Introduction

Pegasus is an extremely advanced piece of spyware developed by the Israeli company NSO Group. It is capable of covertly infecting smartphones (iPhones and Android devices) without the owner's knowledge and giving attackers near-total access to the device

. NSO Group advertises Pegasus for law enforcement and counterterrorism, but in reality the tool has been widely abused – governments across the world have used Pegasus to secretly surveil journalists, human rights defenders, lawyers, and political opponents

. The spyware gained global notoriety in 2021 when the **Pegasus Project** (a media consortium investigation) revealed a leaked list of about 50,000 phone numbers selected for targeting by Pegasus clients, suggesting widespread abuse and prompting international outrage

. Since then, Pegasus has become a focal point in debates about cybersecurity, privacy, and the unchecked use of surveillance technology by state actors.

Origins and Development

Pegasus was first developed around 2011 by NSO Group, a private Israeli "cyber-intelligence" firm founded in 2010

. (The company's name "NSO" actually comes from the initials of its founders Niv Carmi, Shalev Hulio, and Omri Lavie

.) From the beginning, NSO Group's business model has been to sell spyware and cyber-intelligence tools to government agencies worldwide, with the stated intent of helping combat serious crime and terrorism

. Pegasus is considered a military-grade cyber weapon – in fact, Israel's government regulates it as an export-controlled product, requiring NSO to obtain export licenses and approval before selling it abroad

For its first few years, Pegasus operated in the shadows. It wasn't until August 2016 that Pegasus's existence became public knowledge, when a suspicious SMS link sent to UAE human rights activist Ahmed Mansoor was analyzed by Citizen Lab and Lookout Security

. Investigators discovered the link was designed to silently jailbreak Mansoor's iPhone and install NSO's spyware – an unprecedented iPhone compromise using three previously unknown ("zero-day") vulnerabilities

. Apple was alerted and rushed out an iOS patch (iOS 9.3.5) within days to close the flaws

. This 2016 incident – dubbed the "Million Dollar Dissident" case – was the first public evidence of Pegasus and revealed that NSO's tool had likely been in active use for years prior

. In fact, subsequent investigations found signs that Pegasus was deployed as early as 2013 by the UAE and had been sold to other countries (a leak showed Panama's government obtained it in 2015)

. From 2016 onward, more information about Pegasus's evolution began to surface: NSO Group continuously improved the spyware with new exploits to keep up with smartphone updates, and by the late 2010s Pegasus had added capabilities to infect Android devices as well (Google researchers identified an Android variant known as "Chrysaor")

. Despite growing controversy, NSO continued to thrive through the 2010s, selling Pegasus to dozens of government clients around the world.

Technical Capabilities

Once Pegasus successfully infiltrates a phone, it can essentially **take full control** of the device, turning it into an all-purpose surveillance tool. The spyware operates with deep system privileges, effectively bypassing or disabling security features (using a "jailbreak" on iPhones or rooting on Android)

. This allows Pegasus to run in stealth mode and avoid detection while it monitors the device. Pegasus can read or siphon off virtually all of the phone's data: it can copy text messages, call logs, contacts, emails, photos, and web browsing history

. It can track the phone's GPS location in real time and harvest information from apps – including encrypted messaging apps like WhatsApp, Signal, Telegram, etc., by capturing messages *before* or *after* they are encrypted

. Notably, Pegasus can also secretly activate the device's **microphone and camera**, turning the phone into a live spying bug to eavesdrop on conversations or snap pictures without the user's knowledge

. In short, an attacker wielding Pegasus gains the equivalent of a remote "administrator" of your phone – able to see and hear almost everything on it – while the victim is left in the dark. Pegasus achieves all this while hiding itself and even cleaning up traces; NSO has claimed the spyware *"leaves no traces whatsoever"*, though forensic experts have found ways to identify its remnants on compromised phones

Diagram from leaked NSO Group documentation (via Citizen Lab) illustrating the data Pegasus can extract from an infected phone – including messages, emails, calls, location, photos, and activation of the mic and camera

Another frightening capability of Pegasus is its proficiency at **evading detection and removal**. Because it operates at the deepest levels of the operating system, traditional antivirus software (which is scarce on mobile phones to begin with) often cannot detect it. Pegasus is also designed to be modular and adaptive – it can receive new commands or software modules from its operators via encrypted communications with its command-and-control servers

. For example, an operator can remotely instruct Pegasus to begin recording from the microphone, or to exfiltrate a specific file or chat history, and the spyware will dutifully comply. Pegasus usually

avoids actions that might obviously alert the user (for instance, it can upload data in small chunks to avoid noticeable spikes in network usage). All these features make Pegasus a *highly potent and covert surveillance tool*, often described by experts as a "weaponized" spyware platform.

