University of Piraeus
School of Information and Communication Technologies
Department of Digital Systems

Master Thesis

Spyware Technologies: Technical Analysis, Detection and Countermeasures

Pappas Nikolaos

MTE2219

Supervisor:

Gritzalis Stefanos, Professor

Peiraeus, 2025

Abstract

The spread of sophisticated spyware like Pegasus and Predator causes dangers to digital privacy, human rights along with democratic processes. Both spyware have been linked to the targeting of journalists, activists and political figures around the world. This paper studies how government sponsored surveillance software works, how people use it as well as what it means for society and digital rights. Through a combined approach of cybersecurity forensics, legal frameworks and geopolitical analysis it assesses the global impact of these tools and focuses on ways people can protect themselves individually and collectively.

The paper highlights specific case studiues that demonstrate real-world detection techniques and consequences. It uses reports from groups and organizations like Citizen Lab and Amnesty International's Security Lab. Several tools are developed and help link infections to their source and help those affected. By examining the similarities and differences between Pegasus and Predator, this thesis aims to raise awareness about the dangers of modern spyware.

The thesis concludes by recommending a multi-tiered response framework involving legal reform, public awareness, and international cooperation to combat unlawful surveillance. The right to privacy is reaffirmed as essential to the preservation of human dignity and civil liberty in the digital age.

Keywords: Spyware, Pegasus, Predator, Surveillance, Privacy, Cybersecurity, Detection, Legal Ethics

Περίληψη

Η εξάπλωση εξελιγμένων λογισμικών κατασκοπείας όπως το Pegasus και το Predator προκαλεί κινδύνους για την ψηφιακή ιδιωτικότητα, τα ανθρώπινα δικαιώματα, καθώς και τις δημοκρατικές . Και ται τα δύο λογισμικά κατασκοπείας έχουν συνδεθεί με τη στοχοποίηση δημοσιογράφων, ακτιβιστών και πολιτικών προσωπικοτήτων σε όλο τον κόσμο. Η παρούσα εργασία μελετά πώς λειτουργεί το κυβερνητικά χρηματοδοτούμενο λογισμικό παρακολούθησης, πώς το χρησιμοποιούν οι άνθρωποι, καθώς και τι σημαίνει για την κοινωνία και τα ψηφιακά δικαιώματα. Μέσω μιας συνδυασμένης προσέγγισης εγκληματολογίας στον κυβερνοχώρο, νομικών πλαισίων και γεωπολιτικής ανάλυσης, αξιολογεί τον παγκόσμιο αντίκτυπο αυτών των εργαλείων και εστιάζει σε τρόπους με τους οποίους οι άνθρωποι μπορούν να προστατεύσουν τον εαυτό τους ατομικά και συλλογικά.

Η εργασία αναφέρει συγκεκριμένες μελέτες που καταδεικνύουν τις τεχνικές ανίχνευσης και τις συνέπειες στον πραγματικό κόσμο. Χρησιμοποιεί αναφορές από ομάδες και οργανισμούς όπως το Citizen Lab και το Security Lab της Διεθνούς Αμνηστίας. Εξετάζοντας τις ομοιότητες και τις διαφορές μεταξύ του Pegasus και του Predator, η παρούσα εργασία στοχεύει στην ευαισθητοποίηση σχετικά με τους κινδύνους του σύγχρονου λογισμικού κατασκοπείας.

Η εργασία ολοκληρώνεται προτείνοντας ένα πολυεπίπεδο πλαίσιο απόκρισης που περιλαμβάνει νομική μεταρρύθμιση, ευαισθητοποίηση του κοινού και διεθνή συνεργασία για την καταπολέμηση της παράνομης παρακολούθησης. Το δικαίωμα στην ιδιωτικότητα είναι απαραίτητο για τη διατήρηση της ανθρώπινης αξιοπρέπειας και της πολιτικής ελευθερίας στην ψηφιακή εποχή.

Λέξεις-κλειδιά: Spyware, Pegasus, Predator, Παρακολούθηση, Ιδιωτικότητα, Κυβερνοασφάλεια, Εντοπισμός, Νομική Ηθική

Acknowledgments

I would like to thank my supervisor Mr. Stefanos Gritzalis for its guidance and the president and the department secretariat for their support and resilience through this endeavor.

Table of Contents

List of tables

List of Acronyms

EU: European Union
NSO: NSO Group
C2: Command and Control

Chapter 1: Surveillance and Spyware – Evolution, Concepts, and Context

1.1 Origins of Surveillance

Surveillance is the practice of observing, monitoring, or collecting data about individuals or groups. Before the development of digital technologies, surveillance was essential for law enforcement, geopolitical strategy, and governance. In its earliest forms, surveillance was anthropocentric and physical: emperors, kings, and generals sent spies to spy on their enemies and infiltrate rival territories or find internal dissenters.

Organized ways to watch people started when states grew in the 1700s. France put in place ways to track its people. Jeremy Bentham's Panopticon idea also came about then. This was a prison layout where guards could see prisoners, but the prisoners did not know when someone watched them. The Panopticon became a symbol for societies that watch their people.

The practice of surveillance was institutionalized in the 20th century. Official agencies were established by governments to collect information and monitor communications. From wiretapping and physical observation to more sophisticated electronic surveillance, these systems developed alongside technology. Secret police networks also began to form to monitor and suppress dissent. Under the guise of national security, surveillance increased even in democracies.

The foundations for modern digital surveillance systems were laid with early surveillance methods, which relied on human intelligence and physical observation. Despite the evolution of tools, the logic of power, visibility, and control has not changed.

1.2 Digital Transformation of Surveillance

The shift from analog to digital methods increased the size and reach of surveillance. Surveillance operates through data networks, digital devices along with automated systems - it does not depend on a person's physical presence or direct interception. This change altered the people involved in surveillance, the locations it reaches, plus the methods it uses.

Many data collection methods became available because smartphones, internet connected devices, and cloud services became common. Each day, people generate also store a lot of personal information - this includes communications, locations as well as behaviors. People can watch this data, and the user may not know it.

Digital surveillance comes in three primary forms:

- **Mass surveillance** collects information from many people without a specific cause. For example, authorities intercept internet traffic or mobile metadata in large quantities.
- **Targeted surveillance** focuses on specific people or groups, often for national security or law enforcement. Spyware and interception tools generally apply here.
- **Predictive surveillance** uses machine learning plus analysis of big data to forecast human actions or future dangers. This method finds increasing use in areas such as border control and predicting crime.

The big change occurred after the September 11, 2001 terrorist attacks in the United States. Governments across the globe increased their surveillance powers allegiantly to fight terrorism. For example, the USA PATRIOT Act let intelligence agencies gather data with less supervision. Programs such as PRISM, which Edward Snowden later uncovered, showed how digital talks were spied on with the help of technology businesses. During this time, widespread data surveillance became common, and better tools appeared quickly.

There are many players on the surveillance universe today:

- Governments and intelligence groups use observation for national security, to stop terrorism along with to keep order among people.
- Some companies, like those in technology plus advertising, gather and study user details for business reasons; they sometimes work with state groups.
- Criminals on the internet use observation tools, like programs that record what people type or ways to access computers from far away. They do this to steal, to watch people, or to threaten them.

The tools used for digital observation are many, also they grow more complex. Some of these are:

- **Spyware programs** that watch people's computers - these programs go into devices quietly and take out private information or watch what a person does (for example the keylogger programs)
- **Big data analytics**. This method collects as well as understands big sets of information to find patterns or actions.
- **Social media monitoring** or social media reverse engineering, which means following public and private posts, messages as well as actions on different websites.

- **Location tracking.** Devices like phones plus apps use GPS and network methods to show a person's spot.
- **Biometric systems**, such as face scanners or finger readers. People often set these up in public places to watch others or to check who someone is.

Digital surveillance works well because it stays hidden and continues over time. The spyware program runs without notice and sends live information.

To sum up, the digital era has changed surveillance. It is a field that uses complex technology and it involves both state and non state players. It also raises severe ethical and security concerns.

1.3 What is Spyware?

Spyware is a kind of software designed to secretly monitor and collect data from a device without the user's knowledge or consent. Its main objective is to monitor its target, regardless of whether it is for governmental, commercial, or illicit purposes. It accomplishes this by multiple ways, either by activating cameras or microphones, either by accessing the data stored in the target.

Spyware software gain illegal access to a device by either exploiting vulnerabilities in the core system or applications or can be installed by the target user if he/she was mislead. It may remain inactive after its installation and can transmit data to the attacker periodically or in real time.

Spyware is a type of software that secretly watches a device - it gathers data from a device without a user knowing or agreeing. It is used for surveillance, such as for a crime, business, or government. It obtains data like messages, call records, or the device's location - it also gets browser activity. A user can remotely turn on microphones and cameras.

Spyware shows a range of details and uses. At its most basic level, it includes simple tracking software used for advertising or for managing devices. More complex types, like Pegasus or Predator, are sophisticated tools sometimes called state grade spyware - these programs get around encrypted messaging applications; they also use zero day flaws. A device does not show any signs when these programs operate.

The spyware softwares collects contacts, messages, emails, photos along with documents - it monitors what a person does in real time. The program accesses the microphone, camera, or screen. It also tracks the person's location. The program uses GPS or the network to follow movement.

With the software, a person can control a device from far away; they can execute commands or change settings. The program updates itself. This lets it adjust to system changes or reinfect a device. The software works without anyone knowing - it avoids discovery by users or security programs.

Spyware is generally categorized based on what its use:

Commercial type of spyware is legally sold to parents to watch their children. Employers use it to check on their workers. People also use it to get back a device.

State-sponsored spyware is built for information gathering and to protect a country against internal or external threats. Governments often use it against terrorism, to watch political groups or for law enforcement.

Criminal spyware serves to steal a person's identity - it also helps commit fraud, or it extorts money.

In the 21st century mobile phones are thriving, so spyware engineers target more and more these devices. The most common devices that are targeted are Android and iOS phones. Modern spyware can infect a phone with zero clicks, which means it can get on a device without the person doing anything.

To sum up, spyware is not one kind of program but a large group of watching tools. It can be categorized by its usage and its complexity. Knowing about its different types and what it can do helps analyze current threats. Pegasus and the most recent one Predator are some of the most complex spyware software used in our days.

