From Pegasus to Pall Mall

Managing Risks of Commercial Spyware

From Insikt Group®

Summary

Commercial offensive cyber capabilities include vulnerabilities and exploits, surveillance-focused malware, and command-and-control (C2) infrastructure sold by private vendors (mainly to governments). Over 80 countries have used such tools.

The misuse of commercial spyware threatens the broader cyber ecosystem by proliferating critical vulnerabilities and enabling widespread human rights abuses, especially in countries with weak oversight.

The Pall Mall Code of Practice (CoP), which has been signed by 25 countries, aims to curb the irresponsible proliferation and use of cyber intrusion tools through voluntary measures promoting transparency, oversight, and alignment with international human rights law.

Countries that implement clear legal frameworks may further legitimize cyber intrusion companies operating in their country, helping the industry grow in ways that support responsible use. However, rising authoritarianism is likely to create alternative markets for surveillance products to be used in ways that violate international human rights principles.

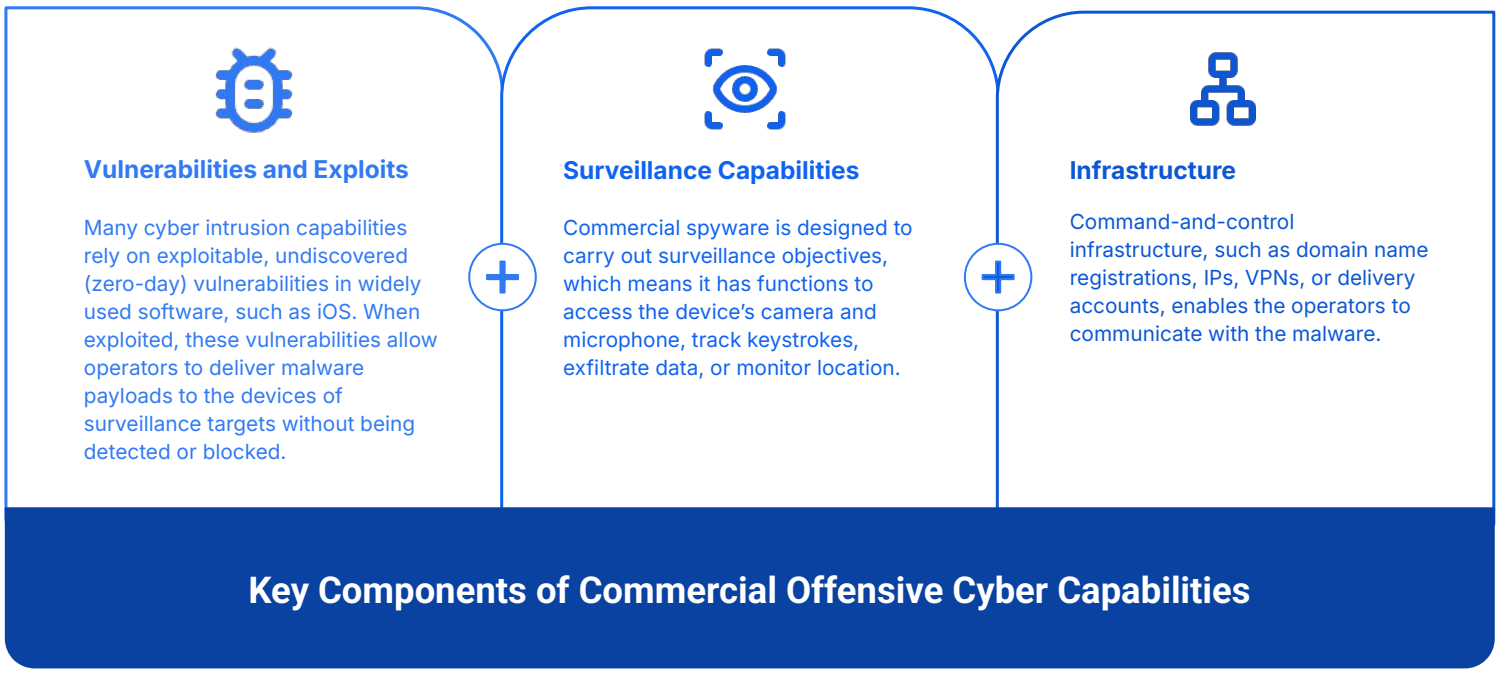
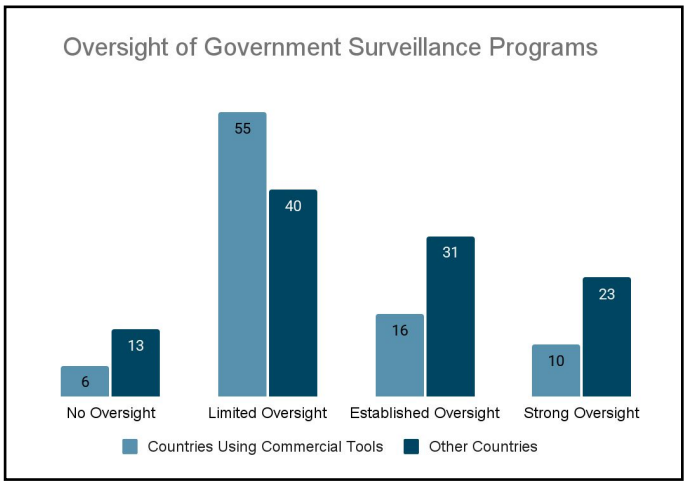