Methods of Infection

Pegasus infection can occur through multiple vectors, ranging from deceptive phishing messages to incredibly sophisticated zero-click exploits. Early versions of Pegasus often relied on **social engineering**: the target would receive a phishing message containing a malicious link, and if they were tricked into clicking it, their device would be silently compromised

. This was the method used against Ahmed Mansoor in 2016 – a text promised "secrets" about torture in UAE prisons with a link, which would have installed Pegasus had he clicked

. In many documented cases, Pegasus operators sent specially crafted SMS or WhatsApp messages tailored to entice the target into clicking (for example, posing as breaking news, bank alerts, or personal messages)

. Once the link was clicked, the Pegasus exploit server would deliver a chain of exploits to penetrate the phone's defenses and install the spyware

More alarmingly, Pegasus has evolved to employ **"zero-click" infection** techniques – meaning the spyware can install itself without *any* user interaction. In these scenarios, the target might simply receive a call or message that they never even see, yet their device gets infected automatically. Pegasus has leveraged undisclosed vulnerabilities ("zero-days") in popular apps and phone systems to achieve this. For example, in 2019 WhatsApp revealed that Pegasus had been deployed via a missed WhatsApp call exploit – the mere act of receiving the incoming call (even without answering) allowed Pegasus to penetrate the phone

. Similarly, Pegasus operators have used zero-day flaws in Apple's iMessage service to push spyware onto iPhones with no user action – one such exploit, dubbed **FORCEDENTRY**, involved sending a malicious image file that automatically ran code on the device to install Pegasus

. These zero-click attacks are virtually invisible to the target: a phone might briefly light up with an incoming message or call, or sometimes not at all, and there would be no lasting trace in the messaging app. This "silent" infection capability is part of what makes Pegasus so dangerous and difficult to stop.

Under the hood, these infections exploit weaknesses in software. Pegasus's developers invest heavily in finding or buying **zero-day vulnerabilities** – unknown bugs in iOS, Android, and common apps – and crafting exploits for them. In the 2016 Mansoor case, researchers found Pegasus used *three* separate zero-days in iOS to jailbreak the phone and install itself

. Over the years, NSO's arsenal reportedly included exploits for iPhone web browsing (WebKit), the kernel, WhatsApp voice calls, iMessage, and more

. By the time these vulnerabilities become publicly known (for instance, through an Apple patch or a WhatsApp update), Pegasus may already have moved on to new exploits. This cat-and-mouse game

enables Pegasus to infiltrate even up-to-date, well-secured devices. As a fallback, if high-tech silent attacks fail, Pegasus can still attempt more traditional installation methods – e.g. persuading a target to install a fake application or using physical access to the device – but such cases are rarer. The hallmark of Pegasus operations in recent years is the **zero-click remote exploit** that catches even the most cautious users off-guard

. In short, Pegasus can find a way in through either human error (phishing) or software error (vulnerabilities), with devastating effectiveness.

Global Incidents and Usage

While NSO Group insists that Pegasus is only sold for legitimate crime-fighting, a growing body of evidence shows **Pegasus has been misused in numerous countries against civil society and political targets**. Investigations by cybersecurity labs and journalists have uncovered Pegasus operations on **almost every continent**, often targeting those who speak out against powerful governments. Below are some of the most notable documented incidents and abuses involving Pegasus spyware:

- **UAE (2016)** – The attempted Pegasus attack on **Ahmed Mansoor**, a prominent Emirati human rights defender, was the first to be uncovered and stopped by researchers

. Mansoor, who had been previously targeted with other spyware, received an SMS with a malicious link. This case exposed Pegasus to the world and showed that even a Gulf country was using it to surveil a peaceful dissident. Citizen Lab later revealed that Mansoor had been in Pegasus's crosshairs as early as 2013