1.4 Evolution and Classification of Spyware

From Keyloggers to Zero-Click Spyware

Spyware evolved much in years. At first, it was basic, like keyloggers. These programs kept a record of what people typed on a device and sent it to someone who attacked the system. People often put them on computers by touching the machine or through simple bad software. Attackers used them to take passwords, emails along with account names.

As computers became safer, spyware got more complex. When remote access tools appeared, attackers could control devices; they captured screen images or used webcams. As mobile phones were introduced to our everyday life spyware targeted mobile devices.

Programs like Pegasus andPredator show the most advanced forms of spyware. These tools use newly found flaws to infect a device without anyone clicking anything. In comparison to older spyware software, this kind of spyware stays hidden - it is hard to detect, and can monitor a person's phone calls, texts, location, camera as well as microphone at the moment things happen.

Commercial Spyware vs. State-Sponsored Spyware

Spyware is divided into two general types.

The first type is **commercial spyware**. People buy these legal products for purposes such as parental control, observing employees, or tracking stolen items. While companies sell them as legitimate products, people may misuse these tools in domestic abuse situations, stalking, or spying without permission. Some examples are mSpy in addition to FlexiSPY.

The second type is **state sponsored spyware**. Companies develop and deploy this spyware when they sell it to governments. This spyware helps with intelligence, law enforcement along with national security work - it has more power and can get around encryption or reach almost all device functions from a distance. From NSO Group as well as Predator, from Cytrox/Intellexa, are examples of this type. Governments often say they use these tools to fight terrorism or organized crime. Using them against journalists, people who disagree with the government, and political opponents caused worries across the world.

Android vs. iOS Targeting

Engineers who build spyware software mostly concentrate on Android and iOS which are the two main mobile operating systems. But the ways they work differ a lot, because of their different architecture and design.

Android devices often become targets more easily, because their system is fragmented. The various manufacturers, irregular update times, and different security settings render Android more open to attack.

iOS devices have tighter security rules plus a more consistent and uniformed system, so people find them harder to attack. When an attack succeeds, which often happens through flaws that need no user action in programs like iMessage or FaceTime, the spyware can get deep access, because users generally trust Apple's security and may act less carefully.

Complex spyware tools work on both systems. But to get into iOS devices, which have better defenses, the tools often use costly and uncommon attack methods.

Passive vs. Active Data Collection

Spyware can also be classified based on how it gathers data:

Passive spyware mostly watches and records user actions without direct involvement - it records browsing habits, GPS coordinates, or messages in the background over time. It sends the data quietly to an outside server.

Active spyware acts on the device immediately. It turns on the microphone, takes pictures, changes system files, or sends orders from afar. This type of spyware enters further into the system. State-sponsored tools usually contain it because it offers the attacker complete control of the target device.

1.5 Infection Vectors and Delivery Methods

Mobile surveillance tools such as **Pegasus and Predator** use several infection methods to get into target devices. The methods they use vary from user exploitation to complex exploits that need no action.

Social Engineering

Social engineering is an old, effective tactic in digital surveillance - it persuades the target to take an action that compromises their device, often by using trust, curiosity,

fear, or urgency. With spyware, this could mean getting a user to install an app that appears harmless but holds hidden spyware.

Attackers also send messages that look like system alerts or official notices; they may pretend to be trusted contacts to get people to act in risky ways. Even though advanced spyware uses technical flaws, social engineering is a common way to spread it, especially with less complex or commercial spyware products.

Phishing

Phishing is a type of social engineering where an attacker sends messages to trick people - these messages often come by email, text, or messaging applications. The attacker wants users to click bad links or download files that have a virus.

The malicious links can lead to several places. People may go to fake login pages that collect their usernames and passwords. The files might contain spyware. Other websites launch an attack when they load - people call these "drive-by downloads."

There are reports that prove that some versions of Pegasus and Predator, used phishing links. These links looked like news stories, government warnings, or cloud storage links. Phishing is a cheap and common way to begin spyware attacks, especially when attackers cannot find new vulnerabilities.

Exploit Chains and Zero-Day Vulnerabilities

Avanced spyware software also use exploit chains - these chains consist of a series of software flaws linked together to obtain total access to a device. They often target mobile operating systems like iOS or Android, so attackers can get around common security measures such as sandboxing or code signing.

Zero-day vulnerabilities are flaws that a software seller does not know about, and no fix exists for them. They offer a good chance of a successful, unseen break in. Because of this, they are of great value. People sometimes sell them for millions of dollars on the black market, or governments save them for their own use.

Pegasus has used several zero days in one attack chain - it raises its access until it controls the device completely, often without the user knowing.

Zero-Click Attacks

The zero click attack is a sophisticated delivery method. They are hard to find and require zero interaction of the target. The spyware is delivered and run quietly. It typically uses weaknesses in messaging applications or operating system services.

For example, an attacker can use iMessage to send a certain infected message. This message then infects the device when it is delivered. No user interaction is necessary. An attacker might also use WhatsApp application vulnerabilities. The spyware installs even if a person does not answer the call.

Zero-click attacks are hard to find and stop mainly because they leave little to no evidence. Forensic checks often uses indirect signs. These signs include odd system actions, strange data transfer and system anomalies.

To sum up, current spyware can come through simple tricks, misleading phishing, or advanced zero click exploits. This variety of delivery methods demonstrates how complex surveillance software is and how it poses a severe threat to society.

1.6 Ethical and Legal Concerns

The increasing use of sophisticated spyware tools like **Pegasus** and **Predator** raises critical ethical and legal concerns. These concerns center on the right to privacy, the legal ambiguity in which spyware vendors operate, and the broader implications of surveillance in both democratic and authoritarian settings. As spyware technologies grow more powerful, the need to balance **security interests with the protection of fundamental rights** has never been more urgent.

The use of spyware programs, like Pegasus and Predator, raises ethical and legal concerns. These concerns involve the right to privacy plus the unclear legal standing of companies that sell spyware. They also touch on the wider effects of watching people in countries that have a democracy and those that do not. The need to weigh safety against protecting basic rights is very pressing.

Privacy vs. Security: Reframing the Debate

It is often argued that society must choose between keeping private matters secret and keeping people safe. This is the scale of privacy on the one hand and security on the other. However, this scale is increasingly seen as misleading. Privacy is not a barrier to security- it is a part of it. Strong rules for privacy build trust and they also restrict misuse and overpower.

People and governments justify spyware as a way to fight terror or criminality. When it gets used against reporters, politicians along with civilians and other public entities, it shows something else. Surveillance without proper checks can eliminate the safety it says it ensures. The challenge is not to get rid of surveillance but to ensure its legal and proportionate and accountable.

The Right to Privacy in International and Regional Law

A person's **right to privacy** appears in international human rights laws, especially in the Universal Declaration of Human Rights (Article 12) and the International Covenant on Civil and Political Rights (Article 17). These rules say that others should not meddle with a person's private life. This includes a person's talks and computer information.

At a local level, data protection rules put privacy protections into law. The European Union's General Data Protection Regulation (GDPR) is the most important of these. The GDPR counts as a wide-ranging privacy law - it grants people rights over their personal data, such as

- The right to be informed when data is collected
- The right to access and correct their data
- The right to withdraw consent
- The right to data portability and erasure

Because spyware software gathers information without a person knowing or agreeing it poses problems on the GDPR regulation. It also usually sends this information across borders, which breaks several main GDPR rules, which include rules about being clear, about only using data for a specific reason, and about collecting little data. If someone uses spyware within or against people in the EU without a legal reason, this breaks GDPR rules and can bring legal penalties for groups that use it.

Legal Gray Zones for Spyware Vendors

Despite growing regulation, spyware vendors and companies often work in areas where laws are unclear. These companies declare that they sell only to governments for valid security reasons. Once the programs are in use, people do not know much about how they work, or if they follow rules about data.

Many spyware firms are headquartered in countries with weak oversight or operate through complex corporate structures, making regulation and enforcement difficult. Even when legal frameworks like GDPR exist, their reach often ends at national borders, while the tools themselves can be used **globally**.

This lack of clear international governance enables a market or surveillance tools with minimal accountability. While some export controls and sanctions have been introduced, a broader legal framework is still missing.

Conclusion

The debate about spyware's ethics and laws concerns is not a discussion about technology. It is a debate on how societies ensure their right to privacy when dangers appear (terrorism acts/illegal actions etc). Rules such as GDPR show that people can shield their privacy with plain, firm standards. The true problem rests in using these shields in a steady way across different countries and against harder surleillance tools.

As time moves on, privacy must stay a main value because it is not an obstacle to safety. Instead, it prevents safety from misuse. The future of digital rights relies on closing regulatory gaps, increasing transparency and ensuring that spyware and its companies are subject to the same rule of law they claim to protect.

Chapter 2: Predator and Pegasus – A Comparative Overview

Spyware programs, such as Pegasus and Predator, are on the center of global conversations about digital surveillance, cybersecurity and human rights. Both software are spyware programs used also by governments with the justification of national security or crime prevention. However, many investigations show that these spyware targeted news reporters, political opponents, activists and civilians. That raises a big concern over surveillance's software misuse.

This chapter introduces these two systems and it gives a short history of where they came from, what they can do as well as how people used them. Lastly, it compares them and highlights their similarities and differences.

2.1 Pegasus Spyware (NSO Group)

NSO Group, an Israeli company, established Pegasus in 2010. They sold it as a legal way to watch terrorists and criminals. Pegasus became known globally after many international investigations, particularly the Pegasus Project in 2021 coordinated by Amnesty International and the Citizen Lab.

Pegasus infiltrate into phones without user interaction. When installed, the spyware does several things. It takes messages, emails, contacts along with call logs - it turns on the camera and microphone from afar. It follows GPS location as it happens. It runs quietly, with no signs that it is there. The program is designed to work on both iOS and Android platforms and uses several zero-day exploits to get past the system defenses.

2.2 Predator Spyware (Cytrox / Intellexa)

Predator is a recently exposed spyware software. Cytrox company in North Macedonia, developed it and the Intellexa Alliance distributes it. Reports about its use in Greece, Egypt along with Armenia brought Predator to global notice in 2022.