Figure 1: *Offensive cyber capabilities consist of multiple components that are sourced through a complex network of vendors, service providers, sub-contractors, and individual researchers (Image source: Recorded Future)*

Analysis

Commercial offensive cyber capabilities refer to cyber tools, platforms, and services offered by private companies to conduct intrusive cyber operations, typically for espionage or surveillance. The size of the commercial spyware industry is unknown. One study identified 435 entities operating across 42 countries. However, this is likely a fraction of the total ecosystem, which includes holding companies, vendors, individual researchers, and investors. Over 80 countries have reportedly purchased spyware. Many companies in this space claim to sell only to governments, typically for law enforcement, military, or intelligence purposes.

There are two primary categories of risk associated with the use of commercial cyber intrusion capabilities. The first is **proliferation**, the unmanaged spread of cyber intrusion capabilities or vulnerabilities that threaten the broader cyber ecosystem. Unpatched vulnerabilities in particular pose a risk to anyone using the relevant technology, not just the intended target. One of the most notorious examples is the leak of EternalBlue, an exploit allegedly developed by the US National Security Agency (NSA) that was later used in WannaCry ransomware. In a more recent example, exploits previously used by spyware vendors Intellexa and NSO Group were used by Russian state-sponsored threat actors in attacks targeting Mongolian government websites.



State Surveillance Risk Notes - Governance Overview	
No oversight	Reporting does not identify any oversight or judicial review process
Limited oversight	Reporting identifies that some oversight may exist but is undermined by corruption or weak governance
Established oversight	Reporting identifies that the country has a system of oversight and an independent judiciary
Strong oversight	Reporting identifies a comprehensive or strong system of oversight

Figure 2: *According to Recorded Future's country risk data, the majority of countries that are assessed or confirmed to use commercial offensive cyber tools have limited oversight into their use (Source: Recorded Future)*

The second category of risk is **human and civil rights violations.** According to Recorded Future's country risk data, 63% of countries observed using commercial off-the-shelf surveillance tools have limited oversight capabilities, meaning they lack an independent judiciary or oversight body capable of monitoring and restraining surveillance activities. Dozens of countries around the world have deployed commercial surveillance tools against political dissidents, journalists, lawyers, and others. Pegasus spyware, developed by the NSO Group, was found on the devices of journalist Jamal Khashoggi and his family and associates after his 2018 murder at the Saudi consulate in Türkiye. States have used surveillance technology to harass and intimidate targets, eroding privacy, free speech and assembly, freedom of movement, and other human rights. This has occurred in democracies like Mexico, Greece, and Spain, highlighting that the misuse of surveillance tools is a global challenge, not confined to authoritarian regimes.

