberts, M. E., "Popular Support for the Chinese Communist Party: The Role of Online Public Opinion Manipulation," *Journal of Contemporary China*, 2018.

32. R. Ahmed, "Theorizing Surveillance in the Digital Age," *University of Westminster Press*, 2021.

33. J.W. Patchin, Hinduja, S., "Cyberbullying Research Summary: Bullying, Cyberbullying, and Sexual Harassment," *Cyberpsychology, Behavior, and Social Networking*, 2014.

34. J. Daciuk, Boersma, K., "Cyber Aggression: Prevalence, Predictors, and Social-Emotional Impact of Cyber Victimization in a University Sample," *Journal of Interpersonal Violence*, 2013.

35. M. Price, Dalgleish, T., "Cyberstalking, Self-Esteem, and Depressive Symptomatology: An Examination of Adult Cyberstalking Victims," *Journal of Anxiety Disorders*, 2012.

36. S.L. Trust, "Fighting for my sanity: Stalking and Post-Traumatic Stress Disorder," 2024; https://www.suzylamplugh.org/fighting-for-my-sanity-stalking-and-post-traumatic-stress-disorder.

37. N. Pereda and D.A. Díaz-Faes, "Family Violence Against Children in the Wake of COVID-19 Pandemic: A Review of Current Perspectives and Risk Factors," *International Journal of Environmental Research and Public Health*, vol. 16, 2019.

38. O.P. Almeida, et al., "Depression, antidepressants and the risk of cardiovascular events and death in older men," *Journal of Affective Disorders*, vol. 350, 2024.

39. L. Wegner, Holloway, B. E., Gordon, D. M., "Cyber Victimization and Psychological Distress: Examining the Moderating Role of Resilience," *Journal of Traumatic Stress*, 2017.

40. A. Sourander, Brunstein Klomek, A., Ikonen, M., Lindroos, J., Luntamo, T., Räsänen, P., "Psychosocial Risk Factors Associated with Cyberbullying among Adolescents: A Population-Based Study," *Depression and Anxiety*, 2013.

41. H.C. Woods, Scott, H., "Sleep and Bullying: A Systematic Review of the Literature," *Sleep Medicine*, 2016.

42. R.S. Tokunaga, "Following You Home from School: A Critical Review and Synthesis of Research on Cyberbullying Victimization," *Computers in Human Behavior* 2015.

43. Y. He, et al., "Exploring symptom-level associations between anxiety and depression across developmental stages of adolescence: a network analysis approach," *BMC Psychiatry*, vol. 23, no. 1, 2023, pp. 941; DOI 10.1186/s12888-023-05449-6.

44. T. Newman, "What connects depression, anxiety, and PTSD?," 2019; https://www.medicalnewstoday.com/articles/326903.

45. NHS, "Causes - Post-traumatic stress disorder," 2022.

46. B. Anwar, "PTSD Acute vs Chronic: What's the Difference?," 2023; https://www.talkspace.com/mental-health/conditions/articles/ptsd-acute-vs-chronic/.

47. Q. Li and J. Hu, "Post-traumatic Growth and Psychological Resilience During the COVID-19 Pandemic: A Serial Mediation Model," *Frontiers in Psychiatry*, 2022.

48. C. Mohiyeddini, Carlson, E., Sukhon, D., Almasri, W., Saad, M., Eshun, D., & Baker, S., "Moral Injury: A Theme in Search of Definition," *OBM Integrative and Complementary Medicine*, vol. 9, no. 4, 2024; DOI 10.21926/obm.icm.2404062.

49. N.C.f. PTSD, "Moral Injury," 2025; https://www.ptsd.va.gov/professional/treat/cooccurring/moral_injury.asp.

50. J. Subotic, & Steele, B. J., "Moral Injury in International Relations," *Journal of Global Security Studies*, vol. 3, no. 4, 2018; DOI 10.1093/jogss/ogy021.