Predator infects devices in ways that differ from Pegasus. It usually uses one click links sent through messaging applications or social engineering. Newer versions also offer zero click exploits. When attackers deploy Predator, it lets them get device data, record calls and surroundings, get into encrypted applications plus messages, and control the phone from afar.

Predator is modular, unlike Pegasus as well as it may combine with other surveillance platforms from Intellexa. Reports say it runs well on Android, but people also saw it target iOS devices.

2.3 Similarities and Differences

Pegasus and carry out similar surveillance but they show differences in how people use them and in their technical details:

Feature	Pegasus	Predator
Developer	NSO Group (Israel)	Cytrox / Intellexa Alliance
Infection Type	Zero-click, silent	One-click (some zero-click cases)
Platform Targeted	iOS and Android	Primarily Android, also iOS
Delivery Vector	Messaging apps (e.g., iMessage)	Links via social platforms
Remote Capabilities	Full device control	Full device control
Public Exposure	Extensive (Pegasus Project)	Emerging (2022 onward)
Known Targets	Journalists, activists, lawyers	Politicians, journalists, critics

The tools show how people use commercial spyware for purposes that exceed its stated goal of fighting crime and terrorism. The spyware shows up in many democratic and non democratic countries. This raises questions about how surveillance software companies are responsible for their products - it also raises questions about whether export rules are good enough. Countries need to know about the use of this software soon.

Chapter 3: Technical Foundations for Spyware Analysis

To understand how spyware like Pegasus and Predator work, a person should understand the basic design of mobile operating systems. They also need to know important cybersecurity ideas and the ways people find spyware or examine digital evidence. This chapter describes all the needed technical information.

3.1 Mobile Operating System Security

iOS Security Model

Apple's iOS rests on a closed/proprietary system where hardware and software connect tightly. The system uses app sandboxing, which separates applications from each other and from central system files and it also has mandatory code signing, so only applications Apple approves can run. Data is also encrypted. A secure enclave, a different chip, handles sensitive data such as Face ID in addition to Touch ID. These steps mean iOS is hard to break into. But Pegasus, got past them using zero click attacks in services like iMessage.

Android Security Model

Android is more open and fragmented across devices and manufacturers. It includes:

Application sandboxing, enforced by the Linux kernel

Permission-based access controls, with user prompts for sensitive actions

Google’s **Play Protect** system and verified boot

More frequent gaps in updates due to manufacturer and carrier delays

This makes Android more flexible but also more vulnerable, especially on older or poorly maintained devices.

Understanding how these systems are secured helps explain how spyware must work to **bypass protections**, **escalate privileges**, and **maintain persistence**.

Android is designed differently than iOS. It is more open but fragmented across devices and manufacturers. It also provides application sandboxing like iOS and it is enforced by the system kernel. There are permission-based access rules which restrict what android applications can do. Unfortunately, due to manufacturer and carrier delays, there are gaps in its updates.

3.2 Must-know Cybersecurity Concepts

Zero-day vulnerabilities: Unknown software flaws are used before the vendor patches them.

Exploit chains: A sequence of linked vulnerabilities used to move from limited access (e.g., sandboxed app) to full system control.

Privilege escalation: A chain of joined weaknesses moved from restricted access, as from a sandboxed application, to complete system control.

Command and control (C2): A remote server infrastructure that is used to receive data from infected devices or send instructions to the infected devices.

Persistence: Techniques used to survive system reboots or updates, ensuring long-term access.

Indicators of Compromise (IoCs): Unusual network activity or changed system files are forensic signs that a device took on an infection.

3.3 Digital Forensics and Spyware Detection Tools

Sophisticated spyware, such as Pegasus and Predator are designed to operate invisibly. On that account, common antivirus software often does not find it. Finding this software requires forensic methods and special tools.

Mobile Verification Toolkit (MVT)

Amnesty International developed Mobile Verification Toolkit (MVT). It is an open-source software that helps identify devices that are infected with Pegasus spyware.

It works by:

- Analyzing encrypted iPhone backups
- Search for known forensic traces such as suspcicious domain/IP contact

Device Logs and Metadata Analysis

Forensic analysts examine:

- **System logs**, especially crash reports and diagnostics
- **Network logs** for unusual or encrypted outbound traffic

- **Application behavior**, such as unexpected battery drain or camera activation

Packet Capture and Traffic Analysis

Applications like **Wireshark** or **tcpdump** are used to monitor device traffic. While Pegasus and Predator often use encrypted channels, anomalies in destination domains/IPs can serve as red flags.

Such ways help build a timeline of infection; they show if a device had an infection, even if the spyware tried to remove signs.

3.4 Research Challenges in Spyware Analysis

Analyzing spyware stays hard because of several technical and ethical problems:

- **Encryption and Obfuscation**: Spyware encrypts its communication plus hides its operations. This makes it hard to look at traffic and memory.
- **Self-destruct mechanisms**: Some spyware deletes itself or its logs if specific events occur, for example, if the SIM card changes or someone finds it.
- **Legal and ethical constraints**: Researchers must respect device owner approval and must also follow data privacy laws.
- **Limited access to source material**: Analysts use public data, samples that got out, or help from victims. Spyware sellers do not publish their tools or methods - this causes limited access to what people can study..

For these reasons, much of the research on Pegasus and Predator has come from a small number of trusted digital rights labs (e.g., **Citizen Lab**, **Amnesty Tech**) and not from commercial security products.

Chapter 4: Pegasus Spyware – Technical Dissection, Exploitation Methodology, and Forensic Implications

4.1 Introduction

Pegasus is a state-graded commercial spyware. This chapter presents a comprehensive technical analysis of Pegasus, with emphasis on its infection lifecycle, architectural components, persistence methods, detection artifacts, and known forensic traces. The analysis draws from primary reports by Lookout [1], Amnesty International [2], and supporting academic studies [3].

4.2 Evolution and Versions of Pegasus

Pegasus has changed and evolved as a response to platform security advancements:

In **2016**, the Trident exploit chain was exposed for the first time. It was targeting iOS 9.3.5 through Safari. This chain used three chained vulnerabilities, CVE-2016-4655, CVE-2016-4656 along with CVE-2016-4657, to run code as it pleased.

In **2018 and 2019,** adroid variants emerged leveraging user permissions, SELinux misconfigurations as well as privilege escalation exploits on Android.

The FORCEDENTRY exploit in **2021** used a zero click exploit in Apple's iMessage. It used a new JBIG2 image processing bug and allowed it to escape the application sandbox and achieve remote code execution [2].

In **2021** the FORCEDENTRY exploit leveraged a zero-click vector in Apple's iMessage, using a novel JBIG2 image-processing bug to achieve sandbox escape and remote execution [2].

4.3 Exploitation Vectors and Delivery Mechanisms

4.3.1 Trident Chain (iOS 9.3)

The Trident chain involved:

CVE-2016-4657: A Safari WebKit vulnerability for remote code execution.

CVE-2016-4655: An info-leak vulnerability that provided the kernel base address.

CVE-2016-4656: Enabled memory corruption and kernel-level code execution.

Users were sent SMS or email messages containing malicious links. If clicked, the payload was executed in Safari, exploiting these vulnerabilities to install the spyware without any user interaction [1].

4.3.2 FORCEDENTRY and JBIG2

The FORCEDENTRY exploit set a new standard for zero click attacks.

The attack involved delivery of special crafted iMessages embedded with a JBIG2 image, containing over 70,000 segment operations.

These segments implemented virtual logic gates to simulate a 16-bit arithmetic logic unit (ALU). To put it simply, it created a Virtual Machine inside the image parser.

The payload bypassed Apple's BlastDoor sandbox and enabled code execution in the IMTranscoderAgent daemon [2].

4.3.3 Other Vectors

Pegasus has also been delivered through:

- WhatsApp VoIP calls, exploiting vulnerabilities in signaling protocols.
- Apple Push Notification Services (APNs), used to wake the device and trigger exploit code.
- URL-based triggers embedded in SMS, FaceTime, and email previews [1, 2].

The delivery systems are mostly unseen by the targets. They usually need no user interaction. This raises the chance of a successful infection.

4.4 Pegasus Architecture and Operational Workflow

4.4.1 Initial Access

When Pegasus is installed on the target device, it uses and exploits the vulnerability in order to gain code execution privileges and root level control. It alters kernel structures and bypasses Apple's and Android's mandatory code-signing enforcement. On iOS, the program usually gets root access, which bypasses the sandbox limits [2].

4.4.2 Exploit Loader

When the privilege escalation succeeds, a program called loader is deployed. This program sets up a malicious environment, disables system logging (where possible),

and installs additional modules. The program uses altered processes, such as mediaserverd, jsc, or IMTranscoderAgent, to perform these steps. [2].

4.4.3 Payload Execution

Pegasus is modular and divided into parts. It places payloads in memory by using calls such as dlopen() or equivalent.

It may include:

- libaudio.dylib: Captures audio streams.
- libcam.dylib: Activates and records from the camera.
- libgps.dylib: Continuously polls geolocation.
- converter: A Cydia-derived injector used to install or modify binaries [1].

4.4.4 Command and Control (C2) Management

The spyware establishes communication with a distant server using encrypted channels. Traffic is secured using self-signed certificates, and domains are hosted on compromised infrastructure. Upon establishing a session, operators may issue commands such as:

- recordMic
- capturePhoto
- exfilData
- selfDestruct

The C2 infrastructure employs a fast-flux DNS mechanism, rendering it resistant to takedown efforts [1, 3].

4.5 Persistence and Anti-Forensics

4.5.1 Daemon Hijacking

To survive reboots or blend in, Pegasus often mimics or replaces system daemons. It registers its payload as watchdogd, systemd, or rtbuddyd.

LaunchDaemon .plist files are created to ensure re-launch on reboot [1].

4.5.2 Memory-Only Execution

Pegasus attempts to avoid detection by executing directly in memory:

- Files are unpacked into temporary memory regions using mmap.
- No permanent installation path is maintained on disk.
- Kernel patches disable logging mechanisms such as syslogd or crash reporters [1, 3].