In 2024, the UK and France launched the Pall Mall Code of Practice (CoP), an international framework regulating commercial cyber intrusion capabilities (CCIC). The 25 signatories committed to limiting the proliferation and misuse of offensive cyber tools by promoting accountability, oversight, precision, and transparency. The CoP encourages greater transparency in the vulnerability supply chain, adoption of disclosure policies that balance security risks against offensive value, and regulation of commercial tool use in line with human rights law. Examples include implementing know-your-customer requirements to prevent sales to rights-abusing entities.

Figure 3: *The United Kingdom and France led the Pall Mall Process, which culminated in the Pall Mall Code of Practice (Source: X)*

Pall Mall signatories pledge to establish national laws and regulations governing the use and export of cyber intrusion capabilities. Most already have strong oversight mechanisms and can expand them to close existing gaps, such as restricting the export of cyber tools to entities likely to abuse them. The Pall Mall Code of Practice follows earlier voluntary diplomatic commitments, including the US-led Guiding Principles on Government Use of Surveillance Technologies (developed by consensus in the Freedom Online Coalition).

Figure 3: *Pall Mall signatory countries are more likely than non-signatory countries to have strong oversight over government surveillance programs (Source: Recorded Future)*

The CoP is most likely to curb abuses by companies that do business with signatory governments and their partners, including major spyware vendors such as Candiru, NSO Group, and Intellexa. Signatories voluntarily commit to implement legal frameworks and accountability mechanisms, including export controls, licensing agreements, and procurement controls, that deter or prohibit irresponsible use of these tools. The majority of Pall Mall signatories have robust oversight of their surveillance programs, so it is likely these laws will be effectively implemented and enforced.

However, less than half of Pall Mall signatories use commercial surveillance tools, while even fewer are home to major offensive cyber firms, potentially limiting the CoP's impact. The new regulations may also fragment the Western cyber capabilities industry, as some vendors shift to less-regulated environments.