51. H.G. Koenig, & Al Zaben, F., "Moral Injury: An Increasingly Recognized and Widespread Syndrome," *J Relig Health*, vol. 60, no. 5, 2021; DOI 10.1007/s10943-021-01328-0.

52. B. Stanton, et al., "Security Fatigue," *Discover Mental Health*, 2024.

53. F. Mizrak, H.G. Demirel and O.Y.T. Karakaya, "Digital detox: exploring the impact of cybersecurity fatigue on employee productivity and mental health," 2025.

54. C. Fletcher, "The Psychological Factors Behind Security Fatigue: A Deep Dive," 2024; https://chat.deepseek.com/a/chat/s/7b2dc59b-3136-446c-a2d7-6ab76a9c50b3.

55. L. Louër, *Transnational Shia Politics: Religious and Political Networks in the Gulf*, Columbia University Press, 2011.

56. C. Holes, *Modern Arabic: Structures, Functions, and Varieties*, Georgetown University Press, 2004.

57. D.F. Eickelman, *The Middle East: An Anthropological Approach*, Prentice Hall, 1981.

58. M. Al-Rasheed, *A History of Saudi Arabia*, Cambridge University Press, 2013.

59. A.K. Longva, *Walls Built on Sand: Migration, Exclusion, and Society in Kuwait*, Westview Press, 2012.

60. M. Herb, *The Wages of Oil: Parliaments and Economic Development in Kuwait and the UAE*, Cornell University Press, 2014.

61. M. Kamrava, *Qatar: Small State, Big Politics*, Cornell University Press, 2013.

62. K. Almezaini, "@ The Gulf Cooperation Council and the concept of collective security: A historical analysis," *Journal of Arabian Studies*, 2016.

63. S. Al-Owais, "Cybersecurity in the GCC: A Critical Assessment," *Journal of Information Warfare*, 2022.

64. G. Akkaya, "How the Gulf Cooperation Council Responded to the Arab Spring," *The World Community and the Arab Spring*, 2018; DOI 10.1007/978-3-319-60985-0_6.

65. L. Louër, "The Shiites of Bahrain: Political Participation and the Quest for Citizenship," Cambridge University Press, 2008.

66. C.M. Davidson, *After the Sheikhs: The Coming Collapse of the Gulf Monarchies*, Hurst & Company, 2012.

67. G. Hughes, "A 'model campaign'reappraised: the counter-insurgency war in Dhofar, Oman, 1965–1975," *Journal of Strategic Studies*, vol. 32, no. 2, 2009, pp. 271-305.

68. J. Kinninmont, *Kuwait's Parliament: An Experiment in Semi-democracy*, Chatham House London, UK, 2012.

69. R.W. Borders, "Reporters Without Borders (RSF) World Press Freedom Index 2023:," 2023; https://rsf.org/en/index.

70. D.J.S. Joyce Hakmeh, *Is the GCC Cyber Resilient?*, 2020.

71. J. Hakmeh, "Cybercrime Legislation in the GCC Countries," *Chatham house*, 2023.

72. R.F. Atkinson, John, "Accessing Hidden and Hard-to-Reach Populations: Snowball Research Strategies," *Social Research Update*, no. 33, 2001.

73. P. Biernacki, & Waldorf, D., "Snowball Sampling: Problems and Techniques of Chain Referral Sampling," *Sociological Methods & Research*, vol. 10, no. 2, 1981; DOI 10.1177/004912418101000205.

74. J.W. Creswell, & Poth, C. N., *Qualitative inquiry and research design: Choosing among five approaches*, SAGE Publications, 2018.

75. L.A. Palinkas, Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K., "Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research," *Administration and Policy in Mental Health and Mental Health Services Research*, vol. 42, no. 5, 2015; DOI 10.1007/s10488-013-0528-y.

76. S.J. Gentles, Charles, C., Nicholas, D., & Ploeg, J., "Reviewing the research on grounded theory and knowledge translation: An integrative review," *Journal of Advanced Nursing*, vol. 71, no. 8, 2015; DOI 10.1111/jan.12651.