. Despite the public exposure, Mansoor was eventually jailed by UAE authorities (on unrelated charges), highlighting how activists remain at risk

- **Mexico (2016-2017)** – Mexico became infamous for its domestic use of Pegasus. In 2017, revelations (the *#GobiernoEspía* scandal) showed that dozens of Mexican journalists, lawyers, anti-corruption investigators, and activists had their phones targeted with Pegasus links

. For example, scientists opposing sugary drink policies and even minor children of government critics were targeted. These abuses sparked an outcry and a criminal investigation in Mexico

. Ironically, Mexican authorities were also Pegasus's earliest "success story," reportedly using it to help capture drug lord **El Chapo** in 2016

. This juxtaposition – being used to both catch cartel criminals *and* spy on civic activists – underscored the spyware's dual-edged nature in Mexico.

- **Saudi Arabia & Pegasus's role in Khashoggi's murder (2018)** – Perhaps the most chilling case was Pegasus's involvement in the Saudi operation against journalist **Jamal Khashoggi**. In the months leading up to Khashoggi's assassination in October 2018, Saudi operatives used Pegasus to infect the phones of people close to him (including his wife and several associates)

. This allowed Saudi intelligence to monitor Khashoggi's private communications and movements

. Investigations confirmed that Pegasus had been deployed against Khashoggi's inner circle, and a lawsuit later alleged that data obtained via Pegasus contributed to planning his killing

. The Khashoggi case drew global condemnation – it starkly illustrated how spyware can facilitate human rights atrocities.

- **Pegasus Project revelations (2021)** – The Pegasus Project, a consortium of media outlets coordinated by Forbidden Stories and Amnesty International, provided the biggest window yet into Pegasus's global spread

. Their July 2021 reports identified **potential targets in more than 50 countries**, including activists, journalists, lawyers, and politicians. Notably, **at least 180 journalists** from outlets around the world appeared on Pegasus target lists

. The investigation also showed heads of state and high-ranking officials were selected as targets: for example, French President **Emmanuel Macron**, South African President **Cyril Ramaphosa**, Pakistani Prime Minister **Imran Khan**, and the King of Morocco **Mohammed VI** were all reportedly on the list of numbers chosen for Pegasus targeting

. These revelations suggested that some NSO clients were using Pegasus for diplomatic or espionage purposes far outside the realm of "criminal investigation." The French government was outraged at Macron's inclusion, and it prompted high-level diplomatic tensions (France even changed President Macron's phone and number as a precaution)

.

- **Europe (2019-2022)** – Although Pegasus is often associated with authoritarian regimes, its use has been detected in democracies as well. For instance, **Hungary** admitted in 2021 that its Interior Ministry had purchased and used Pegasus – investigations found that dozens of Hungarian journalists, media owners, and opposition figures were surveilled, allegedly on orders of the government

. In **Poland**, evidence emerged that Pegasus was used to hack the phones of opposition politicians and a prosecutor, leading to a scandal and an inquiry by Poland's Senate in 2022. **Spain** faced its own Pegasus controversy when Citizen Lab revealed that at least 65 Catalan separatist politicians and activists were spied on (the so-called "CatalanGate"), raising questions about abuses by the Spanish security services. **Israel** – the home country of NSO – also had a domestic scandal: reports alleged that Israeli police improperly deployed Pegasus against Israeli citizens without warrants, leading to a public outcry and investigations

. These cases show that Pegasus has been used in secret surveillance even in countries with strong democratic institutions, blurring the line between national security needs and unlawful spying.

The above examples are just a sampling of Pegasus's reach. Other confirmed cases span **India** (where dozens of opposition leaders, journalists, and activists were identified as targets, sparking a Supreme Court inquiry), **Morocco** (accused of spying on journalists and French officials), **Rwanda**

(allegedly using Pegasus to monitor dissidents abroad), **United Arab Emirates** and **Bahrain** (hacking the phones of exiled dissidents and human rights defenders)

, and many more. In 2022, Poland's use of Pegasus and similar tools even prompted the European Parliament to set up a committee (PEGA) to investigate spyware abuse within EU states. In short, Pegasus has been implicated in a **global web of surveillance incidents**, from North America and Europe to Asia, Africa, and the Middle East. Its misuse against journalists and activists is so widespread that organizations like Amnesty International and Citizen Lab have called Pegasus a tool of "unlawful surveillance and human rights abuses" on a massive scale

.