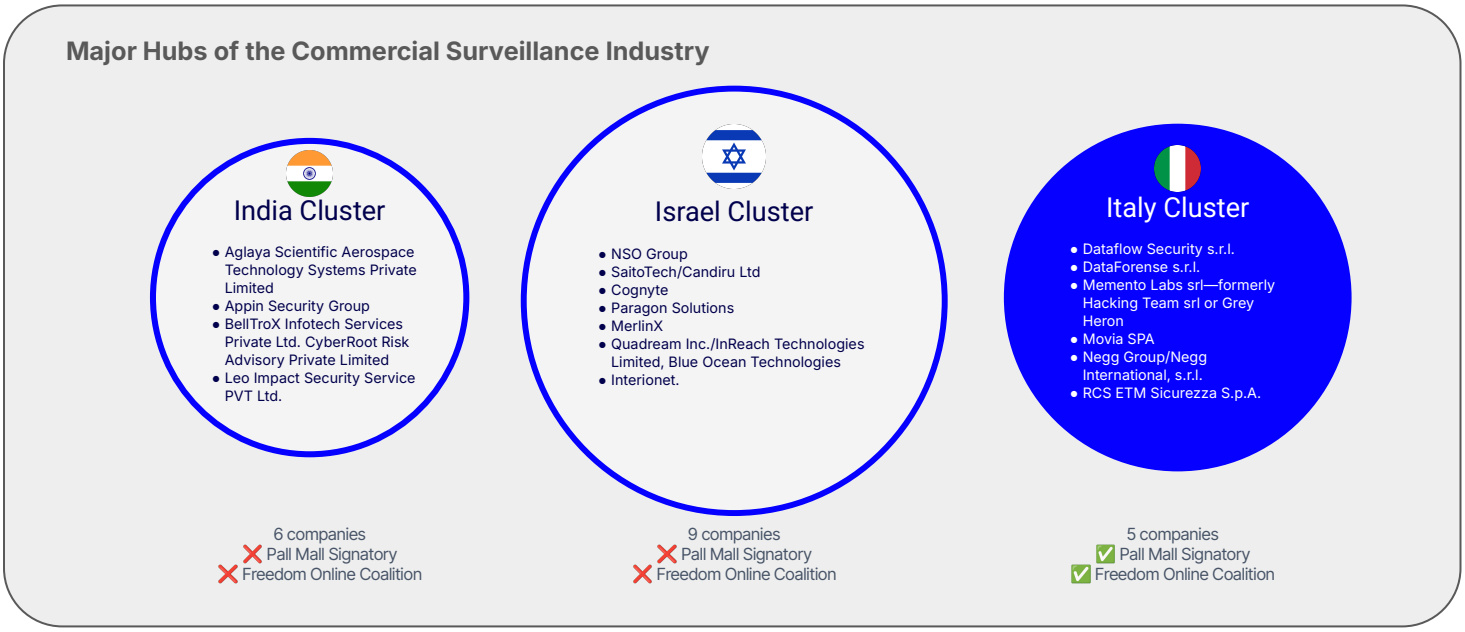


Figure 4: *Based on an assessment of 435 entities in the cyber surveillance industry, researchers at the Atlantic Council observed that the majority of offensive cyber firms operate out of three countries; of these, only Italy is a signatory to the Pall Mall CoP or a member of the US-led Freedom Online Coalition (Source: The Atlantic Council; Image: Recorded Future)*