77. G. Guest, K.M. MacQueen and E.E. Namey, *Applied Qualitative Data Analysis: A Practical Guide*, SAGE Publications, 2012.

78. A.L.a.D.G.A.a.J.P.T.a.C.M.a.P.C.G.a.J.P.A.I.a.M.C. and P. J. Devereaux and J. Kleijnen and D. Moher, "he PRISMA Statement for Reporting Systematic Reviews and Meta-Analyses of Studies That Evaluate Health Care Interventions: Explanation and Elaboration," *PLoS Medicine*, vol. 6, 2009; DOI 10.1371/journal.pmed.1000100.

79. V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, no. 2, 2006, pp. 77–101.

80. L.S. Nowell, et al., "Thematic analysis: Striving to meet the trustworthiness criteria," *International Journal of Qualitative Methods*, vol. 16, no. 1, 2017, pp. 1609406917733847.

81. N.U. Library, "Qualitative Rigor or Research Validity in Qualitative Research," *Book Qualitative Rigor or Research Validity in Qualitative Research*, Series Qualitative Rigor or Research Validity in Qualitative Research, ed., Editor ed.^eds., National University, 2023, pp.

82. J. Lukat, et al., "Psychometric properties of the Positive Mental Health Scale (PMH-scale)," *BMC Psychology*, vol. 4, no. 1, 2016, pp. 8; DOI 10.1186/s40359-016-0111-x.

83. C.J. Kemper and G. Laux, "Positive Mental Health: The Construction and Validation of a New Scale," *European Journal of Psychological Assessment*, vol. 23, no. 3, 2007, pp. 154-162.

84. S. Coulombe, Radziszewski, S., Trépanier, S.-G., Provencher, H., Roberge, P., Hudon, C., Meunier, S., Provencher, M. D., & Houle, J. , "Mental Health Self-Management Questionnaire," *Journal of Affective Disorders*, 2015.

85. M.A. Schwartz, R. Smith and J. Lish, "A Short Form of the Mental Health Self-Management Questionnaire," *Journal of Mental Health*, vol. 15, no. 6, 2006, pp. 723-731.

86. A. Anastasi and S. Urbina, *Psychological Testing*, Prentice Hall, 1997.

87. R.F. Mollica, et al., "The Harvard Trauma Questionnaire: Validating a Cross-Cultural Instrument for Measuring Torture Trauma and Posttraumatic Stress Disorder in Indochinese Refugees," *Journal of Nervous and Mental Disease*, vol. 180, no. 2, 1992, pp. 111-116.

88. P. Bolton and J.N. Mutamba, "The Harvard Trauma Questionnaire: A Critical Review," *Clinical Psychology Review*, vol. 34, no. 5, 2014, pp. 444-454.

89. P.-T. Integration, “Post-Traumatic Integration,” https://onlinematerial.posttraumatic-integration.eu/.

90. K.A. Fetters, L.A. Curry and J.W. Creswell, “Achieving Integration in Mixed Methods Designs—Principles and Practices,” *Health Serv. Res.*, vol. 48, no. 6pt2, 2013, pp. 2134–2156.

91. J.W. Creswell and V.L.P. Clark, *Designing and Conducting Mixed Methods Research*, SAGE Publications, 2017.

92. T. Guetterman, *Using Joint Displays to Integrate Qualitative and Quantitative Approaches*, International Institute for Qualitative Methodology, University of Alberta, 2019.

93. L.A. Palinkas and et al., “Mixed methods in implementation research: a systematic review and critical appraisal,” *Implement Sci.*, vol. 6, no. 1, 2011, pp. 21.

94. A. Tashakkori and C. Teddlie, *SAGE Handbook of Mixed Methods in Social & Behavioral Research*, SAGE Publications, 2010.