4.5.3 Self-Destruction

If Pegasus detects threat analysis tools or signs of forensic inspection, it can automatically:

- Erase itself
- Delete related logs
- Overwrite memory with null bytes [2]

This self-destruction logic makes real-time analysis and full capture challenging for investigators.

4.6 Detection Artifacts and Forensic Evidence

4.6.1 Crash and System Logs

Forensic researchers have found recurring evidence in:

- Crashes and instability in daemons such as SpringBoard and IMTranscoderAgent
- Anomalous system restarts
- Suspicious absence of diagnostic logs [2]

4.6.2 File System Indicators

Pegasus leaves subtle traces:

- Temporary files: /private/var/tmp/jailbreak.sh
- Hidden launch agents in /Library/LaunchDaemons
- Binaries without matching Info.plist metadata [2]

4.6.3 Network Forensics

Indicators include:

- TLS connections to rare IPs using malformed headers
- Domains such as cdnproxy[.]info, securecloudsync[.]com
- Rapid creation and resolution of C2 domains [1, 3]

4.6.4 MVT Forensics

The Mobile Verification Toolkit (MVT) detects:

- Known binary strings and JBIG2 payloads
- Timestamp discrepancies in app databases
- Differences between known clean backups and suspected devices [2]

4.7 Countermeasures and Mitigation Strategies

4.7.1 OS Hardening

Platform vendors have responded by:

- Introducing Apple Lockdown Mode
- Patching CVEs promptly
- Enforcing stricter sandboxing and signed code execution [3]

5.7.2 Network Monitoring

Network defense tools can:

- Detect anomalous encrypted traffic to C2 domains
- Use threat intel feeds to block known IPs and TLS fingerprints [1, 2]

4.7.3 Behavioral Analysis

Advanced endpoint detection and response (EDR) systems can:

- Flag processes missing parent-child lineage
- Detect hidden daemons
- Use memory snapshotting to detect injection activity [3]

4.7.4 Physical and Operational Measures

Regularly rebooting devices can disrupt memory-only implants. Restoring devices to factory settings removes non-persistent malware. Users should avoid engaging with unknown links and use secure messaging platforms [2]

4.8 Real-World Cases with Technical Evidence

Morocco & Khashoggi

Amnesty Internation recovered JBIG2-based exploits from phones belonging to Moroccan activists and associates of Jamal Khashoggi.

Payloads matched known Pegasus binaries; devices showed evidence of tampering and stealth deletion [2]

Catalonia (CatalanGate)

Citizen Lab confirmed infections on more than 60 devices.

Forensic evidence included hijacked daemons and timestamp irregularities [2, 3]

India

Journalists' phones showed deletion of log entries and suspicious DNS activity.

Infections coincided with political events and protests [2]

4.10 Conclusion

Pegasus shows what mobile surveillance can do. The software uses file emulation, zero click exploits along with ways to avoid detection. This sets a standard for spyware. Detecting and countering such threats requires an integrated approach: from OS-level defenses and secure communication practices to advanced forensic capabilities and international regulation.

References

[1] Lookout & Citizen Lab, "Technical Analysis of NSO Group's Pegasus Spyware," 2016.

[2] Amnesty International Security Lab, "Forensic Methodology Report: How to catch NSO Group’s Pegasus," 2021.

[3] Athanasopoulos, N., "A Comprehensive Analysis of Pegasus Spyware and Its Implications for Digital Privacy and Security," MSc Thesis, 2022.

Chapter 5: Predator Spyware – Technical Analysis, Exploitation Workflow, and Detection Challenges

5.1 Introduction

Predator poses a particular threat because it functions as the new global surveillance system - it is not just a simple spyware program. It works as a full system. Reports from Cisco Talos, Amnesty International, and Recorded Future show its global use. Changing infrastructure, complex exploit chains, and strict control panels support the program - this section explains the infection methods, the design, how it works as well as the digital traces of Predator in detail. It includes information from Amnesty International's "Predator Files," Cisco Talos, Recorded Future, the European Parliament's spyware investigations, and some commercial documents that became public. That provides a combined look at the dangers that Predator presents.

5.2 Predator Architecture and Capabilities

5.2.1 Design Philosophy and Modularity

Predator's design is modular. This allows separate loading and control of surveillance components.

Each phase of its operation such as exploitation, payload deployment, data transfer, and command execution, is distinct. Each component has dedicated modules responsible for each function. This architecture permits silent updates, remote module activation, and tailored infection profiles per target. The spyware runs in memory only when it can, so it avoids antivirus plus inspection programs.

The system on the other side, which Intellexa calls the "Cyber Intelligence Platform" includes GUI dashboards for live target management, map visualizations, and remote control on microphones, cameras, and screen. People who use the system can pick between an "aggressive" mode and a "stealth" mode.

5.2.2 Supported Platforms

Predator supports:

- **Android**: Versions 9 to 11. Exploits take advantage of IPC misconfigurations, browser vulnerabilities, and privilege escalation flaws. It enables GPS tracking, camera handling and file access.

- **iOS**: Versions 12 to 14.3. Exploits use WebKit, sandbox escaping and code signing bypass techniques. Notably, iOS implants remain in volatile memory and leverage native system daemons for persistence until reboot.

From leaked documents, Intellexa offers tailored builds for each device maker. Huawei, Samsung along with Xiaomi are some of the included companies. This shows the careful way they target specific systems.

5.2.3 Surveillance Modules

Surveillance modules are installed in stages and can be further customized. According to leaked documentation it supports:

- **Mic recording**: Can enable the target microphone and configurable it to be enabled on keywords or specific sound levels.
- **Keylogging**: Records typing across all apps, including encrypted messengers.
- **Camera access**: It provides snapshots or continuous recording with light suppression.
- **File harvesting**: It can pull and investigate files on the system or external storage such as SD memory sticks.
- **App targeting**: There are predefined templates to extract conversations from Signal, WhatsApp, Telegram, and Messenger, including encrypted local databases.
- **Exfiltration controls**: Exfil intervals and bandwidth can be controlled manually to reduce detection risk.

The surveillance modules offer real time C2 feedback. An operator can watch device activity. He issues custom scripts - he also gets new modules that come from target behavior.

5.3 Infection Vectors and Exploit Chains

5.3.1 One-Click Exploits

Amnesty documented infections in Vietnam and Egypt. In these infections, attackers sent Predator spyware through malicious links in messages or SMS. These links used url redirects to create payloads based on the device's fingerprint (user agent, locale and OS). The payloads then took advantage of vulnerabilities in WebKit rendering or application flaws causing code execution.

5.3.2 Zero-Click Exploits

In 2023, reports showed zero click exploits that used Apple's iMessage in addition to WhatsApp preview rendering. Signs of these attacks include JBIG2 image streams, bad GIFs or image previews. By this method payloads were triggered through push notification services. Such attack vectors are effective and work well on important targets.

5.3.3 Tactical and Strategic Delivery

Tactical attacks involve:

- **Rogue Wi-Fi implants** (e.g., SpearHead360 vehicle kits)
- **Fake charging stations** equipped with USB payload delivery
- **Proximity targeting** through IMSI catchers and physical drop-offs

5.4 Command and Control (C2) Infrastructure

5.4.1 Network Behavior

C2 communications use encryption over TLS and the DNS used were changing rapidly. At times, the traffic was proxied through Cloudfare or other CDNs.

- Use of uncommon TLS cipher suites
- Self-signed certificates
- User-agent spoofing to mimic legitimate apps (e.g., Facebook, Gmail)

Intellexa regularly moves its infrastructure - it does this to stop people from knowing who owns it and to prevent shutdowns. Accorning to Cisco Talos the C2 structure has three parts. It includes payload distribution, session control along with data aggregation.

5.4.2 Exfiltration Patterns

Data is transfered via HTTPS, often disguised as background synchronization service. The spyware also uses DNS over HTTPS (DoH) tunneling in addition to TLS session padding to hide the size of the data transfered. Burst timing, frequency hopping along with compression lower the chance of detection. Operators divide the data into parts and reassemble it on the server

5.5 Detection Artifacts and Forensic Analysis

5.5.1 Mobile Verification Toolkit (MVT) Evidence

Forensic experts using MVT found the following artifacts:

- There were Predator-related C2 domains in Safari history in addition to DNS caches.
- Crash logs showed JBIG2 decoding errors. This signaled zero click methods.
- Security logs from Apple's BlastDoor sandbox engine were not there.

These signs show exploit actions and module loads that fit with Predator.

5.5.2 Log and Memory Artifacts

Predator is often memory-resident only. Logs may reveal unusual launchctl behavior or network daemon crashes. Analysts have found unauthorized execution permissions on binaries in /tmp, /var, or RAM disks, indicating memory injection. Some implants attempt to patch logging binaries like syslogd or diagnosticd.

5.5.3 Anomalous Behaviors

High-fidelity behavioral anomalies include:

- Mic or camera activation while screen is off
- GPS usewhen no apps are in use
- Excessive battery drain at night or during lockscreen idle

When combined with signs in memory and DNS records, they point to a system compromise.

5.6 Countermeasures and Mitigation

5.6.1 Platform Hardening

Since 2022 when Predator was exposed, Apple and Google have deployed mitigations and patches targeting the vulnerabilities Predator exploits:

- Lockdown Mode blocks preview-based exploits
- Enhanced memory isolation for rendering engines
- Mandatory app attestation for sensitive permissions

Regular firmware updates and app sandboxing have also made it harder to succeed in a device beng compromised.

5.6.2 Detection Tools

Forensics labs developed custom YARA rules to find module signatures. Products such as MVT, Zimperium along with CrowdStrike Falcon Mobile identify infected devices. They use behavioral analytics and static signatures. Agents on Android endpoints locate privilege elevation attempts - these agents also find changed init processes.

5.6.3 Operational Mitigation

Predator payloads do not usually stay on a device after it restarts. Restarting devices often, resetting them to their original settings, and limiting app permissions help protect them. People should not open links they do not know; they also need to turn off picture previews. Using encrypted communication apps, such as Signal, that have link protection is a good practice.