Legal and Ethical Implications

The proliferation of Pegasus spyware has triggered serious legal and ethical questions about privacy, human rights, and the regulation of cyber surveillance. A fundamental concern is how to protect individuals from intrusive surveillance by their own governments or foreign entities – especially when such sophisticated tools are available for purchase. Pegasus effectively enables **warrantless wiretapping** and covert search of personal devices on a scale never seen before, raising issues under privacy laws and constitutional rights in many countries. Human rights experts argue that Pegasus has been used to facilitate human rights violations (harassment, unlawful arrests, even potential extrajudicial violence as in the Khashoggi case), calling it a threat to freedom of expression and dissent

. In response, there have been mounting calls for greater oversight and accountability for spyware companies like NSO and their government clients

.

Several **lawsuits and legal actions** have been launched to curb Pegasus's misuse. In 2019, Facebook (now Meta) and its subsidiary WhatsApp sued NSO Group in a U.S. federal court, after discovering that NSO had exploited a vulnerability in WhatsApp to infect approximately 1,400 users' phones with Pegasus

. That lawsuit alleged NSO violated U.S. anti-hacking laws, and in 2021 a U.S. judge ruled that NSO does not have sovereign immunity (despite selling to governments) and could be held liable for the WhatsApp attacks

. Separately, Apple Inc. filed a lawsuit against NSO Group in late 2021, accusing the company of flagrantly violating Apple's terms of service and targeting Apple's customers with spyware

. Apple sought to bar NSO from using any Apple software or services. In an unusual move, Apple also began **notifying victims** of suspected state-sponsored spyware attacks – dozens of iPhone users around the world received alerts that their device may have been targeted by Pegasus, further spotlighting the issue.

Government authorities have also taken action. Notably, the United States Department of Commerce added NSO Group to its **export blacklist (Entity List)** in November 2021, citing Pegasus as a threat to U.S. national security and interests

. This sanction bars U.S. companies from providing technology or support to NSO, hampering its operations. Additionally, the U.S. government in 2023 announced it would impose visa bans on officials of any country misusing commercial spyware against civil society

. In Europe, the EU Parliament's PEGA committee in 2022 investigated Pegasus abuses in member states and has called for stricter EU-wide regulations on spyware. Several countries have launched national probes or court cases: e.g. France and India are examining allegations of Pegasus use against their citizens, and Hungary's data protection authority actually concluded that Hungarian intelligence's use of Pegasus was lawful (a result that many found unsatisfactory). Meanwhile, NSO Group claims it has an internal compliance process and has cut off some clients for abuse, but it faces heavy skepticism. In one case, an Israeli court ordered NSO to **hand over the source code** of Pegasus to aid the WhatsApp lawsuit's discovery process

– a significant legal pressure on the normally secretive firm.

All these developments underscore a larger ethical debate: **How should surveillance technology like Pegasus be controlled?** On one hand, law enforcement and intelligence agencies argue that tools like Pegasus are vital for national security – enabling them to track terrorists and criminals who increasingly "go dark" behind encryption. On the other hand, the Pegasus scandal has exposed *alarming regulatory gaps* in the sale and use of such spyware

. Unlike traditional weapons, cyber weapons like Pegasus have been loosely regulated, allowing private companies to trade them globally with limited oversight. The fact that authoritarian regimes have readily bought Pegasus to target dissidents shows the danger of treating such spyware as just another export commodity. Many observers and rights organizations are calling for stronger international frameworks – potentially a ban or moratorium on the export of spyware to governments with poor human rights records

. Others urge stricter liability for companies like NSO and even for the states that use these tools, to create accountability for abuses. So far, the Pegasus controversy has prompted more scrutiny – lawsuits, sanctions, and inquiries – but it remains to be seen if these will coalesce into effective regulation. The ethical challenge is striking a balance between legitimate needs for surveillance and the protection of privacy and civil liberties in a digital age where a phone can be turned into a spy device without its owner ever noticing.