95. J.W. Creswell and J.D. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, SAGE Publications, 2018.

96. V.L.P. Clark and K. Sanders, “An Overview of the Use of Joint Displays in Mixed Methods Research,” *J. Mixed Methods Res.*, vol. 9, no. 2, 2015, pp. 179–192.

97. T.C. Guetterman, M.D. Fetters and J.W. Creswell, “Integrating Quantitative and Qualitative Results in Health Sciences Mixed Methods Research Through Joint Displays,” *Ann. Fam. Med.*, vol. 13, no. 6, 2015, pp. 554–561.

98. E.P.R. Service, *Pegasus Spyware: The Role of Forensic Evidence in Confirming Infections and its Impact on Victims' Psychological State and Advocacy Efforts*, European Parliament, 2022.

99. A.A. Kekre, *The Impact of Spyware on Human Rights Defenders: A Harm Assessment*, The Graduate Institute Geneva, 2024.

100. M. Foucault, *Discipline and Punish: The Birth of the Prison*, Vintage Books, 1995.

101. A.P.P.S.A.P.A. Pooley, *An Exploration of the Psychological Impact of Hacking Victimization*, ResearchGate, 2021.

102. S.A. Eldridge II and J. Steel, "From "flooding the zone" to "churnalism": The evolution of news industry discourses about journalism's crisis," *Journalism Practice*, vol. 13, no. 6, 2018; DOI 10.1080/17512786.2018.1555006.

103. B. Inkster, C. Knibbs and M. Bada, "Cybersecurity: a critical priority for digital mental health," *Front Digit Health*, vol. 5, 2023; DOI 10.3389/fdgth.2023.1242264.

104. E.Z. Bell, Ethan; Stray, Jonathan; Coronel, Shelia; Schudson, Michael *Comment to Review Group on Intelligence and Communications Technologies Regarding the Effects of Mass Surveillance on the Practice of Journalism*, 2013.

105. J. Laidler, "High tech is watching you," 2019; https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/.

106. M. De Witte, "Hoover initiative addresses the erosion of trust in American institutions," 2025; https://news.stanford.edu/stories/2025/01/hoover-initiative-addresses-the-erosion-of-trust-in-american-institutions.

107. I. Tarnowski, "How to use cyber kill chain model to build cybersecurity?," *European Journal of Higher Education IT*, 2017.

108. M. Theoharidou, A. Mylonas and D. Gritzalis, "A Risk Assessment Method for Smartphones," 2012; DOI 10.1007/978-3-642-30436-1_36.

109. A.a. Silberschatz, *Operating system concepts／Abraham Silberschatz, Peter Baar Galvin, Greg Gagne*, Wiley, 2019.

110. W.R. Marczak, et al., "When governments hack opponents: A look at actors and technology," *Proc. 23rd USENIX Security Symposium (USENIX Security 14)*, 2014, pp. 511-525.

111. S. Yoon and Y. Jeon, “Security threats analysis for Android based Mobile Device,” *Proc. 2014 International Conference on Information and Communication Technology Convergence (ICTC)*, 2014, pp. 775-776.

112. B. Yee, et al., “Native Client: A Sandbox for Portable, Untrusted X86 Native Code,” 2009; DOI 10.1109/sp.2009.25.

113. T.P. Nguyen, Zheng, C., & DeLoach, S. A., “A study of app permissions in Android and iOS: How many permissions are needed and why?,” 2019.

114. K.M. Awan, et al., “Resource Management and Security Issues in Mobile Phone Operating Systems: A Comparative Analysis,” 2017; DOI 10.7287/peerj.preprints.3344v1.

115. A. Gurung, X. Luo and Q. Liao, “Consumer Motivations in Taking Action Against Spyware: An Empirical Investigation,” *Information Management & Computer Security*, 2009; DOI 10.1108/09685220910978112.

116. Y. Ye, et al., “CIMDS: Adapting Postprocessing Techniques of Associative Classification for Malware Detection,” *Ieee Transactions on Systems Man and Cybernetics Part C (Applications and Reviews)*, 2010; DOI 10.1109/tsmcc.2009.2037978.