5.7 Greek Case Study: Predator in Greece

From 2021 to 2023, people in Greece were subject to Predator. SMS messages became public and showed malicious links that were sent to Christos Spirtzis, a member of the opposition in parliament, as well as to reporters plus to those in civic groups. Citizen Lab and the PEGA Committee said that domains went with Intellexa's system. Studies of the phones that had trouble showed that DNS requests went to Predator C2 servers. There was also unusual program action also log times that did not match.

Intellexa was a business registered in Athens, and it worked with phone companies that had ties to the government. This has raised concerns about the government surveillance. The events in Greece show that spyware can be used in wrong ways when rules are loose or when politics affects them.

5.8 Conclusion

Predator is not just another spyware platform - it represents a change in the design and use of commercial surveillance tools. Its modular design, stealth capabilities, and support for nation-state delivery infrastructure make it a highly adaptable and potent surveillance weapon. Unlike legacy spyware, Predator seamlessly integrates tactical and systemic infection capabilities, delivered with precision or scale depending on operator needs.

Countermeasures such as Lockdown Mode and the development of forensic toolkits offer some detection. But Predator loads its content only into memory and uses custom attack methods, so real time defense is hard. The spyware has been used against political opponents as well as journalists, which threatens democratic practices and personal freedoms. Its spread shows the immediate need for international rules, public knowledge about government spyware use, plus more responsibility from sellers like Intellexa.

Predator shows a worrying change in how spyware develops. It started as secret tools for specific law enforcement cases. Now it is a commercial system that spies on many people. If people do not control these platforms, they might become normal tools of control in both democratic and authoritarian governments.

References

[1] Amnesty International Security Lab. "Predator Files Report." 2023.

[2] Cisco Talos Intelligence. "Mercenary Intellexa Predator." 2023.

[3] Recorded Future. "Predator Spyware Infrastructure Returns." 2024.

[4] GovWatch. "Christos Spirtzis Targeted by Predator." 2023.

[5] Intellexa. "Predator Premium Commercial Proposal." Leaked Document, 2021.

[6] IPOL Study. "Spyware Use in the EU: Legal and Political Challenges." European Parliament, 2022.

[7] AlMasri, T. and AlDalaien, M. "Detecting Spyware in Android Devices Using Random Forest." 2023.

[8] Amnesty International Security Lab. "Technical Review of Predator Forensics." 2023.

[9] PEGA Committee, European Parliament. "Use of Spyware in Greece." Interim Report, 2023.

Chapter 6: Comparative Analysis of Pegasus and Predator, and Conclusions

6.1 Architectural Differences and Commonalities

Pegasus and Predator both represent expensive and high-end mobile spyware software. They vary in their modular design, how they are delivered and with what systems they work with.

NSO Group developed Pegasus - it uses a modular loader design with code running in memory. The software bypasses security through zero click exploits.

The Intellexa Alliance developed Predator. This software uses a dashboard to manage its modules - allowing an operator to input data/code real-time, turn modules on and off, and change attack tactics quickly.

Both programs work on Android and iOS. Pegasus's iOS method, called FORCEDENTRY, is very complex. It escapes the sandbox and stays on the device by using problems in JBIG2 parsing. Predator, though capable of zero-click deployment, is more frequently observed using one-click vectors or ISP-level network injection, focusing on scalability over complexity (Recorded Future, 2024).

6.2 Exploitation and Delivery Mechanisms

Pegasus is known for pioneering the zero-click attack landscape. The 2021 FORCEDENTRY exploit used a JBIG2-based virtual machine to gain execution on iMessage without user interaction (Amnesty, 2021). It also employed sophisticated delivery mechanisms such as silent push notifications via Apple’s APNs service.

Predator uses both one-click and zero-click attack vectors but demonstrates preference for ISP-assisted delivery or tactical Wi-Fi injection, using redirection-based attacks to fingerprint devices and deploy custom payloads (Lookout, 2024). In cases observed by Citizen Lab, Predator was able to coexist on devices already infected by Pegasus (Marczak et al., 2021). That shows how different those spyware are and what different systems they exploit and use.

6.3 C2 Infrastructure and Survivability

Pegasus uses layered TLS communication and its infrastructure employs dynamic DNS and multiple encryption layers. The command-and-control (C2) channels use domain fronting in addition to CDN obfuscation. Exfiltrated data is AES-encrypted. This data

moves over common ports, such as 443 and 80, so it appears like normal HTTPS traffic, as Lookout reported in 2021.

Predator's C2 setup focuses more on the operator - it has three parts - payload delivery, real time control along with data aggregation. Data exfiltration avoids discovery because of TLS padding, bursty transmission as well as DoH (DNS-over-HTTPS) tunneling. Cisco Talos explained this in 2023. The system also uses user agent spoofing plus changes domains to get past intrusion detection systems.

6.4 Detection and Forensics

Forensic analysis of both spyware software remains very hard. Pegasus leaves traces such as crash logs, including IMTranscoderAgent - it also leaves unusual plist entries in addition to DNS records. Tools like the Mobile Verification Toolkit (MVT) and Zimperium's zIPS find these by using indicators of compromise and studying behavior.

Predator shows patterns like SELinux context problems on Android. On iOS, it leaves unexplained launchctl entries. The program also causes JBIG2 decoding errors when it tries to attack a device without user interaction. Its memory resident nature means that people cannot find it after a device turns off, unless the device runs plus has root access during an examination.

6.5 Geopolitical Deployment and Use Cases

Around the world, Pegasus has seen use in more than 40 nations, in both democracies and autocracies. People use the program to watch journalists, figures in the opposition, and activists (Deloitte, 2023). Cases that stand out involve Jamal Khashoggi's family plus some journalists from Mexico.

Governments in Greece, Egypt, Armenia along with Vietnam have connections to Predator. Thorough investigations show that the program deploys at the internet service provider level, which links it to state sanctioned targeting (GovWatch, 2023; Amnesty, 2023). In Greece, an SMS message with Predator payloads went to Christos Spirtzis, an opposition Member of Parliament. Forensic analysis later showed that this occurred.

6.6 Ethical and Legal Implications

Pegasus in addition to Predator contest the global rules on digital privacy. Some people say that countries use these programs to fight terrorism, but stories tell of common misuse for political or business spying.

The EU's GDPR and the ECHR confirm privacy as a basic right. When someone uses spyware against a person in the EU, it breaks Articles 7 plus 8 of the EU's Charter of Fundamental Rights. Lawsuits and blacklisting, like the U.S. sanctions against NSO Group, show a growing worry also a legal answer to this problem.

6.7 Final Evaluation and Recommendations

Findings:

Both Pegasus and Predator rely on modular, in-memory implants, zero-day exploits, and network stealth.

Pegasus specializes in high-value, individualized infections; Predator supports scale-based and tactical deployments.

Forensics remains limited, and regulatory oversight is minimal.

Recommendations:

OS-level hardening (e.g., Lockdown Mode, stricter sandboxing).

International spyware regulations and transparency mandates.

Open-source forensic development and cloud-based anomaly detection.

Periodic independent audits of surveillance tech vendors.

6.8 Conclusion

Pegasus and Predator show a basic change in cyber-espionage; they demonstrate how private companies now do what only governments used to do. This refers to surveillance that targets specific people, stays hidden along with continues over time. The programs are technically good, but their use outside of laws affects how democracy works and how people maintain digital human rights.

Their evolution continues. Without global regulation and good forensic answers, people will spread these tools. Spying will go more into civilian life. The line between national security plus authoritarian control will become unclear.

References

Amnesty Tech. (2021). *Forensic Methodology Report: How to catch NSO Group's Pegasus*. https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

Marczak, B., Scott-Railton, J., et al. (2021). *Pegasus vs Predator: Dissidents Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware*. Citizen Lab. https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/

Cisco Talos. (2023). *Mercenary Intellexa Predator*. https://blog.talosintelligence.com/mercenary-intellexa-predator/

Lookout. (2021). *Technical Analysis: Pegasus Spyware*. https://info.lookout.com/rs/051-ESQ-475/images/pegasus-exploits-technical-details.pdf

Lookout. (2024). *Predator and Pegasus Threat Intelligence*. https://www.lookout.com/documents/threat-reports/us/predator-and-pegasus-tg-us.pdf

Deloitte Greece. (2023). *Unauthorized Surveillance with Predator and Pegasus*. https://www.deloitte.com/gr/en/services/financial-advisory/perspectives/unauthorized-surveillance-and-breaches-with-predator-pegasus.html

Recorded Future. (2024). *Predator Infrastructure Rebuild*. https://www.recordedfuture.com/research/predator-spyware-infrastructure-returns-following-exposure-sanctions

GovWatch. (2023). *Surveillance of Christos Spirtzis with Predator*. https://govwatch.gr/en/finds/apopeira-parakoloythisis-toy-christoy-spirtzi-me-to-paranomo-logismiko-ypoklopon-predator/

Chapter 7: Forensic and Technical Tools for Detecting Mobile Spyware

7.1 Theoretical Foundations

Detecting spyware like Pegasus and Predator, is a difficult and complex technical job. Spyware engineers build these tools to stay hidden and they often remove their presence after they finish their tasks. So investigators cannot depend on normal antivirus scans or simple log traces.

Organizations such as Citizen Lab and Amnesty International's Security Lab have been central to this effort. Their work doesn't just involve technical dissection; it incorporates legal scrutiny and ethical awareness, ensuring that the conclusions drawn from an investigation hold up not just technically, but also in human rights contexts (Amnesty International, 2021; Marczak et al., 2021).

Typically, analysts look for secondary indicators—what might be called the "shadows" left behind. These could include anomalous crash reports, unusual system processes, unexpected configuration changes, or silent communications with known malicious domains. Rarely is a payload directly visible; most often, its activity must be inferred from surrounding patterns.

A key tool in detecting mobile spyware is the Mobile Verification Toolkit (MVT). It helps trained investigators get encrypted logs and backup data from a mobile phone. The investigators then put together a timeline of when an infection happened. A single bit of data, like when a system service crashes or when a quiet push message arrives at a strange time, causes more looking into. Checking these odd things against known Pegasus control spots supports what the investigators find. This also shows how often someone gets targeted.