Countermeasures and Detection

Pegasus is notoriously difficult to defend against, especially for the average individual, but there are steps that high-risk users and organizations can take to *mitigate* the threat of spyware infections. Cybersecurity experts emphasize a combination of good security hygiene, specialized defensive features, and rigorous monitoring to counter tools like Pegasus:

- **Keep devices updated**: Since Pegasus relies on exploiting software vulnerabilities, it's critical to install operating system updates and security patches as soon as they are released. Regular updates can fix the known flaws that spyware might use to get in. (For example, the 2016 Pegasus iPhone attack was thwarted once Apple issued an iOS patch

.) While zero-day exploits can bypass even fully updated phones, staying updated closes easier paths of attack

- **Practice cautious behavior**: Avoid clicking on links or attachments from unknown or suspicious messages – this basic precaution can foil many phishing-based attacks

. Users should also be wary of unusual calls or prompts (e.g. repeated missed calls from unknown numbers on WhatsApp). High-risk individuals might consider using separate devices or accounts for sensitive communications to limit exposure.

- **Use smartphone security features (e.g. Lockdown Mode)**: In 2022, Apple introduced an optional **Lockdown Mode** for iOS 16, designed specifically to protect users at risk of targeted spyware. When enabled, Lockdown Mode restricts or disables certain features (like unsolicited iMessage attachments, link previews, JavaScript just-in-time compilation, etc.) to reduce the attack surface that Pegasus and similar spyware rely on. This mode has been hailed by experts as *"the best defense we have today for Pegasus and Predator spyware"*

, although it comes at the cost of some convenience. For those who can tolerate the trade-offs (primarily journalists, activists, and others who suspect they could be targeted), enabling Lockdown Mode provides an extra layer of protection – so far there are no public reports of Pegasus bypassing it

.

- **Disable unneeded apps/services**: Some security researchers suggest turning off or uninstalling apps that you don't use, especially messaging apps that have been exploited by Pegasus. For instance, if you do not need Apple's iMessage or FaceTime, disabling them could block certain zero-click vectors

. Similarly, using hardened messaging apps or alternate communication methods for sensitive conversations might help. Essentially, by minimizing the avenues of attack, you make it harder for spyware to find a way in.

- **Use detection and monitoring tools**: Detecting Pegasus is very challenging, but not impossible. Amnesty International's Security Lab released an open-source tool called **MVT (Mobile Verification Toolkit)** to help users scan their iPhone or Android backups for indicators of Pegasus infection

. There are also apps like iVerify (for iOS) that can check a device for known spyware traces on a continuous basis (iVerify found Pegasus on multiple phones in recent scans)

. Tech companies like Apple and Google have also begun alerting users if they suspect a device has been targeted by Pegasus or similar spyware. Users at high risk should regularly audit their device logs and network traffic if possible – unusual symptoms like sudden battery drain, unexpected reboots, or strange messages can be warning signs, though Pegasus generally tries to avoid detection

. Organizations can engage professional digital forensics experts to analyze devices for compromise if they have reason to suspect spyware; forensic analysis has successfully uncovered Pegasus infections by finding telltale artifacts in phone logs and memory

- **Network defenses and isolation**: Enterprises and governments worried about Pegasus can employ mobile device management (MDM) solutions and network monitoring to detect anomalies. For example, DNS monitoring might catch a phone trying to contact known Pegasus command-and-control domains, alerting security teams (though Pegasus can use rotating domains and encryption to obfuscate its traffic). High-security environments may also enforce policies like periodic device rebooting (in some cases, restarting an iPhone can temporarily disable Pegasus until it re-infects via persistence mechanisms) or even prohibit smartphones in sensitive meetings to prevent eavesdropping.

Despite these countermeasures, it is important to note that **no defense is foolproof** against a tool as resourceful as Pegasus. Well-funded attackers (often nation-states) can develop new exploits to get around security features. As one cybersecurity memo quipped, truly stopping Pegasus might require giving up modern smartphones altogether – an impractical solution for most. However, the goal of countermeasures is to *raise the cost and difficulty* for attackers, and to detect breaches as quickly as possible. By staying informed about the latest threats, using available protective features (like Lockdown Mode), and employing rigorous security practices, individuals and organizations can significantly reduce the risk of Pegasus compromises

. The ongoing development of defensive tools – such as antivirus scans for mobile, anomaly detection scripts

, and improved encryption of phone internals – will hopefully tilt the balance in favor of defenders over time.