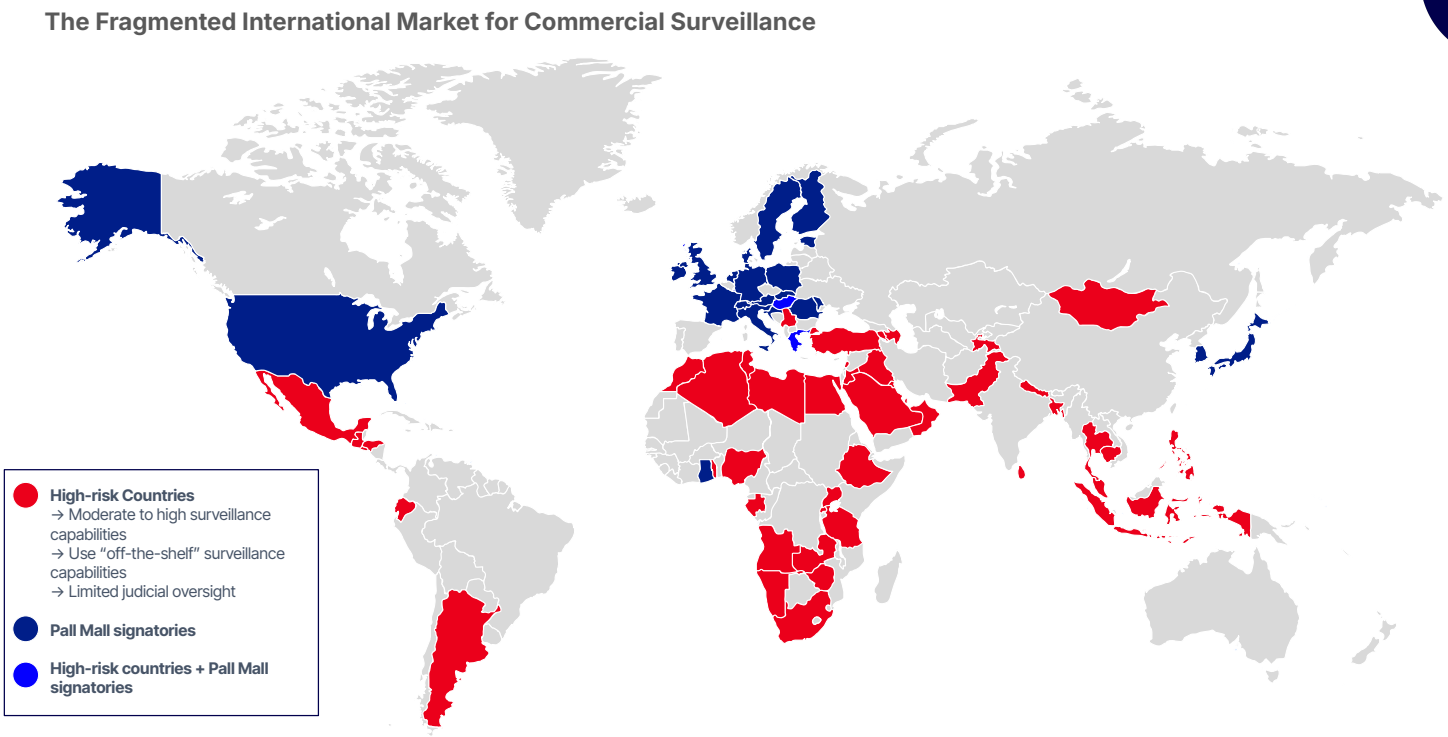


Figure 5: *The commercial offensive cyber capability industry will likely split to serve either Pall Mall signatories (in dark blue) and markets at high risk of abusing commercial surveillance tools (in red) (Source: Recorded Future)*

Furthermore, the Pall Mall CoP will almost certainly have limited influence on countries with abusive surveillance practices that rely on alternative tools or direct interference in telecommunications. For example, Russia exports its System for Operative Investigative Activities (SORM) to neighbors and, increasingly, to partners in Central Asia and Latin America, embedding surveillance at the ISP level to enable mass monitoring without compromising individual devices. Similarly, China has promoted Huawei-based "Safe City" systems in several African capitals. China also supports a robust vulnerability research ecosystem, accounting for 30% of all detected zero-days in 2024. These practices represent a significant proliferation of cyber vulnerability risk that is unlikely to be curtailed by Pall Mall-oriented regulations.

Figure 6: *Huawei is expanding its "Safe City" surveillance products into Uganda and other African countries (Source: The Africa Report)*

Outlook

The Pall Mall Code of Practice will likely accelerate fragmentation in the commercial cyber intrusion industry: By adopting regulatory frameworks aligned with the CoP, signatories commit to working only with companies that demonstrate responsible use. This shift will affect not only direct providers of surveillance capabilities but also their vendors and subcontractors, reshaping supply chains. As a result, the industry will likely splinter: Some companies will adapt to CoP markets, while others will deliberately avoid them, deepening the divide between regulated and unregulated players. This will also likely shift which countries act as spyware industry "hubs," forming new powerhouses outside of India, Israel, or Italy that cater to specific markets.

Expanding authoritarian governance may create legal cover for mass surveillance: Increasingly authoritarian governments are relying on surveillance to monitor dissidents and suppress online speech. Some may attempt to sidestep human rights-driven export controls by criminalizing protected behavior or weakening oversight bodies. Because the Pall Mall agreement allows exceptions for domestic law, signatories could also exploit this loophole, reducing its effectiveness.

Changing attitudes toward private-sector offensive operations may expand the cyber offensive tools market: The Salt Typhoon hacks against nine major US telecommunications companies have renewed discussions around "hacking back," or conducting offensive operations to counter cyber attacks. If allowed, this would open up the offensive cyber tools market to private companies, significantly increasing the risks of proliferation. Regulations on this industry should consider the potential for future non-government users, including mechanisms to ensure transparency and responsible use.

Mitigations

Defenders can strengthen resilience against commercial cyber intrusion capabilities through prioritizing cyber hygiene best practices, especially for high-value targets such as lawyers, journalists, or political opposition figures.