117. E. Eide, “Chilling Effects on Free Expression: Surveillance, Threats and Harassment,” 2019, pp. 227-242.

118. I. Beer and S. Groß, “A deep dive into an NSO zero-click iMessage exploit: Remote Code Execution,” *Book A deep dive into an NSO zero-click iMessage exploit: Remote Code Execution*, Series A deep dive into an NSO zero-click iMessage exploit: Remote Code Execution, ed., Editor ed.^eds., URl: https://googleprojectzero. blo gspot. com/2021/12/a-deep-dive-into-nso ..., 2021, pp.

119. C. Lab, “BLASTPASS: NSO Group iPhone Zero-Click, Zero-Day Exploit Captured in the Wild,” 2023.

120. B. Marczak, et al., *FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild*, 2021.

121. NIST, "CVE-2023-41061 Detail," 2023.

122. V.P. IGOR KUZNETSOV, LEONID BEZVERSHENKO, GEORGY KUCHERIN, "Operation Triangulation: iOS devices targeted with previously unknown malware," *SecureList by kaspersky*, 2023.

123. checkpoint, "THE NSO WHATSAPP VULNERABILITY – THIS IS HOW IT HAPPENED," *Check Point*, 2019.

124. C. Tamir, "WhatsApp Buffer Overflow Vulnerability: Under the Scope," *zimperium*, 2019.

125. E.C. John Scott-Railton, 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," *Citizen Lab*, 2022.

126. C. Lab, "The Citizen Lab Booklet," *Citizen Lab*.

127. P. Bhandari, "Ethical considerations in research| Types & examples," *Retrieved*, vol. 1, no. 18, 2021, pp. 2023.

128. U.o. York, *Research Data Management policy*, 2025.

129. U.o. York, *Research Ethics*, 2025.

130. U.o. York, *Code of Practice on Research Integrity*, 2025.

131. U.D. Service, "Data Protection Act and GDPR," 2023; https://ukdataservice.ac.uk/learning-hub/research-data-management/data-protection/data-protection-legislation/data-protection-act-and-gdpr/.

132. B. Barry, *Social work and the ethics of human service*, Oxford University Press, 2019.

133. British Psychological Society, *Code of ethics and conduct*, 2021.

134. H.L.A. Hart, *The Concept of Law*, Oxford University Press, 2012.

135. O.o.t.U.N.H.C.f.H.R. (OHCHR), "International Human Rights Law," https://www.ohchr.org/en/instruments-and-mechanisms/international-human-rights-law.

136. E.C.f.C.a.H.R. (ECCHR), "Hard law/soft law," https://www.ecchr.eu/en/glossary/hard-law-soft-law/.

137. L.L. Fuller, *The Morality of Law*, Yale University Press, 1964.

138. T.A. Birkland, *An introduction to the policy process*, Routledge, 2019.

139. M.R. Howlett, M. Perl, A., *Studying public policy*, Oxford UP, 2020.

140. N.I.o.S.a.T. (NIST), *Cybersecurity policy fundamentals*, SP 800-12 Rev. 1, 2021.

141. T.R. Dye, *Understanding public policy*, Pearson, 2017.

142. C.M. Chinkin, "The challenge of soft law: Development and change in international law," *The International and Comparative Law Quarterly*, vol. 38, no. 4, 1989.

143. R.J. Deibert, *Reset: Reclaiming the Internet for Civil Society*, House of Anansi Press, 2019.

144. U.H.R. Council, *Report on the right to privacy in the digital age*, A/HRC/48/31, 2021.

145. F. Patel, "Weaponizing surveillance: Spyware and authoritarian entrenchment."," *Weaponizing surveillance: Spyware and authoritarian entrenchment." International Security*, 2023.

146. *Universal Declaration of Human Rights,* U.N. Doc A/810.