These investigations are not just technical work; they involve ethical considerations. People who are looked at often work as activists, reporters, or politicians. Amnesty's forensics group, for example, follows strict rules about privacy. Its analysts work closely with legal groups. They check that no one gets hurt, and that all findings get reported and explained properly.

To sum up, finding out how spyware like Pegasus operates involves careful, layered study rather than simple discovery. Investigators piece together what is not there instead of what is

clear - this way of working stresses exactness and understanding - it balances the need for technical proof with the truth of political issues.

7.2 Open-Source Forensic Toolkits

7.2.1 Mobile Verification Toolkit (MVT)

The Mobile Verification Toolkit, which Amnesty's Security Lab put out in 2021, quickly changed how people examine spyware. This command-line toolkit, open to everyone, lets technical and also non technical users look at encrypted iOS in addition to Android device backups; they search for known Indicators of Compromise, which include unusual crash logs, suspicious programs along with threat notices from Apple.

MVT supports workflows such as:

1. Automatically decrypting and parsing encrypted backups (.zip, .tar).
2. Extracting crash log files (.ips, log_archive, etc.).
3. Matching observed artifacts against structured IOC feeds (Pegasus, Predator, BLASTPASS).
4. Generating JSON-based forensic reports for legal, academic, or journalistic use.

The strength of MVT lies in its transparency. It is an open-source and community-driven project published on GitHub. Its contributions were vital during the *Pegasus Project* in 2021, where MVT validated Apple’s threat notifications and tied them to crash footprinting (Apple, 2021; Amnesty International, 2021), confirming systematic surveillance campaigns.

7.2.2 Android Quick Forensics (AndroidQF)

Unlike iOS, Android devices have various hardware and different logging systems, so investigators face problems with forensic consistency. Amnesty Security Lab released Android Quick Forensics (AndroidQF) in 2024 to address these issues. The tool, written in Go and available on GitHub, helps collect information from Android devices using ADB. This program specifically finds temporary programs, such as Predator, that do not stay on the device after a restart.

AndroidQF harvests:

- SELinux status and policy violations.
- Core system logs and crash files (including logcat, tombstones).
- Android's package metadata with installation timestamps.
- Filesystem anomalies and timestamps mismatches suggesting unauthorized operations.

The tool helped obtain proof from devices infected with Predator - it showed differences in timestamps between when programs installed plus when backups happened. It also showed unusual memory use. This brought clarity to systems that would remove their own evidence.

7.3 Case Studies

7.3.1 Pegasus in Jordan

From 2019 to 2023, Citizen Lab with Access Now led an investigation and uncovered the deployment of NSO Group's Pegasus spyware against Jordanian civilians including journalists, lawyers, and human rights defenders (Citizen Lab, 2024; Human Rights Watch, 2024). The hacking attempt was deeply invasive, with 35 confirmed infections - 30 independently verified - highlighting its systematic nature and duration.

Investigators used the Mobile Verification Toolkit, or MVT, to find the spyware. That tool helped them look at encrypted iOS backups from the devices of affected people; they found crash logs tied to IMTranscoderAgent.ips. They also saw AppleService error reports besides Safari/WebKit crash dumps. These reports showed Pegasus used flaws that did not need a click, such as problems in HomeKit and iMessage - they compared these logs with Apple's Threat Notification system, which helped confirm the attacks.

Among those targeted were two Human Rights Watch staff members based in Jordan, Adam Coogle and Hiba Zayadin. Coogle's device got infected in October 2022. Apple sent him a warning in March 2023. Zayadin had at least two infection attempts. One was successful in October 2022. Another attempt was in early 2023 but it likely failed because of Apple's "Lockdown Mode". The timing of these exploit attempts correlates strongly with their public-facing human rights work.

Several devices got infected repeatedly. This showed that dynamic zero day exploits could bypass later security patches. For example, one activist's iPhone was hacked three times from February 2022 to September 2023. This suggested that someone kept targeting him and perhaps used newer zero click vulnerabilities. The pattern showed that the surveillance operation was continuous and adaptive when needed.

The technical analysis also included network and metadata forensics. Analysts traced DNS and TLS handshake data to known Pegasus C2 domains. The infection was during political events or protests, which implied that exploitation happened in coordination with important times for civic activism.

From a technical view, sophisticated exploit chains like FORCEDENTRY and possibly new HomeKit-based zero click vulnerabilities allowed this operation to happen (Citizen Lab, 2024; Access Now, 2024).

Table 7.1 – Forensic Findings in the Jordan Pegasus Case Study

Category	Indicators / Tools	Findings	Notes
Device Crash Logs	IMTranscoderAgent.ips,	Present in 30+ infected devices post-	Identified using MVT analysis (Citizen Lab, 2024)

	AppleService logs	exploitation attempts	
Threat Notifications	Apple's internal "Threat Notification" alerts	Used to confirm active infections and categorize timelines	Notifications often occurred 4–5 months after infection (HRW, 2024)
Repeat Infections	Multiple crash logs from same device over time	At least 8 individuals were reinfected; some 3+ times between 2022–2023	Suggests evolving use of zero-click exploits (Access Now, 2024)
Apple Lockdown Mode	Attempted infections post-Lockdown Mode	Zayadin's phone showed interference in early 2023	Indicates Apple's patch reduced but did not eliminate risk
Network Forensics	DNS/TLS logs matching Pegasus C2 domains	Corroborated data exfiltration and espionage linkage	Active during political events; used for command instructions (AP News, 2024)
Exploits Employed	FORCEDENTRY, HomeKit/iMessage -driven vectors	Confirmed through crash log signatures and exploit timeline reconstruction	Looks to be multi-vector, zero-click methodology (Citizen Lab, 2024)[i1]

Implications

- **Targeting Local Civil Society**: The campaign demonstrates how spyware is repurposed internally—against domestic journalists and activists—rather than solely for intelligence or counterterrorism.
- **Persistence Despite Patching**: Repeated infections illustrate that NSO-like tools rapidly adapt to evolving security patches, emphasizing the need for proactive defence.
- **Company Responsibility**: Apple's Lockdown Mode reduced infection success, but delayed threat notifications limit their timely effectiveness.
- **Human Rights Context**: The targeting of human rights defenders prompted strong reactions from NGOs and the UN, intensifying calls for international regulation on spyware use.

7.3.2 Dual Infections: Pegasus + Predator

In December 2021, the Citizen Lab at the University of Toronto's Munk School found a rare and important case of two spyware software on one iPhone that belonged to Ayman Nour, a well known Egyptian political dissident. The phone was infected with Pegasus and Predator at the same time. This event showed the first publicly recorded time when two different surveillance

1

tools were used on one device. This depicted how complex the surveillance operations were and how attackers used many ways to target important people (Marczak et al., 2021).

The investigation used the Mobile Verification Toolkit. MVT checked the iPhone's backup data and showed many crash logs and signs that fit a Pegasus infection. Investigators found crash parts linked to IMTranscoderAgent.ips, a known sign of NSO Group's FORCEDENTRY exploit chain. This exploit uses vulnerabilities in iMessage to deploy the spyware on a phone without the user's interaction. Dynamic libraries such as forcedEntry.dylib also appeared in crash logs. This agreed with Apple's later message to the person that a state sponsored attacker using Pegasus compromised his device.

Pegasus is noted for its persistent implantation. It can survive reboots and use encrypted network infrastructure through the Pegasus Anonymizing Transmission Network (PATN). Predator, on the other hand, uses a "hit-and-run" method that is not persistent. It is put into memory during exploitation and then erased following a reboot. Because of this, it's tougher to find unless the gadget is looked at just after it gets infected. In this case study, researchers detected traces of Predator by looking at inconsistent timestamps, revoked provisioning profiles, and strange system snapshots. These strange things included backup timing gaps that weren't expected and proof that profile installations on devices were getting around App Store security - behavior that fit with Predator's attack structure.

The technical investigation focused at more than just artifacts on the device level. Investigators did a network forensic investigation and found short-lived DNS requests and TLS connections linked to known Predator command-and-control (C2) domains. These short network connections, which frequently happened right after a reboot or when the user wasn't using the device, were similar to the behavior of prior infections. On the other hand, Pegasus communication was more constant, hidden, and layered with many anonymizing nodes, giving each spyware a unique signature.

Citizen Lab's team further investigated an Android device linked to the same target, using**Android Quick Forensics (AndroidQF)** to extract low-level system logs. They identified changes in the SELinux policy and errors in the logcat, repeated crashes of the zygote process- a central Android system service - indicating early-stage Predator deployment. These findings demostrated that Predator cross-platform design. It can be installed on different operating systems and it could be run when the device started, using temporary root permissions.

This case study provides critical lessons for spyware detection. It highlights the need for **multi-vector, multi-tool forensic workflows**. Relying only on lasting evidence from spyware does not work. Instead, investigators must now incorporate **complementary tools and methods**—iOS backup analysis (MVT), Android memory and SELinux inspection (AndroidQF), TLS/DNS network correlation, and profile provisioning traceback.

Table 7.2 Summary of Technical Indicators and Methods

Spyware	Artifacts and Indicators	Detection Method
Pegasus	IMTranscoderAgent.ips, forcedEntry.dylib, Apple notifications	MVT (iOS backup analysis), Apple Threat Alerts
Predator	Revoked profiles, timestamp gaps, ephemeral DNS/TLS traffic, WebKit crash loops	MVT, network correlation, manual log analysis
Predator	zygote crash logs, SELinux policy deviations	AndroidQF, logcat and dmesg inspection

The dual infection of Ayman Nour's device revealed that **spyware is no longer an isolated phenomenon**. Several state linked groups or commercial groups can target devices at the same time. Each group uses its own set of tools - this situation raises the difficulty for digital forensic experts - it also questions the way security works now and how policy frameworks oversee it. Spyware systems grow and become more varied. Civil societies, academia along with technologists need to work together often. That helps them stay aware of the danger plus protect the right to privacy.

7.3.3 CatalanGate

In April 2022, Citizen Lab released a report called CatalanGate. It recorded the use of Pegasus spyware against many people tied to the Catalan independence group. This surveillance operation focused on more than 65 confirmed people; they included members of the European Parliament, Catalan government workers, leaders of civil society, lawyers along with reporters. The operation went on between 2017 and 2020. This was a major use of Pegasus spyware inside a democratic European state, and it brought up many legal, ethical as well as political worries.