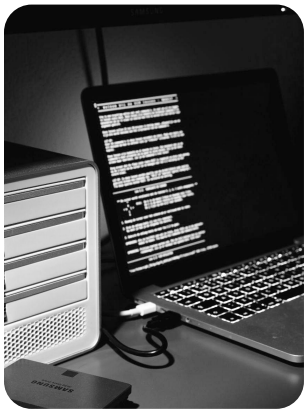
- **Enforce Secure Mobile Practices:** Maintain strict separation between personal and corporate devices, keep all devices up-to-date, and enable features like lockdown mode and periodic reboots to reduce mobile spyware risks.
- **Monitor Indicators of Compromise (IoCs) Used by Spyware:** Recorded Future tracks infrastructure used by Candiru and other commercial offensive cyber tool providers that can be used to detect the presence of spyware.
  Recorded Future's Secops Intelligence and Threat Intelligence can help support these efforts.
- **Implement Device Management:** Use mobile device management (MDM) solutions to monitor and enforce security controls across employee devices.
- **Strengthen Human Defenses:** Invest in employee security awareness training and foster a culture of minimal data exposure to reduce spearphishing risks and mitigate the impact of a breach.

Further Reading

SOURCE	TITLE
Insikt Group	Tracking Candiru's DevilsTongue Spyware in Multiple Countries
Insikt Group	Predator Still Active, with New Client and Corporate Links Identified
Insikt Group	Predator Spyware Infrastructure Returns Following Exposure and Sanctions
Insikt Group	Predator Spyware Operators Rebuild Multi-Tier Infrastructure to Target Mobile Devices
Insikt Group	"Mobile Not-Petya": Spyware Zero-Click Exploit Development Increases Threat of Wormable Mobile Malware

Risk Scenario

Scenario: A highly successful and growing cyber intrusion service provider reports a data breach, indicating that a variety of sensitive data — including exploits and targeting information — has been compromised.



First-order Implications

Threat

Data Exposure or Theft: Operational tools, zero-days, client rosters, or target information are exfiltrated. Attackers may leak this data or repurpose it for other intrusions.

Risks

Operational disruption: Ongoing activity is disrupted and exploit stockpile is compromised.

Competitive disadvantage: Current and future customers no longer trust that the company will be able to safeguard highly sensitive operations.

Legal and compliance failure: Investigations will be carried out to determine whether the company failed to meet contractually required security standards.

Second-order Implications

Threat

Cyber Weapons Proliferation: Companies race to patch exposed zero-days, while criminals take advantage of newly exposed tools. The rapid exploitation increases the risk of rapidly spreading mobile exploits (see, for example, this Insikt Group report on "Mobile NotPetya").

Risks

Operational disruption: Widespread exploits of the unpatched vulnerabilities to disable systems, steal data, or compromise infrastructure, disrupting core business functions.

Brand impairment: Public incidents stemming from zero-day exploitation can damage user trust and brand credibility, particularly if the vendor is slow to respond.

Third-order Implications

Threat

Diplomatic fallout: Worsening relations as revelations of who is deploying cyber surveillance tools emerge. Increased sanctions and other economically punitive measures shift international trade.

Risks

Diplomatic or legal consequences: Surveillance operations may violate international law or treaties.

Operational disruption: Exposure of surveillance tools and methods can burn intelligence operations, weakening situational awareness and response capabilities.

Increased surveillance and harassment of dissidents: Exposure of tools and targets emboldens countries to target political adversaries.

Imprisonment, harassment, or assassination: Targets of surveillance face increased risk of human rights violations.

Increased surveillance or harassment: Travelers to countries using these capabilities may be under increased scrutiny.

Key

Legal or compliance failure: Breach of laws, regulations, or industry standards resulting in liability or sanctions.
Operational disruption: Interruption to normal business processes affecting productivity or service delivery.
Brand impairment: Damage to reputation that reduces customer trust and market value.
Financial fraud: Unauthorized manipulation or theft of financial assets for personal or organizational gain.
Competitive disadvantage: Loss of market position due to inferior capabilities, intelligence, or innovation.

References:

The Risk Business: Second Edition
Intelligence to Risk
The Intelligence Handbook