147. H. Hannum, "The Status of the Universal Declaration of Human Rights in National and International Law," *Georgia Journal of International and Comparative Law*, vol. 25, no. 1-2, 1995.

148. B. Simma and P. Alston, "The Sources of Human Rights Law: Custom, Jus Cogens, and General Principles," *Australian Year Book of International Law*, vol. 12, 1992.

149. H.R. Council, *The right to privacy in the digital age*, 2022.

150. *The right to privacy in the digital age*.

151. B. Room, "Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware," *Book Joint Statement on Efforts to Counter the Proliferation and Misuse of*

Commercial Spyware, Series Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware, ed., Editor ed.^eds., 2023, pp.

152. E. Parliament, *Report on the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware*, 2023.

153. *European Parliament recommendation of 15 June 2023 to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware*, 15/06/2023.

154. J. Goldsmith and T. Wu, *Who Controls the Internet? Illusions of a Borderless World*, Oxford University Press, 2006.

155. S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, 2019.

156. NSO Group, *HUMAN RIGHTS POLICY*, 2021.

157. U. Nations, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, 2011.

158. A.A. Bill Marczak, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, John Scott-Railton, and Ron Deibert, "From Pearl to Pegasus

Bahraini Government Hacks Activists with NSO Group Zero-Click iPhone Exploits," 2021.

159. J.S.-R. Bill Marczak, Noura Al-Jizawi, Siena Anstis, and Ron Deibert, "The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit," 2020.

160. J.S.-R. Bill Marczak, and Ron Deibert, "Independently Confirming Amnesty Security Lab's finding of Predator targeting of U.S. & other elected officials on Twitter/X," *Citizen Lab*, 2023.

161. J. Penney, "Chilling Effects: Online Surveillance and Wikipedia Use," *Berkeley Technology Law Journal*, vol. 31, no. 1, 2016.

162. M. Kremnitzer and Y. Shany, "Exporting Oppression? Regulating the Export of Cyber-Surveillance Technologies from Israel," *Israel Law Review*, vol. 54, 2021.

163. M. Eriksson and V. Stenport, “Regulating the Trade in Intangibles: The Case of EU Export Controls on Cyber-Surveillance Technology,” *Journal of Contingencies and Crisis Management*, vol. 25, no. 4, 2017.

164. T. Staff, “Israel said to drastically slash number of countries allowed to buy cyber-tech,” *Book Israel said to drastically slash number of countries allowed to buy cyber-tech*, Series Israel said to drastically slash number of countries allowed to buy cyber-tech, ed., Editor ed.^eds., 2021, pp.

165. U.S. Department of Commerce, “Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities,” 2021; https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list.

166. S. Kirchgaessner, “WhatsApp sues Israeli firm NSO Group over alleged spyware attack,” *Book WhatsApp sues Israeli firm NSO Group over alleged spyware attack*, Series WhatsApp sues Israeli firm NSO Group over alleged spyware attack, ed., Editor ed.^eds., The Guardian, 2019, pp.

167. *WhatsApp Inc. v. NSO Group Technologies Ltd.,* vol. No. 3:19-cv-07123, 2019 (United States District Court for the Northern District of California).

168. K.K. Paskal, “Foreign Sovereign Immunity and Private Spyware,” *Harvard Law Review*, vol. 136, no. 5, 2023.

169. H. belson, et al., “Keys under doormats: Mandating insecurity by requiring government access to all data and communications,” *Journal of Cybersecurity*, vol. 1, 2015.

170. D.E. Pozen, “Transparency's Ideological Drift,” *Yale Law Journal*, vol. 128, no. 1, 2018.

171. K. Klonick, “The New Governors: The People, Rules, and Processes Governing Online Speech,” *Harvard Law Review*, vol. 131, no. 6, 2018.

172. B. Schneier, *Data and Goliath: The hidden battles to collect your data and control your world*, W. W. Norton & Company, 2015.