Future Outlook

The Pegasus saga has demonstrated that commercial spyware is a thriving industry with serious geopolitical implications. Looking ahead, experts predict that spyware like Pegasus will continue to **evolve** and proliferate unless stronger curbs are put in place. NSO Group and its competitors (companies like Candiru, Cytrox, Intellexa and others marketing similar spyware) are constantly researching new exploits to defeat the latest security enhancements on phones. In 2022, for instance, Citizen Lab reported that NSO had already developed a *trio of new zero-click exploit chains* capable of penetrating iPhones running iOS 15 and 16

– indicating that Pegasus was adapting to Apple's latest software. We can expect this cat-and-mouse dynamic to continue: as Apple and Google patch one hole, spyware developers will attempt to find or create another. There is also a risk of **wider availability** of such tools – while Pegasus is sold to governments, the underlying vulnerabilities could be discovered by criminal hackers or rival states, leading to potential copycat malware. The longer a lucrative market exists for offensive cyber tools, the more companies (or even governments themselves) will be incentivized to build their own Pegasus-like capabilities.

On the other hand, the worldwide backlash against Pegasus may *constrain its future*. NSO Group has faced financial and legal troubles due to mounting lawsuits and sanctions; reports suggest the

company's valuation has plummeted and it has had difficulty retaining clients under the glare of bad press. If NSO were to falter, however, other players might simply fill the void – the demand for such spying tools among governments is not likely to disappear. This raises the question of an international response. So far, the response has included blacklisting NSO by the U.S.

, and initiatives at the EU and UN level calling for tighter control of spyware exports

. In March 2023, U.S. President Biden signed an executive order banning federal agencies from using commercial spyware like Pegasus that pose security risks or have been misused against activists

, which could set an example for other democracies. There are discussions about establishing global norms or agreements to regulate the sale of cyber surveillance tools – akin to arms control treaties for digital weapons. Such measures could include requiring transparency and human rights due diligence before companies sell spyware to a government

, and perhaps an independent international body to investigate abuse claims.

Technologically, smartphone vendors will continue hardening their platforms. Google's Android and Apple's iOS are adding more lockdown features and exploit mitigations (e.g., Apple's BlastDoor sandbox for messages, rapid security response updates, etc.) specifically because of Pegasus-like threats

. Security researchers are also focusing on detection; for example, antivirus companies like Kaspersky have announced new methods to detect Pegasus on devices

, and academic efforts are underway to develop spyware-resistant phone architectures. In an ideal scenario, these defensive advances, combined with legal pressure, could significantly curtail Pegasus's reach over the next few years.

However, the **cat-and-mouse game** is likely to persist. As long as there are undiscovered software vulnerabilities and buyers willing to pay for spyware, tools like Pegasus (or its successors under different names) will pose a threat. We may see spyware becoming even more stealthy, employing techniques like zero-day exploits in baseband (cellular modem) code or novel attack vectors such as cloud service exploits that bypass the phone entirely. The global community's challenge will be to adapt legal frameworks at the same pace as the technology. The Pegasus scandal has *exposed critical gaps in oversight* of surveillance tech

– whether those gaps will be filled by effective regulation remains uncertain. What is clear is that Pegasus has served as a wake-up call. It has highlighted the need for greater transparency in cyber-intelligence contracting, stronger safeguards for targets (like notification and legal recourse), and perhaps a rethink of how we balance national security with digital privacy. In the coming years, the legacy of Pegasus might be a set of new laws and norms that ensure the "global spyware industry" cannot operate unchecked. Failing that, we risk entering a future where any government agency (and by extension, potentially any motivated hacker with resources) can silently rifle through the pockets of anyone in the world – a dystopian scenario of ubiquitous surveillance. The world's response in the near term – through policy, technology, and advocacy – will determine whether Pegasus remains an outlier or the blueprint for a troubling new normal in cybersecurity.

Sources: Recent investigative reports, technical analyses, and news articles have been cited throughout this report to provide factual evidence and insights into Pegasus spyware and its impacts. These include research by Citizen Lab and Amnesty International, credible news outlets like *The Washington Post*, *The Guardian*, and *The New York Times*, as well as expert commentary

. These references offer a trail for further reading on each aspect of the Pegasus story discussed above.