The investigation used the Mobile Verification Toolki. MVT helped examine encrypted iTunes backups from iOS devices. It looked for signs of Pegasus. Among the most important findings were system crash logs, such as IMTranscoderAgent.ips. The tool also found odd things in WebKit processes and other error reports linked to FORCEDENTRY. NSO Group's known zero click exploit turned iMessage into a weapon - these forensic signs matched what Apple found in 2021 when it did its own Pegasus studies.

To check when infections occurred, Citizen Lab coupled device data with network evidence. They traced DNS and TLS logs to domains linked to the Pegasus Anonymizing Transmission Network (PATN). This way, they maped the timeline of the infections. In many cases, Pegasus was deployed on devices when political events were happening, like votes, protests, or court cases.

Even though Citizen Lab's report was descriptive, people criticized it. Researchers from the London School of Economics (LSE), led by José Javier Olivas Osuna, wrote a reply that pointed out several problems with how Citizen Lab did its work. For example, they did not use phones that were not infected as a base for comparison. The report did not clearly explain how they

handled the evidence, and they did not tell the difference between times when the spyware worked and times when it did not get on the phone. The LSE review also said that the work should follow official rules, such as the Berkeley Protocol on Digital Open Source Investigations and the standards that ENISA besides OHCHR suggested (Olivas Osuna et al., 2023).

Nevertheless, *CatalanGate* had a big impact. It caused the PEGA Committee in the European Parliament to start an inquiry into the use of surveillance technology inside EU borders. The committee advised more rules for spyware sellers and legal limits on what governments do with it. The report also pressed Apple, which later sued NSO Group. It also shaped public talk about surveillance, digital rights along with democratic integrity.

Citizen Lab's investigation represents a milestone in civilian-led technical documentation about spyware. The LSE review helped improve future rules for forensic checking - it also showed how important openness and working together between NGOs, universities as well as reporters are - these groups help to hold states and companies responsible. CatalanGate became more than just a study of digital surveillance. It also drove changes in rules, technical methods in addition to laws throughout Europe.

Table 7.3 – Summary of Forensic Indicators and Analysis Methods in the CatalanGate Case

Category	Indicator / Tool	Findings	Notes
Device Forensics	IMTranscoderAgent.ips, WebKit crash logs	Present in infected iPhones using FORCEDENTRY	Detected using Amnesty's Mobile Verification Toolkit (MVT)
Network Forensics	PATN domain queries, TLS traffic patterns	Matched known Pegasus command-and-control infrastructure	Used for attribution and temporal analysis
Exploit Used	FORCEDENTRY (iMessage zero-click)	Enabled access without user interaction	Exploited iOS versions prior to 14.8
Detection Tool	Mobile Verification Toolkit (MVT)	Identified log anomalies and Pegasus indicators	Open-source and widely adopted in civil society investigations
Timeline Reconstruction	Device + Network logs	Infections occurred during political events (referenda, protests)	Supports inference of politically motivated surveillance
Peer Review Critique	Methodological review by LSE	Identified flaws in transparency, chain-of-custody, sampling rigor	Led to calls for forensic standardization in digital surveillance reporting
Legal Impact	PEGA Committee	Catalyzed policy discussion at EU level	Helped redefine spyware as a human rights issue within

	inquiry, Apple lawsuit against NSO		democratic states

References

- Amnesty International (2021). *Forensic Methodology Report: How to Catch Pegasus*. Amnesty Security Lab. Available at: https://www.amnesty.org/en/documents/doc10/4870/2021/en/
- Apple (2022). *Apple sues NSO Group to curb the abuse of state-sponsored spyware*. Apple Newsroom. Available at: https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/
- Citizen Lab (2022). *CatalanGate: Extensive Mercenary Spyware Operation Against Catalan Civil Society*. Available at: https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalan-civil-society/
- European Parliament (2023). *PEGA Committee Final Report on the Use of Pegasus and Equivalent Surveillance Spyware*. Available at: https://www.europarl.europa.eu/
- Marczak, B., Scott-Railton, J., et al. (2021). *FORCEDENTRY: NSO Group Exploit Captured in the Wild*. Citizen Lab. Available at: https://citizenlab.ca/2021/09/forcedentry-nso-group-exploit-captured-in-the-wild/
- OHCHR (2020). *The Berkeley Protocol on Digital Open Source Investigations*. United Nations Human Rights Office of the High Commissioner.
- Olivas Osuna, J.J. (2023). *Critical Review of Citizen Lab's CatalanGate Report*. London School of Economics, Working Paper.
- Scott-Railton, J., Marczak, B., et al. (2022). *CatalanGate Report*. Citizen Lab, Munk School of Global Affairs, University of Toronto.

7.4 Emerging Trends in Forensics

As mobile spyware like Pegasus and Predator reach new levels of stealth and complexity, forensic responses have shifted toward more dynamic, real-time, and cloud-integrated investigative strategies. The growing use of memory-resident implants and zero-click vulnerabilities has rendered traditional forensic imaging insufficient in many cases. Consequently, two major trends have emerged: **AI-enhanced runtime monitoring** and **cloud-based forensic analysis**.

7.4.1 AI-Enhanced Runtime Monitoring and System Telemetry

Recent advances in **extended Berkeley Packet Filter (eBPF)** technology - i which began for filtering network traffic at the kernel level, now has new uses in mobile forensic analysis. Forensic researchers can put lightweight, sandboxed code inside kernel space and trace low level system activity such as process creation, file access, or memory modification in real time without modifying the operating system itself.

Forensic frameworks such as BPFroid, built for Android, use eBPF to monitor suspicious activity with machine learning models These models are trained on behavioral baselines and detect deviations indicative of spyware presence, such as unexpected dynamic library loads, persistent background data transmissions, or root-level access requests (Agman & Hendler, 2021).

Reference: Agman, T., & Hendler, D. (2021). *Detecting Mobile Malware with BPFroid: Leveraging eBPF on Android Devices*. Proceedings of the Workshop on Mobile Security Technologies.

Conclusion

Spyware detection and defense is no longer the exclusive domain of nation-states or elite cybersecurity firms. As tools like MVT and AndroidQF democratize access to mobile forensics, a new ecosystem of investigators, activists, and civic institutions is emerging. To sustain this progress, we must invest in **technology, law, and education** together - building a future in which surveillance is both **visible and accountable**, and in which the right to privacy is **defended by design**.

Chapter 8: Countermeasures & Recommendations

8.1 Personal-Level Protection

As advanced spyware like Pegasus and Predator spread, individuals need ways to mitigate the surveillance risk and keep digital privacy. A normal person probably cannot block all zero day exploits, but using good digital habits and defensive tools can make them much less open to attack.

One of the most effective recent innovations is the introduction of hardened operating system modes. Apple's "Lockdown Mode" introduced with iOS 16, turns off several services that attackers might use, which include link previews, just-in-time (JIT) JavaScript compilation, plus untrusted configuration profiles. This mode helps people at high risk, for example, journalists, diplomats along with activists - it already stopped certain zero click methods that Pegasus used (Amnesty International, 2021).

On Android, Google's Advanced Protection Program offers users more safety. It makes them use stronger ways to log in, stops apps that do not come from the Play Store, and limits how much data they share. Special security operating systems such as GrapheneOS improve Android safety; they do this by making memory use tougher, lowering permissions as well as allowing automatic reboots to remove spyware from memory (GrapheneOS, 2023).

Mobile antivirus and security apps can also help find spyware, though their use is small. Apps like Zimperium, Norton Mobile Security, also Kaspersky Mobile look for strange actions. They point out things such as the microphone turning on when not used, the battery losing power fast, or data moving in the background - they do not find spyware that stays hidden in memory, but they can show changes in how the system acts that might mean a problem (Lookout, 2024).

Behavioral precautions remain crucial. People should not click on links that look strange or that they did not ask for - this is especially true for links from SMS, messaging apps, or email. Turning off and on the device often can clean out spyware that stays in memory, for example, early Predator programs. Do not use public charging spots, turn off image previews, and limit what apps can do. That helps make fewer places for attackers to strike.

Some non profit groups as well as digital rights groups now provide ways to check devices for people who think someone targets them. Groups like Access Now, Amnesty International's Security Lab, and Citizen Lab offer help with forensics. They often use open source tools such as the Mobile Verification Toolkit (MVT). This tool scans iOS besides Android devices for signs of known spyware infection (Citizen Lab, 2021).

8.2 Institutional, Government & EU-Level Defenses

While personal security measures are important, the scope and scale of spyware deployment - often involving state actors - require systemic intervention at national and international levels. Organizations need to act to restrict the wrong use of spy tools. They also need to shield their people from illegal entry into their private lives.

8.2.1 Legal Frameworks & Regulation

The European Union took several legal actions to deal with the increasing danger of surveillance tools. The General Data Protection Regulation and the suggested ePrivacy Regulation set basic rights for data privacy; they demand openness, purpose limits along with fair use. But these rules did not start with military spyware in mind. More rules are necessary to handle the making, sending as well as local use of surveillance programs.

New plans, like the European Parliament's PEGA Committee, asked for closer checks. Their ideas include needing court approval to use spyware, required reports about its use, and creating separate groups to watch over it. In addition, the Dual-Use Regulation manages the export of sensitive tools, such as spyware, by requiring licenses. But problems still exist, particularly regarding transfers within the EU plus private company workers.

Outside the EU, the United States put NSO Group and other spyware sellers on its Entity List. This stops American companies from doing business with them - these actions seek to slow down the spread of spyware to governments that do not allow public freedom. They form part of a wider plan to put surveillance technology under international control.

Along with export checks, member states must put in place strict rules for buying items that control their own intelligence and law enforcement groups - they should only use surveillance tools with a court order. These tools must face review by parliament also independent groups should regularly check them - this includes not only national governments but also local bodies and groups that hire private businesses. If they do not do this, it could hurt democratic oversight.