173. M. Al-Qahtani, “The Legal Framework of Cybersecurity in the Gulf Cooperation Council: A Critical Analysis of Cybercrime Legislation and its Impact on Human Rights,” *International Review of Law, Computers & Technology*, vol. 36, no. 2, 2022.

174. A. Al-Dhaqm and M. Al-Hashedi, “National Security Exemptions in GCC Data Protection Laws: Implications for Privacy and State Surveillance,” *Journal of Information Privacy and Security*, vol. 19, 2023.

175. H.R. Watch, *World Report 2024: Saudi Arabia (Country Chapter)*, 2024.

176. H.R. Watch, “UN Censors Criticism of Saudi Arabia at Internet Conference,” 2025; https://www.hrw.org/news/2025/02/06/un-censors-criticism-saudi-arabia-internet-conference.

177. A. International, “Qatar: New cybercrimes law endangers freedom of expression,” 2014; https://www.amnesty.org/en/latest/news/2014/09/qatar-new-cybercrimes-law-endangers-freedom-expression/.

178. A. International, “UAE: Concerns around authorities’ use of digital surveillance during COP28,” 2023; https://www.amnesty.org/en/latest/news/2023/11/uae-concerns-around-authorities-use-of-digital-surveillance-during-cop28/.

179. V. Kavaleff and D. Peterson, “Al-Masarir v Saudi Arabia: A route to state accountability for spyware,” 2022; https://www.ejiltalk.org/al-masarir-v-saudi-arabia-a-route-to-state-accountability-for-spyware/.

180. H.S.F. Kramer, “Crossing Digital Borders: The English Court of Appeal's Ruling in Shehabi v Bahrain,” *Book Crossing Digital Borders: The English Court of Appeal's Ruling in Shehabi v Bahrain*, Series Crossing Digital Borders: The English Court of Appeal's Ruling in Shehabi v Bahrain, ed., Editor ed.^eds., 2024, pp.

181. C. Ryngaert, *Jurisdiction in International Law*, Oxford University Press, 2015.

182. P. International, “R (on the application of Privacy International) v. The Commissioner for HM Revenue & Customs (Gamma FinFisher Exports),” 2013; https://privacyinternational.org/legal-action/r-application-privacy-international-v-commissioner-hm-revenue-customs-gamma-finfisher.

183. S.M. Berthold, et al., “The HTQ-5: revision of the Harvard Trauma Questionnaire for measuring torture, trauma and DSM-5 PTSD symptoms in refugee populations,” *European Journal of Public Health*, vol. 29, no. 3, 2018, pp. 468-474; DOI 10.1093/eurpub/cky256.

184. p.o.H.T. Questionnaire, “Harvard trauma questionarre,” https://onlinematerial.posttraumatic-integration.eu/.

185. D. George and P. Mallery, *SPSS for Windows step by step: A simple guide and reference*, Allyn & Bacon, 2003.

186. A. Ehlers, & Clark, D. M. , “A cognitive model of posttraumatic stress disorder,,” *Behaviour Research and Therapy*, vol. 38, 2000; DOI 10.1016/s0005-7967(99)00123-0.

187. M. Shelton, “Research Methods With Media Activists Under Surveillance,” 2016; https://mshelton.medium.com/research-methods-with-media-activists-under-surveillance-979cef44fa55.

188. K.M. Kareem, “A Comprehensive Analysis of Pegasus Spyware and Its Implications for Digital Privacy and Security,” *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 3, 2024.

189. J.R. Volllhardt, *The Social Psychology of Collective Victimhood*, Oxford University Press, 2020.

190. M. Button, C. Cross and R.G. Smith, *Cyber-victimology: An Examination of the Psycho-Social and Economic Harms of Cybercrime*, Routledge, 2022.

191. E. Newman and D. Scott, *Reporting on Trauma: A Guide for Journalists, Students, and Educators*, Routledge, 2021.

192. S. Anstis and R. Deibert, “Silenced by Surveillance: The Impacts of Digital Transnational Repression on Journalists, Human Rights Defenders, and Dissidents in Exile,” 2025; https://knightcolumbia.org/content/silenced-by-surveillance-the-impacts-of-digital-transnational-repression.