8.2.2 Technological Infrastructure and Detection Systems

Governments and public groups use advanced network monitoring systems - these help them find spyware activity. The methods include DNS anomaly detection, TLS fingerprinting along with machine learning classifiers. These classifiers learn to spot command-and-control (C2) messages. Deep Packet Inspection (DPI) tools reveal

hidden attempts to send out data; these work well when they link with endpoint detection plus response (EDR) solutions (Cisco Talos, 2023).

Public sector IT systems should also add mobile threat defense systems. Zimperium zIPS or Lookout MTD are examples. These tools find risky settings, detect known threat signs, and watch for strange behavior on many devices. Putting these systems in government offices, healthcare groups as well as schools helps form a wider net against infections that spread.

The EU Agency for Cybersecurity (ENISA) suggested that member states set up national centers for forensics - these centers would study spyware infections also share what they learn across countries. When forensic labs and regulatory groups work together, it helps them react quickly as well as spread early warnings (ENISA, 2022).

8.2.3 Transparency, Audits, and Public Awareness

Public trust grows when people see what a government does. The government ought to show when it uses watch tools, particularly when it watches its own citizens. Public groups and private sellers could have a rule to put out reports about what they see, similar to how tech firms like Apple in addition to Microsoft do.

Separate checks should begin to look at buying plus using spy tools - these checks must include experts in technology and law to confirm they meet human rights rules. Groups that help people also schools should get money and legal support. This lets them look into matters, publish what they find, as well as sue if they need to.

Work to inform the public also matters. People need to know the dangers of digital watching and what they can do to keep safe. School projects, programs to teach about computers, plus news stories help build a society that knows more and can handle problems. People should learn to watch for dangers as policies change.

In sum, countering the threat posed by Pegasus, Predator, and similar spyware demands a coordinated, multi-layered approach. Individuals must stay watchful. Governments also need to change systems, prepare with technology, and put legal and ethical rules in place. This framework must show that the right to privacy matters as a main part of countries with democracy.

8.3 Strengthening Spyware Detection and Response

8.3.1 Institutional Recommendations

A. Standardized Forensic Protocols and Tooling

Security labs, human rights groups along with governmental Computer Emergency Response Teams (CERTs) ought to work together on a standard forensic response structure for mobile spyware. This involves:

- Common indicators of compromise (IoC) databases updated regularly through verified disclosures.
- Federated testing and benchmarking of forensic tools (e.g., MVT, AndroidQF).
- Shared infrastructure for submitting anonymized forensic traces to academic repositories or NGOs such as Citizen Lab or Amnesty Security Lab.

Investigators do not always agree on how to do their work. This causes them to repeat tasks and miss details about who is responsible. A single plan for responding to incidents would help find problems sooner - it would also improve how good the evidence is for arguments in court.

B. Regional Digital Security Hubs

The success of mobile forensic investigations in cases in Catalonia and Jordan show that local digital security centers are important - these centers sit within groups of people in the community. These hubs could:

- Train highly risked individuals to perform baseline forensics with MVT or AndroidQF.
- Act as intermediaries in incident escalation to global organizations.
- Collaborate with telecom providers to monitor for IMSI catchers or abnormal SIM activity.

Such clinics would not only detect threats but also serve as trust anchors for whistleblowers and victims of digital repression.

8.3.2 Legal and Policy Recommendations

A. Strengthen Legal Obligations for Notification and Transparency

States should mandate that platforms like Apple and Google issue prompt user notifications when targeted with known spyware, based on corroborated forensic data or

system heuristics. Citizen Lab's report on dual infections emphasized how Apple's notifications helped initiate broader investigations (Citizen Lab, 2021).

Additionally, spyware vendors should be compelled to publish annual transparency reports, detailing deployments, clients, and justification summaries (excluding sensitive operations). EU and UN bodies could impose export restrictions or procurement bans on non-compliant firms.

B. Enact Legal Safeguards for Victims and Researchers

Current legislation often fails to protect digital rights researchers and victims of surveillance. As such, we recommend:

- Legal immunity for accredited forensic analysts conducting public-interest investigations.
- Whistleblower protections for insiders at surveillance firms or telecom providers.
- Guaranteed access to digital redress mechanisms, including data correction and compensation procedures.

Legal frameworks such as the GDPR, while strong in principle, must be expanded with spyware-specific provisions and robust enforcement mechanisms.

8.3.3 Education and Public Awareness

Finally, broader public literacy in digital forensics and spyware risks remains essential. Governments and universities should launch campaigns to:

- Raise awareness of spyware threats, especially among journalists, activists, and political dissidents.
- Promote usage of secure messaging apps (e.g., Signal), hardened OS configurations (e.g., Lockdown Mode), and routine mobile hygiene practices.
- Provide forensic self-assessment kits and visual guides via public portals or nonprofit collaborations.

By embedding security awareness in civic education and professional training, societies can reduce their vulnerability to covert surveillance.

References

Amnesty International. (2021). Forensic Methodology Report: How to catch NSO Group’s Pegasus. https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/
Apple. (2022). Transparency Report. https://www.apple.com/legal/transparency/
Cisco Talos. (2023). Mercenary Intellexa Predator. https://blog.talosintelligence.com/mercenary-intellexa-predator/
Citizen Lab. (2021). Pegasus vs. Predator: Dissidents Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware. https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/
ENISA. (2022). Threat Landscape Report. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
European Commission. (2022). The GDPR and ePrivacy Regulation. https://ec.europa.eu/info/law/law-topic/data-protection_en
GrapheneOS. (2023). GrapheneOS Documentation. https://grapheneos.org
Lookout. (2024). Pegasus and Predator Technical Report. https://www.lookout.com/documents/threat-reports/us/predator-and-pegasus-tg-us.pdf
PEGA Committee. (2023). Final Report on the Use of Spyware in the EU. https://www.europarl.europa.eu/committees/en/pega/home/highlights
U.S. Department of Commerce. (2021). Entity List Additions. https://www.commerce.gov/news/press-releases

Chapter 9: Ethical Reflections and Final Conclusions

9.1 Ethical Reflections on Spyware Deployment

The use of advanced spyware, like Pegasus and Predator, raises basic ethic concerns. People wonder how to balance what the state needs for security with the need to protect individual freedoms. Governments have long thought that watching people is a necessary tool for national security and law enforcement. Using complex, hidden spyware against regular citizens, especially reporters, people who defend human rights, plus political rivals, goes against democratic rules.

Spyware programs work secretly; they avoid normal legal steps, and they leave few signs, so it is almost impossible for a democracy to watch also hold them accountable. When people use these tools without a clear legal reason and without independent checking, they risk making invasive watching normal. This stops free speech, disagreement along with journalistic work. Watching people crosses a moral line when it becomes a tool to control rather than protect.

The involvement of private businesses in making as well as selling watching tools presents another moral problem - these sellers often work in places with little oversight, and they sell their products to governments that have poor human rights records. Selling spying technology for money weakens the idea of balance that is important to democratic policing plus collecting information.

9.2 Advocating for Privacy as a Fundamental Right

The spyware discussion focuses on a larger principle - the right to privacy. Article 8 of the European Convention on Human Rights and the EU Charter of Fundamental Rights acknowledge privacy. This is not just a personal matter - it forms the basis of free thought, free association along with free speech.

People must see privacy as a right that changes with technology, which means that software and hardware should include privacy by design. Surveillance methods should be specific, clear as well as subject to public review.

Societies that operate under democratic rule should not accept that security excuses all types of surveillance. The assumption should change. Invading personal life should be rare - not common. It also must always have legal approval. The act must be necessary, and it must fit the situation. The talk should change from "how much surveillance can people allow" to "how do people protect privacy from illegal entry."

9.3 Toward a Future of Rights-Respecting Digital Governance

The revelations surrounding Pegasus and Predator should serve as a wake-up call. This thesis has demonstrated that these tools are not just abstract cyberweapons - they are actively used against real people, often without accountability.

To move forward, societies must:

- Set up global rules for selling surveillance technology.
- Strengthen domestic oversight bodies with independent powers of investigation.
- Foster partnerships between civil society, academia, and technology providers to improve forensic tools and transparency.
- Educate the public on privacy rights and empower citizens with knowledge and tools to detect and resist intrusive surveillance.

People should view digital rights as important for human respect and for democracy to last. They are not problems for safety. When people protect privacy, they show the importance of self rule, belief as well as freedom in a world that is more connected.

9.4 Final Words

Spyware poses a serious digital threat. This is not only because of its complex technology but also to the secret, unregulated systems where it grows - this paper shows the technical and legal features of that threat - it studied the cases of Pegasus in addition to Predator. It also presented ways to stop it plus future problems.

The fight for privacy is the fight for democracy. If surveillance is the tool of repression, then transparency, regulation, and digital literacy are our tools of resistance. Let this thesis not be a final word, but a call to action—toward a digital world where rights, not just power, shape the future.

Bibliography

Amnesty International. (2021). Forensic Methodology Report: How to Catch NSO Group's Pegasus.

Amnesty Tech. (2021). Mobile Verification Toolkit (MVT). Retrieved from https://github.com/mvt-project/mvt

Apple. (2022). Transparency Report.

Cisco Talos. (2023). Predator: Inside a Mercenary Spyware Operation.

Citizen Lab. (2021). The Pegasus Project: An Investigation into NSO Group's Surveillance Operations.

Deloitte. (2023). Unauthorized Surveillance and Breaches with Predator and Pegasus.

ENISA. (2022). Threat Landscape for Spyware and Surveillance Tools.

European Commission. (2022). Data Protection and Privacy in the Digital Age.

Foucault, M. (1977). Discipline and Punish: The Birth of the Prison. Pantheon Books.

GrapheneOS. (2023). Hardened Android Operating System. Retrieved from https://grapheneos.org/

Lookout. (2021). Pegasus: The Invisible Spy. Lookout Threat Report.

Lookout. (2024). Pegasus and Predator Technical Analysis.

Marczak, B., Scott-Railton, J., & Deibert, R. (2021). ForcedEntry: NSO Group iMessage Zero-Click Exploit Captured in the Wild.

PEGA Committee. (2023). Final Report on the Use of Pegasus and Equivalent Surveillance Spyware.

Recorded Future. (2024). Predator Spyware Infrastructure Returns.

U.S. Department of Commerce. (2021). Entity List Additions: NSO Group and Candiru.

---

i