193. M. Winters, “International Human Rights Legal Compliance Must Be At the Center of Multilateral Regulation of Commercial Spyware,” *Minnesota Journal of International Law*, 2025.

194. F.N. Aoláin and A.E. Jones, “Spyware Out of the Shadows: The Need for A New International Regulatory Approach,” 2023.

195. E. Ahmed, & Atamni, H. , “smartphone security: A survey of current trends and future directions.,” *Journal of Internet Services and Applications,*, 2021.

196. S. Zhang, et al., “How Usable Are iOS App Privacy Labels?,” *Proceedings on Privacy Enhancing Technologies*, 2022; DOI 10.56553/popets-2022-0106.

197. R. Balebako, et al., “The Privacy and Security Behaviors of Smartphone App Developers,” 2014; DOI 10.14722/usec.2014.23006.

198. M. Compastié, et al., “From Virtualization Security Issues to Cloud Protection Opportunities: An in-Depth Analysis of System Virtualization Models,” *Computers & Security*, 2020; DOI 10.1016/j.cose.2020.101905.

199. A. Armando, A. Merlo and L. Verderame, “Security Issues in the Android Cross-Layer Architecture,” 2012; DOI 10.48550/arxiv.1209.0687.

200. A. Quattrone, Kulik, L., Tanin, E., & Ramamohanarao, K. , “PrivacyPalisade: Evaluating App Permissions and Building Privacy into Smartphones.,” *Book PrivacyPalisade: Evaluating App Permissions and Building Privacy into Smartphones.*, Series PrivacyPalisade: Evaluating App Permissions and Building Privacy into Smartphones., ed., Editor ed.^eds., 2015, pp.

201. J.S.-R. Bill Marczak, Noura Al-Jizawi, Siena Anstis, and Ron Deibert, “The Great iPwn Journalists Hacked with Suspected NSO Group iMessage ‘Zero-Click’ Exploit,” *Citizen Lab*, 2020.

202. Apple, “PassKit (Apple Pay and Wallet),” 2023.

203. A. International, “Forensic Methodology Report: How to catch NSO Group’s Pegasus,” 2021; https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/.

204. M. Suiche, “Researching FORCEDENTRY: Detecting the Exploit With No Samples,” *Magnet Forensics*, 2022.

205. M. Labs, “Latest iPhone exploit, FORCEDENTRY, used to launch Pegasus attack against Bahraini activists,” 2021.

206. G.K. LEONID BEZVERSHENKO, IGOR KUZNETSOV, BORIS LARIN, “How to catch a wild triangle,” 2023.

207. S.b. Kaspersky, “In search of the Triangulation: triangle_check utility,” 2023.

208. g.p. zero, “Ios Messaging Tools,” 2019; https://github.com/googleprojectzero/iOS-messaging-tools/blob/master/iMessage/dumpIncomingMessages.py.

209. M. Srivastava, “WhatsApp voice calls used to inject Israeli spyware on phones,” *Financial Times*, 2019.

210. N.V. Database, “CVE-2019-3568 Detail,” 2019.

211. E.a. Meta, “Enhancing the security of WhatsApp calls,” 2023; https://engineering.fb.com/2023/11/08/security/whatsapp-calls-enhancing-security/.

212. Gadgets360, “Facebook Can Pursue Malware Lawsuit Against Pegasus Maker NSO Group: US Appeals Court,” 2021; https://www.gadgets360.com/apps/news/facebook-meta-pegasus-nso-group-lawsuit-whatsapp-hack-spyware-us-appeals-court-2604175.

213. B. Marczak, “ByteCheck,” 2020; https://github.com/billmarczak/bytecheck.

214. S. Planner, “Keep Your Data Secure With a Personalized Plan,” https://securityplanner.consumerreports.org/.